Information Security Manual

Contents

1. Scope

1.1 Purpose

Through a comprehensive suite of information security control objectives and supporting policy statements, this manual explains how the international standard code of practice for information security management, applies within MDINetworX. Its purpose is to communicate management directives and standards of care to ensure consistent and appropriate protection of information throughout MDINetworX. It can be used as part of an Information Security Management System as specified in ISO/IEC 27001 and related standards. The policy also covers control objectives as specified in HiTrust.

1.2 Definition and objective

MDI's definition of Information security is to keep data secure from unauthorized access or alteration, both when it's stored and when it's being transmitted from one system to another or from one location to another.

MDI has a need to implement information security as MDI is handling sensitive data of US citizens and are required to follow HIPAA privacy rule.

1.3 Target Audience

This document applies to all MDINetworX (US & India) and affiliate associates, including temporary associates and associates of affiliated third-party organizations.

1.4 Status and Applicability

This manual has been reviewed and approved by the Chief Technology Officer (CTO). The guiding principles listed in Appendix A have been approved by Sr. Management to apply throughout MDINetworX.

It is applicable:

- Throughout MDINetworX including any subsidiaries and joint ventures in which MDINetworX has a controlling Interest
- At all MDINetworX locations in all countries
- To all MDINetworX associates and others working on behalf of MDINetworX in a similar capacity including contractors, consultants, temporary workers, student placements, and so on (known collectively throughout as "workers")
- To all information/data, information processing/computer systems and networks (collectively known as "information assets") owned by MDINetworX, or those entrusted to MDINetworX by third parties.

The policy statements in this manual are supported by a range of security controls documented within operating procedures, technical controls embedded in information systems, and other controls advised to associates from time to time by management through information security standards, procedures and guidelines. The supporting controls refer to, and gain authority from, the information security policy statements included in this manual.

1.5 Policy Exceptions

Despite the care that has been taken in authoring, reviewing, and approving this policy manual, the authors cannot possibly foresee all possible circumstances or situations in which it might apply. It is therefore conceivable that exceptional situations or emergencies may occur when practical considerations clearly override or negate the policy statements made herein. Examples include the introduction of new legal or regulatory obligations that conflict with specific policy statements, or where slavishly following the policies to the letter would cause unacceptable health and safety risks.

2. Glossary

Term	Description
ESO	Enterprise Security Officer
HIPAA	Health Insurance Portability and Accountability Act
EPHI	Electronic PHI
PHI	Protected Health Information
SIT	Software Team
CTO	Chief Technology Officer
IT	Information Technology Team
NDA	Non-Disclosure Agreement
HR	Human Resource Team
IAO	Information Asset Owner
Removable Storage Media	Removable storage media includes any device that can be plugged to the information system for example: pen drive, CD Rom, DVD ROM etc.,
Sr. Management	Applies to any or all the employees of the management having designation Associate Vice President or above.
Secure Area	Area where information systems contains sensitive information.

3. Risk Assessment and Treatment

3.1 Assessing Security Risks

3.1.1 Cooperation

The execution, development and implementation of remediation programs are the joint responsibility of the Compliance Team and process owners of each process. Associates are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable. Associates are further expected to work with the Compliance Team in the development of a remediation plan.

3.1.2 Assessing Security Risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques should be applied to the whole organization.

Risk assessment is systematic consideration of the following two areas:

- The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets
- The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented

The results of this assessment are required to help, guide and determine the appropriate MDINetworX management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of MDINetworX's organization or individual information systems.

Annual reviews of security risks and implemented controls must be carried out in order to:

- Take account of changes to business requirements and priorities
- Consider new threats and vulnerabilities
- Confirm that controls remain effective and appropriate

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that MDINetworX management is prepared to accept. Risk assessments should be carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

3.2 Treating Security Risks

Before considering the treatment of a risk, the Sr. Management decides the criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not reasonable in light of low risk. Such decisions should be recorded.

For each of the risks identified following the risk assessment, a risk treatment decision needs to be made. Possible options for risk treatment include the following:

- Applying appropriate controls to reduce the risks
- Knowingly and objectively accepting risks, providing they clearly satisfy MDINetworX's policy and criteria for risk acceptance
- Avoiding risks by not allowing actions that would cause the risks to occur
- Transferring the associated risks to other parties, for example, insurers or suppliers

For those risks where the risk treatment decision has been to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by a risk assessment. Controls should ensure that risks are reduced to an acceptable level taking into account the following:

- Requirements and constraints of legislation and regulations
- Organizational objectives
- Operational requirements and constraints
- Cost of implementation and operation in relation to the risks being reduced, and remaining proportional to MDINetworX's requirements and constraints
- The need to balance the investment in implementation and operation of controls against the harm likely to result from security failures

Information security controls should be considered at the systems and projects requirements specification and design stage (failure to do so can result in additional costs and less effective solutions, and maybe, in the worst case, inability to achieve adequate security).

It should be kept in mind that no set of controls can achieve complete security, and that additional management action should be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support MDINetworX's goals.

4. Security Policy

4.1 Management Intent

MDINetworX management is committed to information security and supports all efforts towards that goal, including the establishment and implementation of policies, procedures, and associate awareness efforts.

Security policies are based on ISO 27001 and are organized in the following high- level areas:

- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Capital Management Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

4.2 Control

MDINetworX's security policies must be approved by the Compliance Team and published and communicated to all associates and relevant external parties.

Information security is characterized here as the preservation of each of the following:

- Confidentiality: ensuring that information is accessible only to those authorized to have access
- Integrity: safeguarding the accuracy and completeness of information and processing methods
- Availability: ensuring that authorized users have access to information and associated assets when required

Information security is achieved by implementing a suitable set of controls, which include policies, practices, procedures, organizational structures, and software functions. These controls are established to ensure that the specific security objectives of MDINetworX are met.

4.3 Review of the Information Security Policies

The Compliance team creates information security policies based on three criteria:

- To obtain regulatory and standards compliance
- To mitigate risk/vulnerabilities
- To prevent and mitigate security incidents

Once the need for a policy has been determined, the Compliance team drafts the proposed policy and presents it to the Sr. Management (see **5.1.1 Management Commitment to Information Security**) for review. Based on feedback,

the Compliance team adjusts the proposed policy and presents it to the Sr. Management for endorsement. Ultimately the policy is approved by the Sr. Management.

The Compliance team reviews all security policies annually and possibly after any incident occurs or whenever there is a change in applicable laws and regulation. The annual reviews include the following considerations:

- Results of independent audits
- Process performance and Security policy compliance
- Changes that could affect policies, such as the following
    - Organization
    - Business circumstances
    - Resource availability
    - Contractual, regulatory, and legal conditions
    - Technical environment
- Trends related to threats and vulnerabilities
- Reported information security incidents (see 13.1.1 Reporting Information Security Events)

If modifications are needed to a policy, the process for policy approval (see above) is repeated. Once the policies are approved, the approved policies are uploaded on the MDINetworX intranet. http://10.0.0.3:8000/Default.aspx

4.4 Authorities

Only the Sr. Management shall have the final authority to approve any change related to Information Security.

5. Organization of Information Security

5.1 Internal Organization

5.1.1 Management Commitment to Information Security

The Board of Directors ("the Board") is ultimately accountable for corporate governance as a whole. The management and control of information security risks is an integral part of corporate governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to the Sr. Management.

Management give overall strategic direction by approving and mandating the information security principles in this manual but delegate operational responsibilities for physical and information security to the Compliance Team.

Sr. Management depends heavily on the Compliance Team to coordinate activities throughout MDINetworX, ensuring that suitable policies are in place to support MDINetworX's security principles. Sr. Management also rely on feedback from the Compliance Team and process owners to ensure that the principles, and policies are being complied with in practice.

Sr. Management shall involve the ISO for the annual Capital Planning and discuss the Capital Planning for information Security. The resources shall be aligned as per the security activities planned.

Sr. Management demonstrates their commitment to information security by:

- Ensuring that information security goals are identified, meet MDINetworX's requirements, and are integrated into this policy manual
- appoint a senior-level information security official for the development, implementation and administration of security matters; In addition, ensures that employees, contractors and third-party users are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems
- ensures that employees, contractors and third-party users achieve a level of awareness on security relevant to their roles and responsibilities within the organization
- establish and communicate the organization's priorities for organizational mission, objectives, and activities;
- appoint a senior-level information security official for ensuring that the organization's information security processes are in place, are communicated to all stakeholders, and consider and address organizational requirements
- formally assign an organization single point of contact or group to provide program oversight (governance), review and update the organizations security plan (strategy, policies, etc.), ensure compliance with the security plan by the workforce, and evaluate and accept information security risk on behalf of the organization
- formulate, review, and approve information security policies and a policy exception process;
- periodically, at a minimum, annually, review and assess the effectiveness of the implementation of the information security policy;
- Provide clear direction and visible management support for security initiatives
- Provide the resources needed for information security
- initiate plans and programs to maintain information security awareness;
- Reviewing and re-approving the principles every year

- Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests, and so on
- ensure that all appropriate measures are taken to avoid cases of identity theft targeted at patients, employees and third parties;
- ensure that the implementation of information security controls is coordinated across the organization;
- determine and coordinate, as needed, internal or external information security specialists, and review and coordinate results of the specialists' advice throughout the organization.
- formally appoints security specialists, and review and coordinate results of the specialists' advice throughout the organization.
- providing guidelines about state security expectations of the ISO's role within the organization
- having motivated and complying with the security policies of the organization
- achieve a level of awareness on security relevant to their roles and responsibilities within the organization
- conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working
- continue to have the appropriate skills and qualifications
- retains responsibility for its cybersecurity program in compliance with applicable regulatory requirements
- designates a senior member of the organizations personnel (ISO) responsible for direction and oversight of the third-party service provider
- requires the third-party service to maintain a cybersecurity program of its own that protects the organization and complies with applicable regulatory requirements

5.1.2 Information Security Coordination

Information security activities must be coordinated throughout MDINetworX to ensure consistent application of the security principles and policy statements in this manual.

Compliance Team is responsible for:

- Providing the strategic direction, support and resources necessary to manage all types of local security issues and thus ensure that MDINetworX's information assets are appropriately and consistently protected
- Coordinating and sharing information with each other to ensure consistent execution of this policy manual across all MDINetworX locations
- Identifying specific Significant Information Assets.
- Gathering metrics and other information on the overall effectiveness of information security controls in their remit, and reporting this to the Sr. Management.
- ensuring security activities across the entire organization are executed in compliance with the information security policy and that deviations are identified and reviewed
- identifying reasonable procedure to handle non-compliance
- assessing the adequacy and coordinate the implementation of information security controls
- effectively promoting information security education, training and awareness throughout the organization
- ensuring that the threat information has been communicated to identified internal and external stakeholders

5.1.3 Allocation of Information Security Responsibilities

The following is a list of the roles involved with information security with clearly defined responsibilities for each:

- Sr. Management / Directors
  - Approving the action proposed by the Information Security Officer
  - Approving the trainings and/or training plans for information security, privacy and HIPAA
  - Approving risk mitigation ideas suggested by the Information Security Officer
  - Approving any task/action that includes costing to the organization.
- Information Security Officer / Data Privacy Officer / Compliance Manager
  - implementing and acting in accordance with the organization's information security & privacy policies;
  - protecting assets from unauthorized access, disclosure, modification, destruction or interference;
  - executing particular security processes or activities;
  - to ensure that the organization's information security processes are in place, are communicated to all stakeholders, and consider and address organizational requirements.
  - responsible for the organization's individual privacy protection program
  - responsible for serving as the point of contact for all privacy-related issues including the receipt of privacy-related complaints,
  - providing privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed
  - responsible to have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing
  - Determines the nature and scope of the security incident
  - Contacts the CIMT members
  - Determines resources necessary to aid in security incident response
  - Coordinates security incident response efforts
  - Provides information for the investigation (e.g. video footage, proximity card transactions, audit logs, etc.)
  - Contacts other departments as appropriate
  - Monitors and reports on the progress of the investigation
  - Ensures evidence gathering, chain of custody and preservation is performed as appropriate
  - Prepares a written summary of the security incident and corrective actions taken
  - Organizes and participates in Post-Mortem/Lessons Learned meetings
- IT Help Desk
  - Performs containment, eradication and remediation tasks based on ISO guidance
  - Installs service packs and patches
  - Installs malware abatement software
  - Ensures that backups are in place for all critical systems
  - Ensures that system logs are available and assists the ISO in analysis/investigations/Forensics
  - Analyzes network traffic
  - Runs network tools such as sniffers, port monitors, traffic analyzers, and other analysis as requested
  - Takes necessary actions to block traffic from suspected sources
  - Investigates signs of firewall breach
  - Contacts Internet Service Providers
- Users
  - Users are required to co-operate with the ISO and the IT Team for carrying out their security roles

5.1.4 Authorization Process for Information Processing Facilities

Significant new IT facilities, systems, applications, and so on, must be authorized by the Sr. Management, specifying and/or confirming their purpose and use and checking that all relevant security policies and other control requirements will be satisfied.

5.1.5 Confidentiality Agreements

All associates, contractors, and third parties must agree with and sign a non- disclosure agreement.

Requirements for confidentiality or “Non-Disclosure Agreements” reflecting MDINetworX’s needs to protect its proprietary and personal information must be identified and regularly reviewed by Sr. Management.

Confidentiality agreements should be reviewed by the Sr. Management before such agreements take effect.

The following requirements for confidentiality agreements should be considered as examples:

- A definition of the information to be protected (for example, information classified as MDINetworX Restricted or MDINetworX Secret (see 7.2.1 Classification Guidelines)
- Agreement duration has been kept as indefinitely
- Required actions when the agreement is terminated (for example, return of all printed materials and media; secure deletion of data copies and backups)
- Assurances of appropriate safeguards to aid in the protection of select information and to help avoid unauthorized uses or disclosures of select information (such as circulation limited on a ‘need to know’ basis)
- Intellectual property rights
- Changes to restrictions on permitted rights and uses of the information
- The right to audit and monitor compliance
- Process for notification of unauthorized disclosure or confidential information incidents, and other anticipated actions
- Liabilities

Confidentiality agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply (see also 14.2.1 Identification of Applicable Legislation).

Confidentiality agreements should be reviewed periodically and when changes occur that influence the requirements.

5.1.6 Contact with Authorities

Only Directors or HR manager has the authority to contact with the following:

- Law enforcement
- Health & Safety department
- All other government authorities excluding fire department

Any associate or manager can contact the fire department in case of any major fire incident that cannot be handled using our fire extinguishers.

5.1.7 Contact with Special Interest Groups

Membership in specialist security forums and professional associations is required as a means to do the following:

- Improve knowledge about best practices and staying up to date with relevant security information
- Ensure the understanding of the information security environment is current and complete
- Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities
- Gain access to specialist information security advice
- Share and exchange information about new technologies, products, threats, or vulnerabilities
- Provide suitable liaison points when dealing with information security incidents (see 13.2 Management of Information Security Incidents and Improvements).

The ISO will coordinate management of such groups plus access to other external sources of information security knowledge and services.

MDI has defined a process to quickly identify newly discovered security threats and vulnerabilities such as a credible subscription service. The organization has a process to map new threats and vulnerabilities into its security policies, guidelines and daily operational procedures.

In addition, no user has any right to post any update/incident/information regarding MDI NetworX on any social network that includes but are not limited to:

- Facebook
- Twitter
- WhatsApp
- Instagram
- Pinterest

5.1.8 Independent Review of Information Security

Given their governance obligations, senior management needs formal assurance that the information security principles and policies are adequate to minimize MDINetworX's information security risks. Therefore, an independent review of MDINetworX's control objectives, controls, policies (including this manual), processes, and procedures for information security is required. The independent review should occur at annually or when significant changes to the security implementation occur. The Date/Time, scope and nature of assessment shall be notified to the Information Security Officer.

Such an independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness of MDINetworX's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives (see 15.2.1 Compliance with Security Policies and Standards). Address the need for changes to the approach to security in light of evolving circumstances, including the policy and control objectives and other opportunities for improvement, including those based on regular vulnerability assessments (e.g., network scans and penetration testing); carefully control information security tests to limit the risks to confidentiality, integrity, and system availability;

At the request of the ESO, such a review must be carried out by individuals independent of the area under review, such as an internal audit organization, an independent manager, or a third-party organization specializing in such reviews.

The results of the independent review must be recorded and reported to the Sr. Management. The independent review records must be maintained for three years. Also, any recommendations made shall be approved by the Sr. Management.

MDINetworX shall continuously improve the information security management program through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventative actions and management review.

If the independent review identifies that the MDINetworX's approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in this Information Security Policy Manual, management must consider corrective actions.

5.2 External Parties

5.2.1 Identification of Risks Related to External Parties

Types of Access

The type of access given to a third party is of special importance. For example, the risks of access across a MDINetworX network connection are different from risks resulting from physical access. Types of access that must be considered are:

- Physical access, for example, to offices, computer rooms, and filing cabinets
- Logical access, for example, to MDINetworX's databases, and information systems
- Network connectivity between MDINetworX's and the external party's networks, for example, permanent connection or remote access
- whether the access is taking place on-site or off-site

Reasons for Access

Third parties may be granted access for a number of reasons. For example, there are third parties that provide services to MDINetworX and are not located on-site but may be given physical and logical access, such as:

- Hardware and software support staff, who need access to system level or low-level application functionality
- Trading partners or joint ventures, who may exchange information, access information systems or share databases

Information might be put at risk by access from third parties with inadequate security management. Where there is a business need to connect to a third-party location, a risk assessment should be carried out to identify any requirements for specific controls. It should take into account the type of access required, the value of the

information, the controls employed by the third party and the implications of this access to the security of MDINetworX's information.

MDI shall ensure that the identification of risks related to external party access takes into account the following issues:

- the information asset(s) an external party is required to access
- the type of access the external party will have to the information and information asset(s), as provided above
- the value and sensitivity of the information involved, and its criticality for business operations
- the controls necessary to protect information that is not intended to be accessible by external parties
- the external party personnel involved in handling the organization's information
- how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed
- the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information
- the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information
- practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident
- legal and regulatory requirements and other contractual obligations relevant to the external party are taken into account
- how the interests of any other stakeholders may be affected by the arrangements.

On-Site Third-Parties and Contractors

Third parties that are located on-site for a period of time as defined in their contract may also give rise to security weaknesses. Examples of on-site third party include:

- Hardware and software maintenance and support staff
- Cleaning, catering, security guards and other outsourced support services
- Student placement and other casual short-term appointments
- Consultants
- External auditors
- Clients

It is essential to understand what controls are needed to administer third party access to information processing facilities. Generally, all security requirements resulting from third party access or internal controls should be reflected by the third-party contract.

MDI shall ensure to enter into legally binding contracts with its third parties that include provisions for the security, protection, and non-disclosure of information (to include PHI) and assets.

For example, if there is a special need for confidentiality of the information, non- disclosure agreements might be used.

Access to MDINetworX's information and information processing facilities by third parties must not be provided until the appropriate controls have been implemented and a contract defining the terms for the connection or access has been signed.

Not-Allowed Behavior While on MDINetworX Premises:

While on MDINetworX premises, third parties and contractors are not allowed the following:

- To use digital photography technologies
- To connect any device, including, but not limited to a personal computer, cellular phone, PDA, router, printer, and so on, to any MDINetworX device, phone line for modem use, or network (except for stand-alone units, such as a projector or printer), unless specifically authorized by the appropriate MDINetworX Business Unit using a MDINetworX established "Guest Kit" connection.
- To use the following wireless technologies:
    - All wireless fidelity (Wi-Fi), non-Wi-Fi fixed wireless, Bluetooth (for non-voice communications), cellular modems (air cards), and cellular technology to be used as a modem for a personal computer.

Security Requirements while dealing with Third Parties

Arrangements involving third party access to MDINetworX information processing facilities must be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the MDINetworX's security policies and standards.

MDI shall develop, disseminate, and review/update annually the list of current service providers, which includes a description of services provided.

MDINetworX organizations should satisfy themselves as to the indemnity of their supplier. The following terms must be considered for inclusion in the contract:

- The requirements in the IT019-Information Security Policy for Supplier Relationships
- Asset protection, including:
    - Procedures to protect organizational assets, including information, software and hardware
    - any required physical protection controls and mechanisms
    - controls to ensure protection against malicious software
    - Remote access connections between the organization and all external parties shall be secured via VPN. VPN password shall be the combination of user defined 4-digit numeric code and real time generated 4-digit code produced by MobilePass (an application from Gemalto for Two Factor Authentication).
    - Procedures to determine whether any compromise of the assets, such as, loss or modification of data, has occurred
    - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract

  - confidentiality, integrity, availability, and any other relevant property of the assets
  - Restrictions on copying and disclosing information
  - A description of each service to be made available
  - The target level of service and unacceptable levels of service
- user and administrator training in methods, procedures, and security
- ensuring user awareness for information security responsibilities and issues
- responsibilities regarding hardware and software installation and maintenance
- Provision for the transfer of staff where appropriate
- The respective liabilities of the parties to the agreement
- Responsibilities with respect to legal matters, such as, data protection legislation
- Intellectual property rights and copyright assignment and protection of any collaborative work
- Access control procedures, that cover the following items:
  - the different reasons, requirements, and benefits that make the access by the third party necessary
  - Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords. In addition, the access granted shall be for limited period and shall be revoked as soon as the task is completed by the third party.
  - An authorization process for user access and privileges
  - A requirement to maintain a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to such use
  - a statement that all access that is not explicitly authorized is forbidden
  - a process for revoking access rights or interrupting the connection between systems
  - The definition of verifiable performance criteria, their monitoring and reporting
  - The right to monitor, and revoke, user activity
  - The right to audit contractual responsibilities or to have those audits carried out by a third party
  - The establishment of an escalation process for problem resolution; contingency arrangements should also be considered where appropriate
  - Responsibilities regarding hardware and software installation and maintenance
- A clear reporting structure and agreed reporting formats
- A clear and specified process of change management
- Any required physical protection controls and mechanisms to ensure those controls are followed
- User and administrator training in methods, procedures and security
- Controls to ensure protection against malicious code
- Arrangements for reporting, notification and investigation of security incidents and security breaches involvement of the third party with their subcontractors.
- arrangements for reporting, notification (e.g., how when and to whom), and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement, stating:
  - the third party, following the discovery of a breach of unsecured covered information, notifies the organization of such breach, including the identification of each individual whose unsecured PII has been, or is reasonably believed by the third party to have been, accessed, acquired, or disclosed during such breach
  - all notifications are made without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of a breach if the third party is an agent of the organization, otherwise the timing of the notification is explicitly addressed in the contract if the third party is not an agent of the organization
  - evidence is maintained demonstrating that all notifications were made without unreasonable delay

  - any other information that may be needed in the notification to individuals, either at the time notice of the breach is provided or promptly thereafter as information becomes available
- a description of the product or service to be provided, and a description of the information to be made available along with its security classification
- the target level of service and unacceptable levels of service
- the definition of verifiable performance criteria, their monitoring and reporting
- the right to monitor, and revoke, any activity related to the organization's assets
- the right to audit responsibilities, defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors
- the penalties exacted in the event of any failure in respect of the above
- the establishment of an escalation process for problem resolution
- service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities
- the respective liabilities of the parties to the agreement
- responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g. data protection legislation) especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries
- intellectual property rights (IPRs) and copyright assignment (see 6. b) and protection of any collaborative work
- conditions for renegotiation/termination of agreements:
  - a contingency plan is in place in case either party wishes to terminate the relation before the end of the agreements
  - renegotiation of agreements if the security requirements of the organization change
  - current documentation of asset lists, licenses, agreements or rights relating to them
- The organization requires third-party providers to notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.

5.2.2 Addressing Security when dealing with Clients

Access by clients to MDINetworX's information and systems should be subject to essentially the same processes of risk assessment and controls implementation as for other external parties (see 6.2.1 Identification of Risks Related to External Parties). For example:

- Legally binding contracts or agreements should be in place, defining information security requirements and obligations on clients (and indeed on MDINetworX), including security incident reporting arrangements.
- Individual clients should be authenticated by suitable user authentication mechanisms and be granted limited access to certain networks, systems, applications, functions and data necessary for legitimate business purposes (with all other access explicitly forbidden).
- MDINetworX retains the right to monitor and record usage and to restrict, suspend or revoke user access rights, and inform clients of this fact.
- Suitable controls should be in place to ensure data and systems confidentiality (for example, access controls), integrity (for example, data entry validation) and availability (for example, resilience, performance, and capacity management).
- The following security terms are addressed prior to giving customers access to any of the organization's assets:
  - description of the product or service to be provided;
  - the right to monitor, and revoke, any activity related to the organization's assets; and

- the respective liabilities of the organization and the customer.

- It is ensured that the customer is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.

5.2.3 Addressing Security in Third Party Agreements

To ensure the confidentiality of Electronic Protected Health Information (EPHI) as well as the availability and integrity of EPHI, MDINetworX enters into a business associate agreement with each of its clients for whom MDINetworX acts as a business associate.

The business associate agreement establishes mutual responsibilities for compliance with the HIPAA Privacy and Security Rules. If MDINetworX shares EPHI with an agent or sub-contractor, MDINetworX requires that the agent or sub-contractor sign a business associate or similar confidentiality agreement as required by the Privacy and Security Rules.

MDI shall ensure that the Third-Party Agreements shall include requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain.

The organization maintains written agreements (contracts) that includes an acknowledgement that the third-party is responsible for the security of the data the third-party possesses or otherwise stores, processes or transmits on behalf of the organization, or to the extent that they could impact the security of the organizations information environment.

MDI's agreements ensure that there is no misunderstanding between the organization and the third-party. Organizations satisfy themselves as to the indemnity of the third-party.

MDI shall ensure that the service provider protects the company's data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.

Security of Third-Party Access

Access to the MDINetworX's information processing facilities by third parties must be controlled in order to maintain the security of MDINetworX information processing facilities and information assets accessed by third parties.

MDI shall ensure that due diligence, including an evaluation of the information security risks posed by external parties, is carried out to identify any requirements for specific controls where access to sensitive information by external parties is required prior to establishing a formal relationship with the service provider. Access by external parties to the organization's information is not provided until the appropriate controls have been implemented and, where feasible, a contract/NDA has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party. It is ensured that the external

party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.

MDI shall perform a background check or obtain its information security certifications (SOC Report, HITRUST, NAID AAA or ISO 27001 Certificate) wherever it is feasible for all its suppliers who will have physical or logical access to MDI's information systems or suppliers who will store MDI's data. Where there is a business need for such third-party access, a risk assessment should be carried out to determine security implications and control requirements. Security requirements must be defined in a contract and agreed to with the third party. A primary goal of the contract is to obtain satisfactory assurances from the third party that they will safeguard MDINetworX information, including EPHI. This contract should include information regarding:

1. Third party's responsibility to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the security, confidentiality, integrity, and availability of EPHI which third party creates, receives, maintains, or transmits on behalf of MDINetworX;
2. Third party's duty to report to MDINetworX any security incidents of which it becomes aware; and
3. Termination of contract by MDINetworX if MDINetworX determines that third party has violated a material term of the contract.
4. Third party agreement/contract shall include the personnel security requirements including security roles and responsibilities for third-party providers that are coordinated and aligned with internal security roles and responsibilities.

Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access.

This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

Roles and responsibilities of Third-party IT consultant:

- Ensure that the network and the infrastructure suggested are up and running and as a whole provide a high degree of reliability and availability.
- Suggesting competitive prices from suppliers when appropriate to ensure cost effectiveness
- Determine problem areas that exist in the infrastructure and identify opportunities to improve the same
- Risk analysis and management, information access controls and sanctions for failure to comply
- Set the access and authorization controls for everyday operations as well as emergency procedures for data
- Evaluation and compliance with security measures
- Disaster recovery and emergency operating procedures
- Managing crises situation, which may involve complex technical hardware or software problems
- Assess information security rise periodically
- Conduct functionality and gap analysis to determine the extent to which key business areas and infrastructures comply with statutory and regulatory requirements
- Evaluate and recommend new information security technologies and countermeasure against threats to information or privacy

- Assists in the planning an implementation of additions deletions and major modification to the supporting infrastructure
- Implement network security at the enterprise level established by corporate security policies
- Oversee the administration and maintenance of the MDI NetworX infrastructure
- Oversee the administration of the MDI NetworX WAN
- Oversee trouble shooting system backups, archiving and disaster recovery and provide expert support when necessary
- Work with IT teams to help implement internal systems
- Ensures that company assets are maintained responsibly
- Email communication with the client
- Attend conference call with client whenever necessary
- Abide by company policies

6. Asset Management

6.1 Responsibility for Assets

6.1.1 Inventory of Assets

Management must identify MD NetworX's significant information assets; Meaning information assets, both individual items and related groups of information assets (such as all the computer hardware and software providing a given IT service). Management must understand their relative values in order to specify appropriate protection.

MDI identifies and inventories all assets including information, encrypted or unencrypted, wherever it is created, received, maintained, or transmitted, including organizational and third-party sites, and document the importance of these assets. This inventory is maintained and reviewed by the IT team, the review takes place once in every three months and the approval is provided by the Associate Director – IT. Further the organizational inventories of IT assets are updated during the installations, equipment removals, system changes.

MDI shall ensure that all the covered information is encrypted and no covered information shall be available within the network that doesn't have encryption.

All media in MDI's environment is considered highly critical and no separate treatment is done to media.

MDI shall ensure that the asset inventory includes all systems connected to the network including the network devices, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory includes every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches and firewalls), printers, storage area networks, the asset inventory created must also include data on whether the device is a portable device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network. The asset inventories include all information necessary to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and a business value. The inventory does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned. Records of property assigned

to employees is reviewed and updated once in three months. The record is be used to document and ensure that all property is returned to the organization upon employee termination.

Information assets include:

- **Intangible information assets:** the information content of databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information, proprietary knowledge, experience and expertise, reputation, and brand
- **Tangible information assets:** documentation, printouts, and so on
- **Software assets:** application software, system software, development tools, and utilities either owned by or licensed to MD NetworX
- **IT-related physical assets:** computer and telecommunications hardware (processors, monitors, laptops, routers, telephone exchanges), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, computer rooms, and so on
- **IT-related services:** computing and communications services, application services and utilities supporting IT equipment, such as computer room air- conditioning, lighting, power and grounding

MDI however does not have any Fax machine installed in any of its location considering the risk that the PHI can be sent/received from the fax machines.

In case if there is any transfer of IT related assets the Inventory shall be updated accordingly.

An accurate and complete inventory must be maintained by IT team. Further the Compliance Manager shall identify all Significant Information Assets along with key parameters, such as the corresponding Information Asset Owners and locations.

The asset inventory shall have the following captured:

- Hostname
- Category of the Asset
- Unique identifier of the IT asset
- Type of information system component (e.g. server, desktop, laptop etc.)
- Model information of the IT asset
- Operating system type and version and application software version/license information of asset
- Presence of virtual machines
- Physical and logical location (e.g. building/room number, IP address) of the IT asset
- Data ownership and custodian by position and role
- Operational status of the IT asset
- Primary user of the IT asset

The MAC address & Administrator is not included in the asset inventory for security reasons.

6.1.2 Ownership of Assets

Accountability should be distributed at the lowest feasible level of management within the organization. Although responsibility for designing, implementing, managing, and/or operating information security controls may be delegated by Compliance Team to other parties (such as IT and the SIT), the Compliance Team remain personally accountable for their proper protection.

IT Team is responsible for classifying their information assets.IT team classifies its assets as either "Medium" or "Critical" based on their importance and sensitivity. These classifications are recorded and maintained in a dedicated sheet, which is regularly reviewed by the IT team to ensure proper categorization.

IT is committed to treating all assets with the utmost care, particularly those classified as "Critical." This commitment to asset security is integral to our information security management system.

The ownership, custodianship, and information classification are based on the identified importance of the asset, the business value of the asset, security classification of the asset, levels of protection of the asset, and sustainment commensurate with the importance of the assets

6.1.3 Acceptable Use of Assets

Information security aspects of local and remote systems access (for example, passwords and authentication devices), corporate and personal e-mail, Internet browsing, use of portable computers and Personal Digital Assistants, and so on, must be covered by a suite of guidelines developed and maintained by the Compliance Team under authority of the CTO; endorsed, supported, and enforced by managers throughout MDINetworX, and communicated to relevant workers by suitable means (for example, hardcopy leaflets, intranet pages, awareness presentations, newsletters, and so on).

MDI understands the seriousness of the information protection, however due to business requirement, MDI cannot restrict the usage of copy/print screen on the systems as the users may take the screen-prints to explain any error message that they may encounter on any of the client systems. However, MDI shall ensure that the access to external emails are restricted to limited users and the same shall be monitored using the Sophos DLP. In addition, the DLP shall also log the copying of data and usage of the print-screen. Further, the suspicious activity on DLP logs will be considered as incidents and further investigations are being performed as per the incident management process.

Acceptable use agreements are signed by all employees before being allowed access to information assets. The acceptable use policy shall state that they provide their consent of monitoring all the activities that is carried by the employee on any of the information assets.

The acceptable use policy shall state the below:

- All mobile and computing devices that connect to the internal network must comply with the User Access Policy & Mobile Device Security Policy.
- System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

- You must lock the screen or log off when the device is unattended.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
- All of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- Where it is believed that a user has failed to comply with this policy, they will face the company's disciplinary procedure. If the user is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the user's disciplinary record.
- I agree to return all the assets assigned to me in good condition once the roles assigned to me are completed or once the asset is no longer required to pursue my roles or upon my termination of roles from this organization.
- All company employees, contractors or temporary staff who have been granted the right to use the company's asset(s) are required to sign this agreement confirming their understanding and acceptance of this policy.

6.2 Information Classification

6.2.1 Classification Guidelines

The information covered in this policy includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All documentation (hardcopy and electronic form) originated within MDINetworX must indicate the Information Classification. It is the responsibility of the Document Owner to determine the correct classification.

All associates should familiarize themselves with the information labeling and handling guidelines that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager.

All MDINetworX information is categorized into the following five main classifications based on the risk of the information or the document:

Information Classification	Description
PHI and EPHI	*PHI and EPHI* information are any MDINetworX or client document containing Protected Health Information or any data containing Electronic Protected Health Information (EPHI).

MDINetworX Public	*MDINetworX Public* information is information that is publicly available without additional contractual obligations.
MDINetworX Restricted	*MDINetworX Restricted* is information shared only on a need to know basis after the parties have signed a contract containing confidentiality protections. For example, the contractual obligations can be in a Master Agreement or NDA
MDINetworX Secret	*MDINetworX Secret is information that is very sensitive in nature and therefore requires special approval to be shared outside of MDINetworX. Prior to sharing MDINetworX Secret information, personnel must get approval from the Compliance Team and Associate Director.*
MDINetworX Internal Use Only	*MDINetworX Internal Use Only is information that is not permitted to be shared outside of MDINetworX.*

Guidelines on handling the above-mentioned categorized data:

(a) **PHI and ePHI:** All the physical forms (Paper PHI) received at MDI US office shall be shredded within a period of 30 days post the scanning activity. The data that is converted to images shall be uploaded on MDI's internal SFTP. The data that is captured from the image along with the images are termed as ePHI. All the ePHI data stored at MDI premises shall be encrypted both when in rest and during the course of transmission. None of the users are allowed to share any data with this classification on emails or any other communication channel. Only IT team is authorized to upload the data with this classification on SFTP. All the data handled by Operations and/or Quality will be classified with this classification by default. Only Operations, Quality, Sr. Management, IT Team and Compliance team can have access to data with this classification. Further, the PHI data will only be stored on the Golem & DocGem (PMS) databases and on the NAS device (where the backup of the DBs are stored).

(b) **MDINetworX Public:** The data with this classification would be something that can be shared with any of the vendors/third-parties and/or client. This includes data that is hosted on MDI's website or is available freely on any of the websites. However, any user who wish to share data without any classification has to primarily contact the compliance team to verify the correct classification.

(c) **MDINetworX Restricted:** The data/file with this classification can only be shared only after approval from the Sr. Management or from the Compliance Manager. All the audit reports and Employee records can be classified under this classification. This can be classified with the term "Confidential". Only HR Team, Compliance Team, Sr. Management and IT team can have access for data with this category.

(d) **MDINetworX Secret:** The data/file that contains the any financial information of the organization then it would be classified under this classification. The finance folder is classified under this category. The access to the finance folder is limited to finance team and Sr. Management. Only Sr. Management, IT Team and Finance team can have access for data with this category.

(e) **MDINetworX Internal Use:** All the reports prepared by managers for their analysis can be classified under this category. These documents/reports are for internal use and is not being published or shared with anyone outside MDI.

6.2.2 Marking

All information should display the assigned security classification. For more detailed information, see 6.2.4 Information Labeling and Handling. If any document is observed without any labelling then the same shall be categorized under Public.

6.2.3 Disposal/Destruction

Information System Disposal:

- The disposal of all the Media is performed in-house as per the below process:
  1. On an annual basis, an inventory review is performed by the IT Team. IT systems to be disposed are identified during the review.
  2. Once systems to be disposed are finalized, approvals are taken from the Compliance lead for initiating the disposal.
  3. Based on the approvals received, the data from the hard disk shall be formatted
  4. Once the data is completely wiped off from the system, a gate pass is raised for moving the systems out of the premises for disposing
  5. Gate pass is approved, and the systems are handed over the vendor for scrapping
- If no longer required, the contents of any re-usable media that are to be repurposed or removed from the MDI NetworX should be made unrecoverable.

Procedure

Initiation of Disposal Request:

The disposal process begins when a disposal request is raised by the asset owner, department, or authorized personnel.

The initiator provides essential details such as the asset name, description, and sensitivity level.

Encryption Verification:

The IT department verifies whether the digital assets are encrypted to protect sensitive data.

Approval of Disposal:

The disposal request is reviewed and approved by the designated authority within the organization.

Documentation:

A disposal log is created, including the following fields:

- Asset Name
- Asset Description
- Disposal Request raised by
- Was Asset Formatted (Yes/No)
- Outward Registry Documented (Yes/No)
- Approved By
- Approval Date
- Disposal handled by

Sensitivity
Technique of Disposal

Asset Formatting:
If required, assets are securely formatted according to the organization's data disposal policy.

Outward Registry Documentation:
The disposal is documented in an outward registry to maintain a record of the transfer to the e-waste company.

Encryption Key Handling:
Encryption keys, if applicable, are securely managed to ensure future decryption is possible, as needed.

Transfer to E-Waste Company:
The digitally disposed assets are securely handed over to a trusted e-waste company for further processing.

E-Waste Processing:
The e-waste company processes the digital assets based on environmental and data security standards.

Confirmation of Disposal:
The e-waste company provides a confirmation of disposal or certificate of data destruction, if applicable.

Documentation Update:
The disposal log is updated to include details of the transfer to the e-waste company, including the date of transfer and any relevant reference numbers.

Monitoring and Compliance:
Periodic audits are conducted to ensure compliance with the disposal process.

Data Security Measures:
All data security measures, including encryption and data handling, are documented and retained.

Paper Disposal:

- Subsequent to the scanning of incoming documents they are marked for secured storage.
- Documents are securely stored for the duration of the retention period (30/60/90 Calander days).
- After the completion of the retention period, they are securely shredded onsite by an AAA NAID-certified shredding vendor.
- Secured bins are provided by the vendor for collecting paper media to be disposed. They are locked to prevent tampering or access, and they are emptied in a timely manner.
- Subsequent to the secure destruction of the documents, a “Certificate of Destruction" verifying the on-site, secure destruction is issued.
- In addition, records are kept detailing when and how documents were disposed of, including the date, responsible employee, and the quantity of documents shredded.
- Employees are trained in the importance of secure document disposal and the procedures in place to ensure compliance.
- Regular audits are performed on the document disposal process to ensure that it is being followed correctly and that all documents are being properly destroyed.

6.2.4 Information Labeling and Handling

All major information assets must be accounted for and have a nominated owner as described in 6.1.2 Ownership of Assets.

It is important that an appropriate set of procedures are defined for information labeling and handling in accordance with 6.2.1 Classification Guidelines. These procedures need to cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity:

- Copying
- Storage
- Transmission by post and electronic mail
- Transmission by spoken word, including mobile phone
- Destruction

Output from systems containing information that is classified as being PHI or Confidential should carry an appropriate classification label (in the output). The labeling should reflect the classification according to the rules established in 6.2.1 Classification Guidelines. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, compact disks, and cassettes), electronic messages, and file transfers. Outputs from application systems handling covered information are limited to the minimum necessary and sent only to authorized terminals/locations.

Physical labels are generally the most appropriate forms of labeling. However, some information assets, such as documents in electronic form, cannot be physically labeled, so an electronic means of labeling needs to be used. For example, all documents must include one of the MDINetworX information classifications.

At MDI, handling and labeling of all physical assets is performed according to asset classification level. Below is the physical labelling convention that is currently followed at MDI:

1. For Laptops: MDI-LPT-<<Emp ID>>
2. For desktops : MDI-D<<Floor Number>>DB-<<Emp ID>>
3. For external hard-drives : MDI-HDD-<<Sequence Number>>
4. For servers : MDI-SVR-<<Sequence Number>>
5. Others generic : MDI-Asset Category-<<Sequence Number>>

The information that MDI receives shall be stored in a secured manner (encrypted) and shall be processed as per the guidelines provided by the client. Covered information is encrypted when stored in non-secure areas and, if not encrypted at rest, the organization documents its rationale.

MDI shall maintain an information asset log that contains the details of the information available on each information system. In addition, it should clearly specify the assets on which the PHI/covered information is available. The information asset log shall be reviewed on annual basis.

6.3 Asset Hardening Policy

This policy applies to all components of the information technology infrastructure and includes:-

(a) Computers including laptops
(b) Servers

(c) Application Software
(d) Peripherals
(e) Routers and switches
(f) Databases
(g) Cell phones

All staff within the IT Department must understand and use this policy. IT staff are responsible for ensuring that the IT infrastructure is hardened and that any subsequent changes to systems do not affect the hardening of systems.

6.3.1 Desktop/Laptop Hardening Process:

(a) Install System

Install the systems as per the vendor's instructions/MDI's standard procedures.

(b) Remove Unnecessary Software/Services

Most of the systems come with a variety of software packages / services to provide functionality to all users. Software / service that is not going to be used in a particular installation should be removed or uninstalled from the system.

(c) Disable or Remove Unnecessary Usernames

Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions, which are not used, should be removed or disabled. For all accounts, which are used, the default passwords should be changed. Consideration should be given to renaming predefined accounts if it will not adversely affect the system.

(d) Patch System

The system should be patched up to date. All relevant service packs and security patches should be applied.

(e) Perform Vulnerability Scan

The system should be scanned with a suitable vulnerability scanner. The results of the scan should be reviewed and any issues identified should be resolved.

(f) Vulnerabilities

If there are no significant vulnerabilities, the system can be prepared for live use.

(g) Install Anti-Virus and Anti-Malware

Sophos anti-virus and anti-malware package should installed on the system to prevent malicious software introducing weaknesses in to the system.

(h) Install Data Loss Prevention tool

Sophos DLP package should be installed on the system wherein to prevent Data Loss.

(i) Browser Settings

MDI shall automate controls (e.g., browser settings) to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations). In addition, access to browser shall be restricted for cell phones.

(j) Production System

Prior to handling the system for production use, ensure that the system hard-drive is encrypted using bit locker.

6.3.2 General Hardening Guidelines:

(a) Do not connect a Server to the Internet until it is fully hardened.
(b) Place the server in a physically secure location.
(c) Install service packs, patches and hot fixes
(d) Secure remote administration of the server and configure for encryption, low session time-outs and account lockouts
(e) The database shall be encrypted using AES 256 encryption algorithm
(f) Disable Telnet service and enable SSH
(g) Only software that has been approved for use by the IT department may be installed on the organization's computing devices.
(h) Non-essential software applications and services will be uninstalled or disabled as appropriate.
(i) Servers, PC's and laptops will be configured to prevent the execution of unauthorized software.
(j) Bios passwords will be implemented on all PCs and laptops to protect against unauthorized changes.
(k) The boot order of PC's and laptops will be configured to prevent unauthorized booting from alternative media.
(l) Access to the local administrator account will be restricted to members of IT Department to prevent the installation of unauthorized software and the modification of security software and controls.
(m) Default passwords will be changed following installation and before use in a production environment.
(n) All PC's and servers will be protected by anti-virus and anti-spyware software. The anti-virus and anti-spyware software will be configured to automatically download the latest threat databases.
(o) The use of removable media will be disabled.
(p) All devices on the organization's network will be scanned for vulnerabilities as and when there is any new patch released. Any issues identified will be reviewed and rectified as appropriate.
(q) MDI shall ensure that strong cryptography would be used to protect the confidentiality and integrity of the remote access sessions to the internal network.

(r) Set separate password for domain and VPN. The VPN password shall be strong and complex and satisfies MDI's password policy.
(s) The passwords for Admin users shall be very strong & very complex and shall be changed once in each quarter.
(t) Wherever encryption is used MDI shall use a minimum of AES 256 encryption or stronger.
(u) The date and time for all the systems shall be synced with one of the server and the server to follow the standard time zone across the MDI premises. (GMT+0530 for India and GMT-0500 for USA)
(v) All the systems shall be taken in the domain so that all the Group Policy applies to all the systems.

6.3.3 Audit Policy Settings:

(a) Configure Account Logon audit policy.
(b) Configure Account Management audit policy.
(c) Configure Logon/Logoff audit policy.
(d) Configure Policy Change audit policy.
(e) Configure Privilege Use audit policy.

7. Human Capital Management Security

Purpose

The objective of Human Capital Management Security or the Human Resource Security is to ensure that all employees (including contractors and any user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated.

Scope

This policy applies to all employees and contracted employees of MDI NetworX.

Management Commitment

Sr. Management shall provide complete cooperation in all the activities performed by HR and need to ensure that HR is performing all the activities as per the guidelines provided to them.

MDI shall ensure that it has defined appropriate resources, roles and responsibilities to establish, implement, operate, monitor, review and maintain the Information Security Management Program.

The ISMP conducts independent audits to determine the continuing suitability, adequacy and effectiveness of the program.

The organization continuously improves the ISMP through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventative actions and management review.

7.1 Prior to Employment

7.1.1 Roles and Responsibilities

Security roles and responsibilities (see 5.1.3 Allocation of Information Security Responsibilities) including compliance with this Information Security Policy Manual as well as any specific responsibilities for the protection of particular information assets or for the execution of particular security processes or activities (such as reporting security incidents or near misses), should be documented where appropriate for example in job descriptions and employment contracts.

Job descriptions and so forth must be maintained and updated to reflect changes in roles and responsibilities, particularly in respect of information security aspects and should indicate a given job's level of authorized access to EPHI. At the very least, an associate's manager, and so on, must review job descriptions, at the time of the annual appraisal or whenever someone is promoted.

HR is responsible for following all the provided guidelines in this section of the document.

7.1.2 Screening

Background verification checks should be carried out in accordance with relevant laws, regulations and ethics, and in proportion to the business requirements, the classification of the information to be accessed, and the perceived risks.

A screening process must be carried out for contractors, and third-party information systems users. Where contractors are provided through an agency, the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party should clearly specify all responsibilities and notification procedures for screening.

All offers of employment at MDI NetworX depend upon clear results of a thorough background check. Background checks will be conducted on all candidates who accept the offers granted by MDI. MDI shall send the request for the background checks to its vendor as soon as the employee joins the organization. The employees are informed about the screening during the joining process and a letter of authorization is being signed by the employees which is later shared with the verification vendor for processing the screening activity.

Access to Information systems would be granted only after receiving positive (green) result in the Background verification report. Domain access shall only be created after getting a confirmation from the Compliance team that the team has reviewed the Background check report. In case, if there is any urgency in creating the domain ID, then the same can be done only after receiving approval from the Sr. Management.

Background Checks will include:-

- Social Security Verification (US Employees only)
- Prior Employment verification
- Personal and/or Professional references
- Educational verification
- Criminal History

7.1.3 Terms and Conditions of Employment

The terms and conditions of employment should reflect MDINetworX's security policy in addition to clarifying and stating the following:

- That all associates, contractors, and third-party users who are given access to sensitive information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities
- The associate's, contractor's and any other user's legal responsibilities and rights, for example regarding copyright laws (see 14.1.2 Intellectual Property Rights)
- Responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the associate, contractor, or third-party user (see 6.2.1 Classification Guidelines)
- Responsibilities of MDINetworX for the handling of personal information, including personal information created as a result of, or in the course of, employment with MDINetworX.
- Responsibilities that are extended outside of MDINetworX's premises and outside normal working hours, for example in the case of working remotely
- Actions to be taken if the associate, contractor, or third-party users disagree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to MDINetworX's assets associated with information systems and services
- Responsibilities of MDINetworX's employee, contractor or third-party user for the handling of information received from other companies or external parties.
- MDI ensures that conditions relating to security policy survive the completion of the employment in perpetuity by getting the NDA signed by each employee or contractor
- All the employees shall coordinate all the activities that HR or Compliance Team carries to get complete compliant on the Information security policy and procedures.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 7.3 Termination or Change of Employment).

7.2 During Employment

7.2.1 Management Responsibilities

All workers must comply with MDINetworX's information security principles, policies, standards, procedures, and guidelines, plus requirements identified in the terms and conditions of their employment or service contracts and applicable laws and regulations.

Acceptable use agreements shall be signed by all employees before being allowed access to information assets. MDI shall maintain a list of all workforce members including employees, contractors, vendors and business partners with

access to sensitive information (e.g., PHI). The same is updated on a monthly basis and shared with Information Security Officer.

Sr. Management shall approve the use of information assets. Further, if any unauthorized activity is identified by monitoring or other means, this activity is brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Managers are responsible for ensuring that associates, contractors, and third-party users:

- Are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems
- Are instructed to fulfill the security policies of MDINetworX
- Achieve a level of awareness on security relevant to their roles and responsibilities within MDINetworX (see 7.2.2 Information Security Awareness, Education, and Training)
- Conform to the terms and conditions of employment, which includes MDINetworX's 5.1.1 Information Security Policy Document and appropriate methods of working

7.2.2 Information Security Awareness, Education, and Training

All associates of MDINetworX and, where relevant, third party users / contractors must receive appropriate information systems security awareness training within 15 days post joining and regular updates in policies and procedures on an annual basis. Access credentials to the information systems are provided to the new joiner / contractors / third parties only after completion of Information security trainings. The training (for new joiner or the annual refresher training) includes security requirements, privacy, state & federal laws, legal & teleworker responsibilities and business controls, as well as training on the correct use of information systems, for example, log on procedures.

Further, ongoing training includes security and privacy requirements as well as training in the correct use of information assets and facilities.

Further, the training shall also cover about :

(a) how the organization addresses each area of incident management
(b) how events or incidents are identified
(c) the actions the organization takes in response to events or incidents as appropriate to the area of training.
(d) Also, during the training sessions users are made aware about not sending covered information using any end-user messaging technologies including but not limited to MS Outlook and MS Teams.

Further refer to section 12 of this documentation for the incident management process.

MDI shall ensure that role-based trainings are also provided that discusses how the organization addresses each area; how events or incidents are identified, and the actions the organization takes in response to events or incidents, as appropriate to the area of training.

The role-based training for the Information Security roles & Responsibilities are provided to:

- CIMT Team members
- All the managers irrespective of the department (Users with Designation Assistant Manager and above)

The role-based training for the Continuity Plan roles & Responsibilities are provided to all the managers irrespective of the department (Users with Designation Assistant Manager and above).

MDI doesn't provide any specific training to senior executives as MDI provides HIPAA & ISMS security awareness training to all its employees including its senior executives.

MDINetworX provides the appropriate training to all its associates on policies, security and the correct use of information processing facilities to minimize possible security risks. It is the responsibility of the associate to enroll and receive such training when offered by MDINetworX.

MDINetworX ensure plan for training activities are developed, implemented, maintained and reviewed for consistency with the risk management strategy and response priorities.

MDI shall ensure that it prohibits users from installing unauthorized software, including data and software from external networks, and ensure users are made aware and trained on these requirements by providing proper instructions on installation of software in its security training provided to all its employees.

MDI shall ensure that all its employees, contractors and third-party users using or having access to the organization's assets are aware of the limits existing for their use of the organization's information and assets associated with information processing facilities, and resources. Users are responsible for their use of any information processing resources, and of any such use carried out under their responsibility. The compliance manager shall include the asset usage limitations in the ISMS training that is provided to all the employees and users having access to MDI's Information systems. In addition to this, the usage of MDI's information assets shall be provided in the acceptable use policy and the same shall be acknowledged by the users.

In case if there is any change in the information security policy or other security policies relevant to the users, then the respective users shall be informed about the same through self-study document within a month the change takes place.

MDI shall ensure that it provides incident response and contingency training to information systems users consistent with assigned roles and responsibilities:

(i) within 90 days of assuming an incident response role or responsibility
(ii) when required by information system changes
(iii) within every 365 days thereafter.

Further, the above meeting will be conducted over a call/classroom related to incident response and contingency roles and responsibilities of each of the members.

All employees shall be appropriately educated and periodically reminded of the following during the information security training or the HIPAA training. Even if users are not having access to printers, facsimile and/or copy machines, it is always good to have knowledge about the risk with these assets in advance.

1) not discussing or leaving critical information in the open or areas where unauthorized individuals could overhear or see the information;
2) taking the necessary precautions, including not to reveal covered information, to avoid being overheard or intercepted when making a phone call by::
   a) people in their immediate vicinity, particularly when using mobile phones;
   b) wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; or
   c) people at the recipient's end;
3) not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing
4) not registering demographic data in software that could be collected later for unauthorized use
5) addressing the problems with printers, facsimile and copy machines, such as:
   a) unauthorized access to built-in message stores to retrieve messages;
   b) deliberate or accidental programming of machines to send messages to specific numbers; and
   c) sending documents and messages to the wrong number either by misdialing or using the wrong stored number;
   d) registering demographic data, e.g., email address or other personal information, in any software to avoid collection for unauthorized use; and
   e) page caches and store page functionality that modern facsimile machines and photocopiers have in case of a paper or transmission fault, which will be printed once the fault is cleared.

MDI shall ensure that its security awareness and training program

(i) will either be provided by online, classroom or by sharing the study material on email and ensuring that everyone has attended the training or has read the training material. If the training is provided online, then the attendance can be collected by looking at the users who has joined the training. If study material has been shared, then the same can be confirmed with an acknowledgement email stating that the user has read and understood the policy or the training material shared.
(ii) MDI shall ensure that all its workforce members shall receive the ISMS and HIPAA trainings which are designed for security awareness amongst the users.
(iii) MDI shall ensure that it provides awareness training to all its workforce members immediately after any change in the information systems and not later than 60 days of the change implemented
(iv) MDI shall ensure that it provides HIPAA, Medicare/CMS FWA & ISMS training to all its workforce within 15 days of the user's joining date and at least once in a year post the initial training.
(v) Violations of any of the security policies by employees and contractors will result in sanctions or disciplinary action. All policies are communicated to all employees and contractors at the time of joining and annually thereafter as part of ISMS & HIPAA training.
(vi) The policy outlines security requirements and procedures for safeguarding unattended equipment, encompassing physical security measures and access controls.
(vii) Users are responsible for promptly terminating active sessions when finished, using appropriate mechanisms like screen savers or logout procedures to secure their sessions.

(viii) Users are required to log off from mainframe computers, servers, and office PCs at the end of their sessions, distinguishing this action from merely switching off the screen or terminal.

(ix) As part of mandatory training, dedicated phishing awareness training is provided to all employees. This training covers the identification of phishing attacks and the correct procedures for reporting such incidents.

HIPAA

All associates of MDINetworX and, where relevant, third party users / contractors must receive appropriate HIPAA awareness training within 15 days post joining and regular updates in policies and procedures on an annual basis. The Compliance Team will work with the Training Department to implement a security awareness and training program to ensure the security of EPHI. Such training will include awareness training for all personnel and education on virus/malware protection, malicious code protection, log on monitoring/reporting, and password management. The training program will also include periodic security reminders for associates, agents, and contractors.

Managers are responsible for making sure that their staff attends required security training and any additional security training appropriate to their job functions.

MDI shall ensure that users of mobile computing devices in public places take care to avoid the risk of overlooking by unauthorized persons. Training is arranged for all personnel whether/not using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that are implemented.

7.2.3 Application Security Awareness, Education, and Training

All the software team is required to follow the below application security measures at a minimum:

- Govern: To do application security well, you must govern the application security program.
- Find: To do application security well, you must find security issues.
- Fix: To do application security well, you must fix security issues.
- Prevent: To do application security well, you must prevent security issues from happening in the first place

The detailed training shall be conducted by the head of the software team

7.2.4 Disciplinary Process

MDINetworX will apply appropriate sanctions against members of its workforce who fail to comply with its security policies and procedures or the requirements of the Security Rules. All workforce members will be subject to sanctions up to and including termination.

MDI ensures that sanctions for violations of the organizations security policies do not commence without prior verification of a breach. The formal disciplinary process ensures that correct and fair treatment for employees who are suspected of committing breaches of security and that a graduated response that takes into consideration factors (impact, number of offenses, training, regulatory requirements, and contractual obligations). And for each incident, the organization documents the personnel involved in the disciplinary process, the steps taken and the timeline associated

with those steps, the steps taken for notification, the rationale for the discipline, whether the discipline was due to a compliance failure, and the final outcome.

Managers will work with the Compliance Lead, and Human Resources (HR) to determine when a violation has occurred and will apply progressive disciplinary action to members of the workforce who fail to comply with MDINetworX's privacy and security policies and procedures. This activity has to be completed within 24 hours of the receipt of the information about the breach. Also, all the employees have been trained during HIPAA & ISMS training on notifying any suspicious activity to the Information Security Officer as soon as they observe without any delay.

Factors that may be considered when determining the level/severity of disciplinary action include whether the violation was the result of:

- Carelessness or negligence
- Curiosity, or
- A desire for personal gain or malice

Sanctions that will be considered include, but are not limited to, any one or combination of the following:

- Counseling – Review the policy and procedure with the associate to make certain that the associate understands the policy and the procedures to follow. Counsel the associate on the importance of following MDINetworX's HIPAA Security Policies and Procedures.
- Retraining – Arrange for the associate to attend re-training on the policies and procedures violated and confirm their completion of the re-training.
- Reassignment – Transfer the associate to another job where they can demonstrate competence.
- Termination – Terminate the associate from further employment with MDINetworX.

MDI shall ensure that the above sanction process is followed for personnel failing to comply with established information security policies and procedures and notifies the personnel's immediate reporting manager within 12 hours when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction.

Sanction Process:

Once any personnel is identified as breaching any of the information security policy. Compliance Manager will decide the suitable sanction for the personnel. However, if compliance manager decides to terminate the access of the personnel, he is authorized to do so without any manager's approval. The Compliance Manager shall ensure that all the access granted to the personnel shall be immediately terminated without further delay.

Documentation Requirements

If any sanctioning/disciplinary action takes place, documentation of such action must be created and retained for a minimum of six years, tolling from the date of the documentation's creation or the date when the document last was in effect, whichever is later.

Further the disciplinary tracker shall have the following:

- the nature and gravity of the breach and its impact on business
- whether or not this is a first or repeat offense
- whether or not the violator was properly trained
- relevant legislation
- business contracts

7.3 Termination or Change of Employment

7.3.1 Termination Responsibilities

Procedures must be established to assure that when the employment of a workforce member ends, physical and logical access to MDINetworX's facilities and information systems are terminated as defined within the Termination Procedures.

The Compliance Manager will work with MDINetworX managers, HR, and the Service Desk to implement and maintain procedures for termination of access to systems and facilities. Managers must report all anticipated terminations to HR in accordance with HR termination policies.

The communication of termination responsibilities must include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within the Acceptable Use Policy and Non-Associate NDA continuing for a defined period after the end of the associate's, contractor's or third-party user's employment.

Responsibilities and duties still valid after termination of employment must be included in associate, contractor, or third-party user contracts.

Changes of responsibility or employment must be managed as the termination of the respective responsibility or employment, and the new responsibility or employment should be controlled as described in 7.1.2 Screening.

During Internal Transfers, the previous access shall be revoked except the domain and emails. The new access (folder/application) shall be requested by the new manager.

A termination checklist is present which identifies all the steps to be taken and assets to be collected during the exit process of a user. The termination process includes the return of all previously issued software, any corporate documents and all other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media, as applicable for the user. HR team is responsible for ensuring the termination checklist activity is carried out at time of employee offboarding (Resigned Employees)

MDI shall ensure that the access rights for the terminated individual is disabled in a timely manner, at least within 24 hours.

7.3.2 Return of Assets

All associates, contractors and third-party users must return all of MDINetworX's assets in their possession upon termination of their employment, contract, or agreement.

The termination process must be formalized to include the return of all previously issued software, corporate documents, and equipment. Other MDINetworX assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also must be returned.

In cases where an associate, contractor or third-party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.

7.3.3 Removal of Access Rights

Access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors including:

- whether the termination or change is initiated by the employee, contractor, third-party user, other workforce member, or by management and the reason of termination
- the current responsibilities of the employee, contractor, workforce member or any other user
- the value of the assets currently accessible

Employees' access to information, computer/network systems, and facilities must be revoked promptly when they leave MDINetworX, or revised if they transfer or change status. This includes logical and physical access rights (including any shared user IDs and group access rights), authentication tokens, access cards, keys, and so on.

In circumstances, such as summary dismissal for fraud or theft, the risks relating to a employees' termination may justify the immediate revocation of their access rights. In conjunction with HR, the Compliance Manager, the employees' manager should ensure that the risks of continued access are assessed and appropriate action is initiated at the earliest opportunity by immediately revoking the worker's network login ID and physical access.

When an employee moves to a new position of trust, logical and physical access controls are re-evaluated as soon as possible but not to exceed 30 days. The organization also ensures employees or workforce members that are terminated understand their obligations to ensure any covered information for which they had prior access remains confidential by adding the same clause in the NDA.

Upon termination or changes in employment for employees, contractors, third-party users, or other workforce arrangement, physical and logical access rights and associated materials (includes but not limited to passwords, keys, documentation that identify them as current members of the organization) are removed or modified to restrict access within 24 hours and old accounts are closed after 90 days.

Further, changes of employment or other workforce arrangement that includes Internal Transfer is reflected in removal of all access rights that were not approved for the new employment or workforce arrangement. Access changes due

to personnel transfer are managed effectively. The access rights are removed or adapted include physical and logical access.

During Termination MDI shall ensure:

- To revoke
  - the physical access
  - the logical access
- To collect
  - Keys
  - identification cards
  - IT systems and application
  - Subscriptions
- To remove from any documentation that identifies them as a current member of the organization.

If a departing employee, contractor, third-party user or other workforce member has known passwords for accounts remaining active, these are changed upon termination or change of employment, contract, agreement, or other workforce arrangement.

Access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors.

MDI shall ensure that access rights to information assets and facilities are reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors that includes

- whether the termination or change is initiated by the employee, contractor, third-party user, other workforce member, or by management and the reason of termination
- the current responsibilities of the employee, contractor, workforce member or any other user
- the value of the assets currently accessible.

8. Physical and Environmental Security

Purpose: The purpose of this section is to establish a procedure regarding the Physical & Environmental security measures MDI has taken.

Scope: The scope shall include all the equipment's, infrastructure and locations of the MDI NetworX.

Management Commitment: Sr. Management shall demonstrate its commitment by giving complete co-operation about the Physical & Environmental Security and by providing feedback and guidance as and when required. Management should prioritize the Physical and Environmental Security measures.

Coordination: Wherever required Admin team shall coordinate with respective teams to ensure Physical & Environment Security measures are implemented. Admin Team shall also ensure that it satisfy all the compliance requirements including legal and contractual compliances.

Responsibility: Admin Head holds the full responsibility to ensure that all the controls specified in this section of the policy are implemented.

Roles:

- Planning: IT along with Compliance team would be responsible for planning of the security of the Data Center
- Funding: Sr. Management would be responsible for releasing/allocating funds required for the Physical and Environmental security requirements
- Reviews: Compliance Team shall review the best practices and standards that can assist with the evaluating physical security controls
- Environmental Controls: Admin Team is responsible for all the security measures for environmental controls
- Natural Disaster Controls: Admin Team is responsible for implementing any/all natural disaster controls
- Supporting Utilities Controls: Admin Team is responsible for implementing all the supporting utilities controls
- Physical Protection and access controls: Admin team is responsible for implementing all the physical protection and access controls
- Physical Security Awareness and training: Compliance Team and Training team are responsible for the physical security awareness and training.
- Contingency Plans: Compliance Team is responsible for implementing suitable contingency plans

Compliance:

i. Determine which managers are responsible for planning, funding, and operations of the physical security of the Data Center.
ii. Review best practices and standards that can assist with evaluating physical security controls, such as ISO/IEC 27002:2013.
iii. Establish a baseline by conducting a physical security controls gap assessment that will include the following as they relate to your campus Data Center:

a. Environmental Controls
b. Natural Disaster Controls
c. Supporting Utility Controls
d. Physical Protection and Access Controls
e. System Reliability
f. Physical Security Awareness and Training
g. Contingency Plans

iv. Determine whether an appropriate investment in physical security equipment (alarms, locks or other physical access controls, identification badges for high-security areas, etc.) has been made and if these controls have been tested and function correctly.
v. Provide responsible managers guidance in handling risks. For example, if the current investment in physical security controls is inadequate, this may allow unauthorized access to servers and network equipment. Inadequate funding for key positions with responsibility for IT physical security may result in poor monitoring, poor compliance with policies and standards, and overall poor physical security.
vi. Maintain a secure repository of physical and environmental security controls and policies and establish timelines for their evaluation, update, and modification.
vii. Create a team of physical and environmental security auditors, outside of the management staff, to periodically assess the effectiveness of the measures taken and provide feedback on their usefulness and functionality.

8.1 Secure Areas

8.1.1 Physical Security Perimeter

Physical risks relating to Significant Information Assets must be formally analyzed using the standard information security risk assessment process approved by the Compliance Manager. In conjunction with the respective manager's, suitable cost-effective controls must be designed and implemented to mitigate the identified risks, typically including:

- Clearly defined security domains (for example, "computer rooms") separated by effective security perimeters with controlled entry/exit points
- Strong walls and access-controlled doors
- Manned reception areas and biometric access doors to restrict physical access to authorized personnel only, and to positively authenticate visitors by suitable means of identification (such as photographic identity cards and facial recognition)
- MDI has the below barriers implemented to access covered information:
    - Locked Perimeter : Biometric access doors installed to enter the MDI premises
    - Secured Interior : Security/Admin Team monitoring the interior from CCTV
    - Security Container : Manned security at the entrance of the main door and CCTV's installed to cover the entire facility.
- MDI shall ensure that the server room door closes automatically and it cannot be kept open. In addition, MDI shall install a door delay alarm and the door should contain electronic locks which can be accessed only by authorized personnel using the biometric access point.

8.1.2 Physical Entry Controls

Designated secure areas housing Physical and/or electronic information systems should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Access to secure areas should be restricted to authorized persons who have been positively authenticated, for example by possession of a physical key/access token, a photographic identity card and, where appropriate, knowledge of a password or PIN. Access to secure areas should be routinely logged and shall be reviewed by Compliance Team according to the risk of unauthorized access.

Third party personnel and other visitors should be granted restricted access to secure areas only if required (for example, for maintenance and support purposes) and authorized by management, and should be supervised by workers. The dates and times of entry and departure should be recorded by workers in a visitor log. Visitors should be issued with instructions on the security requirements of the area and on emergency procedures.

Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter (for example, using locked equipment racks and equipment cages to prevent unauthorized access to MDINetworX equipment by third parties on a shared site).

Workers and visitors should keep their identification badges on display about their person at all times whilst on site. Workers and security guards should politely but firmly challenge unsupervised/unescorted strangers and anyone not wearing visible identification.

Access to a delivery and loading area from outside of the US office building is restricted to identified and authorized personnel. The external doors of a delivery and loading area are secured when the internal doors are opened. Visitor/courier delivery personnel are not allowed to enter the office premises.

MDI shall develop, approve and maintain a list of individuals with authorized access to the facility where the information system resides. Issues authorization credentials for facility access and reviews the access list and authorization credentials at least quarterly, removes individuals from the facility access list when access is no longer required.

Access rights to secure areas should be regularly reviewed and if necessary updated by management, for example, to prevent former workers gaining access (see 7.3.3 Removal of Access Rights).

MDI follows the Physical access matrix for providing the access to each individual. Further the access for each individual is reconciled at least once in each quarter. If the access is no longer required, the compliance team shall ensure that the access is suspended.

8.1.3 Securing Offices, Rooms and Facilities

Sensitive facilities should be located to minimize access by the public, where possible. Areas, such as computer rooms housing significant information assets must be relatively unobtrusive with no obvious signs identifying their presence, especially from public areas.

Support functions and office equipment, such as photocopiers and fax machines should be sited appropriately within the secure area if this is cost-effective.

Offices should be locked shut when unattended; especially doors and windows to designated secure areas. Secure areas should ideally not have windows accessible from public areas but if external windows are necessary, additional protection, such as toughened glass or bars should be applied.

CCTV should be professionally designed, installed, tested, and maintained, covering all external doors and accessible windows, and internal secure areas.

Administration Team is responsible for ensuring that physical security measures are operating correctly. Admin Team is responsible for monitoring CCTV and intimating Compliance Team on any suspicious notices. Physical protection of the equipment is required to maintain the security of the equipment identifier; and, if the identifier is digital/electronic, it is stored and transported in an encrypted format to protect it from unauthorized access.

8.1.4 Protecting against External and Environmental Threats

Secure areas, such as computer rooms must incorporate suitable protective measures to minimize the possibility and impacts of incidents, such as fires, floods, earthquakes, explosions, civil unrest, and so on, while also complying with relevant health and safety obligations (for example, clearly marked fire exits and clear passageways).

Physical risk assessments must consider threats both inside and outside computer rooms, for example fires or floods within the computer equipment or in neighboring rooms or buildings. This includes the possibility of smoke and flames spreading through voids or being introduced via air conditioning intakes, and leaky pipes or roofs above the computers.

Fire protection for computer rooms (especially automated ‘full-flood’ or water sprinkler fire extinguisher systems) must be professionally designed, installed and maintained, taking into account the level of risk (for example, the value of equipment at risk and the business criticality of the services provided) and the special requirements typical of computer facilities (for example, fast flowing air will disperse smoke and ‘fan the flames’, requiring careful location of high-sensitivity smoke detectors and power interlocks between fire and air conditioning systems).

Handheld fire extinguishers must be of a type suitable for use on electrical fires and must be placed near properly identified fire exits such that a person fighting a fire has ready access to the exit. They must be professionally maintained and regularly tested even if located in access-controlled areas.

Fire extinguishers are located throughout the facility, and are no more than fifty (50) feet away from critical electrical components.

MDI shall ensure that the fire authorities are automatically notified when a fire alarm is activated in all its US offices. However, this is not feasible in India as the due to the restrictions from the fire department. However, MDI India office shall ensure that it notifies the fire department as soon as there is any fire incident.

Maintenance of the fire extinguishers and the fire protection systems shall be performed in each quarter.

Computer room workers should be properly trained in fire procedures including responding to alarms, evacuating the premises safely, fighting small fires if safe to do so and delaying the release of extinguishant until the room is evacuated.

Hazardous or combustible materials, such as cardboard and plastic packaging and solvents should be stored securely at a safe distance away from computer rooms.

Bulk supplies, such as stationery and backup tapes, redundant equipment and spares should not normally be stored within computer rooms until required, unless they are stored within suitable fire safes.

Fallback equipment and backup media must be located well away from the primary site to reduce the risk of coincident damage or restricted access due to a major physical incident.

8.1.5 Working in Secure Areas

Workers should not normally be informed of the existence of, and nature of assets and activities within, computer rooms, and so on, unless they have a legitimate need to know.

Unsupervised (lone) working in secure areas should be avoided wherever possible, especially outside normal working hours.

Vacant secure areas should be physically locked and periodically checked by security guards and/or workers.

Photographic, video, audio, or other recording equipment (such as camera phones) should be forbidden from designated secure areas unless authorized by management. Notices to this effect should be displayed (for example on access passes and/or signs) and security guards and managers should be alert potential non-compliance.

8.2 Equipment Security

8.2.1 Equipment Siting and Protection

IT equipment, storage facilities, and associated items should be located to minimize unnecessary access into work areas. Keyboards, displays, printers, fax machines, and so on, should be positioned to reduce the probability of being overlooked by unauthorized people.

MDI shall ensure that all its network equipment is located in such a location that no unauthorized user can get access to them. The network equipment includes but not limited to WIFI router, firewall, switches etc.,

Only personnel with designation of Assistant Manager and above shall have the access to the printers to reduce the risk. The managers who are taking prints are responsible for its proper usage and destruction.

Specific controls may be required to protect Significant Information Assets against unauthorized access in addition to the general physical controls. These should be specified by the IT manager following a risk assessment.

Appropriate controls must be in place to minimize risks, such as theft, fire/smoke, explosion, flood, lightning, vibration, chemicals, and electromagnetic radiation, or failure of or interference with key supplies, such as cooling water, chilled air, and power (see 8.2.2 Supporting Utilities).

The organization restricts physical access to wireless access points, gateways, unattended handheld devices, networking/communications hardware, and telecommunication lines.

All buildings should be suitably protected against lightning for example using earthed lightning rods on high points. Lightning protection filters should be fitted to external copper communications lines. Wherever possible, servers and magnetic media (whether in use or in store) should be located several meters away from lightning conductors to minimize the possible effects of intense magnetic fields induced by lightning strikes.

Eating, drinking, and smoking must be expressly forbidden in secure areas or elsewhere in proximity to Significant Information Assets.

Environmental conditions (such as temperature, humidity, and power supply) should be controlled and monitored for situations or trends which could adversely affect the operation of IT facilities.

The impact of a disaster in nearby premises (such as a fire in a neighboring building or floor, water leaks or an explosion in the street) should be considered. Where it is uneconomic to minimize these threats, suitable contingency plans must be in place (see 13 Business Continuity Management).

MDI shall ensure that computers that store or process covered information are located in rooms with doors and windows that are locked when unattended. External protection is considered for windows, particularly at ground level (public, sensitive, and restricted areas), and are not located in areas that are unattended and have unrestricted access by the public.

MDI shall ensure that it has biometric / access card entry/exit point to access any of the information system. Also, only authorized personnel shall have access to area where sensitive information is located. In addition, the MIS/Compliance Team shall review the physical access log at least monthly.

The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, and considers the physical and environmental hazards in its risk mitigation strategy.

For the systems at home, the users shall ensure that they are taking adequate care by not leaving the systems in any unsecured place. They lock the room doors/windows in which they are keeping the system.

Regardless of ownership, the use of any information processing equipment outside the MDI’s premises is authorized by management.

8.2.2 Supporting Utilities

IT equipment must be protected against power failure, surges/spikes, low voltage, electrical interference, and similar disturbances, according to the risk. Utilities, such as power, chilled air/water, and so on, must be adequate to support the IT systems.

MDI shall ensure that it has a suitable electrical supply that conforms to the equipment manufacturer's specifications.

IT equipment providing or supporting critical business services must be powered from generator-backed computer-grade on-line Uninterruptible Power Supplies (UPSs), ideally with dual-routed electrical power feeds from separate substations. Tier 2 systems should be powered from Uninterruptible Power Supply (UPSs), at least.

Where it is uneconomic to provide dual-routed electricity supplies and/or standby generators to guard against extended power cuts, suitable contingency plans must be in place (see 14 Business Continuity Management). Contingency plans and procedures should cover eventualities, such as UPS failures, faults in or maintenance of electrical distribution cabling or switch panels, and so on.

MDI shall have an uninterruptable power supply (UPS) used for its equipment supporting critical business operations to support orderly shutdown or continuous running (transition to long-term alternate power). UPSs and their batteries should be regularly checked and tested in accordance with the manufacturer's recommendations to ensure they remain reliable and have sufficient capacity to meet the load requirements for the full rated period.

Backup generators should be regularly tested on-load in accordance with the manufacturer's instructions. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period.

Shrouded "Emergency Power Off" buttons should be located near emergency exits within equipment rooms to facilitate rapid power down in case of an emergency. On advice from fire safety experts, power supplies (especially to air conditioning units) should normally be interlocked with fire/smoke alarms (see also 9.1.4 Protecting against External and Environmental Threats). Emergency lighting should be provided in case of main power failure, in accordance with health and safety obligations.

Supporting utilities must be adequately monitored and alarmed in case of faults (ideally with local and remote-reading alarm panels monitored 24x7), with suitable response and incident procedures.

Hazardous or combustible materials shall not be allowed to be carried inside the MDI premises. Bulk supplies such as stationery are not stored within a secure area to avoid catching/spreading fire. Backup media shall be stored safely at Secure site identified by MDI to avoid damage from disaster affecting the main site.

Admin shall ensure that all supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning are adequate for the systems they are supporting. Admin shall inspect and test the support utilities regularly to ensure their proper functioning and to reduce any risk from their malfunction or failure.

It is the responsibility of the facility provider to have water supply arranged 24/7.

8.2.3 Cabling Security

Power and telecommunications cabling feeding IT facilities should be physically protected from interception and damage. Cables should be fed underground where possible, or else protected by armored cabling or conduit and sensibly routed to avoid high risk areas, such as corners near passing traffic.

Where possible, power cables should be physically separated from communications cables to minimize interference.

Cable inspection and termination points (including patching racks) should be protected against unauthorized access for example using locked rooms, boxes or cages.

Where possible, multiple routings and/or transmission media should be used to avoid single points of failure for critical data and voice communications.

Where possible, fiber optic cabling should be used in preference to copper or radio links for carrying data.

If unauthorized interception of data is considered a significant risk, IT facilities, cables and equipment should be swept periodically for unauthorized monitoring devices, cable taps, and so on.

MDI ensure that each cable is being labelled appropriately in order to identify and to avoid confusion.

8.2.4 Equipment Maintenance

Purpose: Equipment must be correctly maintained to ensure its continued availability and integrity. In addition, MDI do not approve any non-local system maintenance and all the maintenance shall happen on MDI premises and by MDI personnel only.

MDI shall ensure that proper maintenance takes place so that:

- if there is any incident like the power outage then there is a backup from the UPS which shall run until the generator is up and running.
- In case of fire, the protection systems shall properly work
- The A.C shall continue to work in order to provide the minimum required temperature

Standard operating procedures must be published for the installation, monitoring and maintenance of environmental support equipment, communications wiring and equipment, electrical wiring and equipment, plumbing and other utilities and services consistent with the manufacturers' specifications.

The Workplace Services at each MDINetworX location must maintain records that document repairs and modifications relating to facility security. These records must include not only maintenance of the physical components of the facility but also maintenance of software related to facility security.

Scope: MDI shall ensure that the maintenance contract for all the facility equipment's (Fire Extinguishers, Smoke detectors, AC, UPS) shall be duly renewed prior to expiry of the contract. It would be the responsibility of the Administration team for follow ups with the maintenance and the contract renewals. In case of any new contract, the Administration team shall take the Directors authorization.

MDI shall maintain a list of authorized maintenance organizations or personnel. In the absence of the SPOC who is responsible for escorting the maintenance personnel appropriate authorizations shall be checked prior to letting the personnel into the premises. In addition, the SPOC who is responsible for escorting the maintenance personnel shall have all the required accesses so that the maintenance can be carried out successfully. The SPOC who is escorting the maintenance personnel shall have technical competence to supervise the maintenance activities.

The Workplace Services must also identify all physical components that require maintenance and/or are subject to needing repair and create a schedule for maintenance for each component.

Procedures for maintenance must address the following controls:

- Equipment must be maintained in accordance with the supplier's recommended service intervals and specifications.
- Only authorized maintenance personnel should carry out repairs and service equipment. Authorized maintenance personnel shall be tracked in the "Maintenance Vendor Authorized personnel" document.
- Records must be kept of all suspected or actual faults, and all preventative and corrective maintenance.
- Appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared.
- All requirements imposed by insurance policies should be complied with.
- Appropriate control measures should be used when sending equipment off premises for maintenance (see also 8.2.5 Security of Equipment Off-Premises).
- All requirements imposed by insurance policies should be complied with.
- Maintenance performed should be tracked in the Maintenance Tracker
- Admin Team should review the tracker on Monthly basis and follow up with the vendors in case of any maintenance is due but not performed
- Maintenance of all the assets is sole responsibility of the Admin head whether performed in house or contracted.
- Maintenance and service are controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organization's maintenance program, taking into account whether this maintenance is performed by personnel on site or external to the organization.
- MDI shall obtain maintenance support and/or spare parts for defined key information system components within the applicable Recovery Time Objective (RTO) as specified in MDI's BCP plan. MDI shall have additional keyboard, mouse, monitors and hard-disks in the IT stock. In addition, MDI shall ensure to have at-least 25% laptops (% for the Operations team only) in the IT stock (at Secure site identified by MDI).

Coordination: Admin Team and IT Team shall ensure that all the respective stake holders shall be informed in advance if any maintenance activity is being carried that could impact their respective team's duties.

Compliance: Admin & IT team shall ensure that all the legal requirements, internal requirements and/or contractual requirements are satisfied while performing any maintenance activities.

Roles & Responsibilities:

IT:

- IT Team to carry out the maintenance of Desktops/Laptops/Servers frequently.

Admin:

- Keeping follow ups with the maintenance and the contract renewals
- Admin to maintain a list of authorized maintenance organizations or personnel

Sr. Management:

- Providing approval for carrying out the maintenance activity

8.2.5 Wireless Security

MDI shall use only one wireless access point in each of its location. Moreover, it shall follow the below hardening and security controls for the access point. The access point that is available is authorized by the Sr. Management.

Physical security mechanism shall be put in place to prevent the theft, alteration, or misuse of access points. The WIFI router shall be placed inside the main entrance and shall be placed in such a manner that it is always visible and captured on CCTV.

The default SSID and administrator username / password shall be changed on all access points. The access points shall be placed strategically and configured so that the SSID broadcast range does not exceed the physical perimeter of the building. Console access shall be password protected. MDI shall ensure that the encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. All the wireless devices owned by MDI shall follow the hardening procedure as listed in the "**IT022 - Infrastructure Hardening Policy**".

If any request is received to configure WIFI on any device, IT team shall accept such request only post receiving the approval from the Sr. Management. IT Team shall never configure the organizations WIFI on any users cell phone. If IT is configuring the WIFI and entering the password and saving the same, IT Team shall ensure that the Wireless properties is restricted to all the systems on which the WIFI is configured. MAC binding shall be implemented on the wireless access point.

The WIFI password shall be changed every 30 days and the WIFI password policy shall be followed as described in "10.3.4 Wireless Password Construction".

MDI shall ensure that the WAP router details are captured in the asset inventory. MDI shall ensure that it protects wireless access to systems containing sensitive information by authenticating both users by verifying domain credentials and devices with the help of Mac binding.

MDI shall ensure to change the default SNMP community strings on all its wireless devices.

8.2.6 Security of Equipment Off-Premises

Regardless of ownership, the use of any equipment outside MD NetworX premises for processing MDINetworX's information should be authorized by Sr. Management. The security provided should be equivalent to that for on-site equipment used for the same purpose, considering the risks of working outside MDINetworX's premises. Information

processing equipment includes all forms of personal computers, organizers, mobile phones, paper or other form, which is held for home working or being transported away from the normal work location.

Equipment and media taken off the premises should not be left unattended in public places. Portable computers should be carried discreetly as hand luggage when traveling.

Manufacturers' instructions for protecting equipment should be observed at all times, for example, protection against exposure to strong electromagnetic fields.

Remote working environments should be risk assessed and suitable controls applied where necessary, for example, lockable filing cabinets, physical and logical access controls for computers. The 11.3.5 Clear Desk and Clear Screen Policy applies.

Copying, move, print, and storage of sensitive data are prohibited when accessed remotely without a defined business need.

Adequate insurance cover should be in place to protect equipment off site. Security risks may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Specification of controls for the protection of off-premises equipment takes into consideration the security risks (e.g., damage, theft, eavesdropping), which may vary considerably between locations.

Equipment, information, or software is not taken off-site without prior authorization; and employees, contractors and third-party users who have authority to permit off-site removal of assets are clearly identified. Additionally, MDI permits only Team Leaders and above to carry their laptops to their residence. No other users are authorized to carry any equipment off premises.

Where necessary and appropriate, equipment is recorded as being moved off-site to another location, time limits are set for its return, and the return is recorded and checked for compliance.

MDI shall ensure that equipment is recorded as being removed off-site and recorded when returned. The Compliance team must maintain an Inward and Outward register for the recording of all the assets.

MDI shall ensure that:

(b) it protects and controls electronic media containing sensitive information during transport outside of controlled areas by encrypting the media using a password. In addition, no non-electronic media shall have sensitive information. Even if it was accidentally printed then the same shall be shredded using the shredder available with the Admin team.
(c) maintains accountability for information system media during transport outside of controlled areas
(d) documents activities associated with the transport of information system media
(e) restricts the activities associated with transport of such media to authorized personnel

8.2.7 Secure Disposal or Re-Use of Equipment

Information can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information must be physically destroyed or securely overwritten rather than using the standard delete function.

All items of equipment containing storage media (see definition of Removable Storage Media) must be checked to ensure that any sensitive data (including EPHI) and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

8.2.8 Removal of Property

IT equipment, information or software should not be taken off-site without prior management authorization.

Portable IT equipment, such as laptop PCs, mobile telephones and Personal Digital Assistants may be allocated by management to individual workers for offsite/home use, provided those workers accept personal responsibility for protecting them against harm and unauthorized access/use.

The removal of Critical Information Assets from site must be explicitly authorized by the Sr. Management for specific purposes on each occasion that is, Critical Information Assets must be logged out to trustworthy carriers and logged back in when returned.

Third parties authorized to remove information assets from site (such as couriers and secure data disposal contractors) should be authenticated by workers (for example, by checking their credentials, such as photo IDs) before the assets are released to their care.

Spot checks should be undertaken by management and/or Site Security to detect unauthorized removal of property or information. Workers and visitors should be notified that such checks take place, for example through warning notices and procedures.

8.2.9 Account Lockout Policy

Passwords are an important step in a security plan for our network. Users may see passwords as a nuisance; however, the security of our enterprise relies on a combination of password length, password uniqueness, and password lifespan. These three items help defend against dictionary attacks and brute force attacks.

A dictionary attack occurs when a malicious user tries known words that are in the dictionary and a number of common password names to try and guess a password.

A brute force attack occurs when a malicious user tries all of the possible permutations until one is successful.

Because most users prefer passwords that they can easily remember, dictionary attacks are often an effective method for a malicious user to find a password in significantly less time than they would with brute force attacks. Therefore, the strength of a password depends on how many characters are in the password, how well the password is protected from being revealed by the owner, how well the password is protected if it is intercepted by a malicious

user on the network, and how difficult the password is to guess. Even good passwords that are protected by cryptography on the network and that are not subject to dictionary attacks can be discovered by brute force in a few weeks or months by a malicious user who intercepts the password on the network.

Currently, several attack methods are based on guessing weak passwords by using dictionary and brute force attacks.

To help prevent the attacks from being successful, we have configured account lockout settings.

The result of this configuration is that the associated account is temporarily disabled after a specified number of incorrect passwords are tried.

This helps to prevent a successful attack by preventing the account from being used. However, a legitimate user cannot use that account until it is unlocked.

MDI's account lockout policy settings:

Account lockout threshold	**Lockout duration**	**Reset account lockout duration**
3 invalid logons attempts	30 minutes	30 minutes

In case of account locked it would be unlocked by consulting with IT department.

9. Communications and Operations Management

9.1 Operational Procedures and Responsibilities

9.1.1 Documented Operating Procedures

All operating procedures having significant information security implications must be formally documented and maintained, with all changes explicitly authorized by management.

The procedures should cover:

- Computer startup and shutdown, including restart and recovery procedures for use in the event of system failure
- Backups and media handling (see 9.5.1 Information Backup)
- Processing and handling of information
- Batch scheduling requirements, including interdependencies with other batches and systems, earliest job start and latest job completion times
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 10.5.4. Use of System Utilities)
- Support contacts in the event of unexpected operational or technical difficulties
- Special output handling instructions including the use of special stationery (such as checks and PIN mailers) and the management of confidential output, plus procedures for secure disposal of output from failed jobs (see 9.7.2 Disposal of Media and 9.7.3 Information Handling Procedures)
- Management of system, security and audit logs (see 9.10 Monitoring)
- Equipment maintenance
- Computer room management

Where feasible, systems should be managed consistently using similar procedures, tools and utilities.

9.1.2 Change Management

Changes to information processing facilities, equipment, systems, applications, and procedures must be controlled and archived through formal management responsibilities and procedures in proportion to the risks involved.

Promotion of new systems or significant changes from development into production is a high-risk activity, particularly where existing production systems and services may be impacted, and especially so if those systems and services are supporting business critical business processes. Such significant changes must be strictly controlled (see 11.5.1 Change Control Procedures). This implies that all proposed changes should be consistently risk assessed to determine their significance, and the associated management decisions and approvals must be recorded.

Significant changes must be identified and recorded in a manual tracker maintained by the IT team for IT-related changes. Application-related changes should be documented within the MDI Ticketing tool. Additionally, the Service Desk is responsible for handling all IT-related changes, while Application-related changes are managed within the DocGem CMS. Procedures relating to the implementation of significant changes must also be suitably planned and

documented, along with fallback procedures for verifying/aborting and recovering from unsuccessful changes (for example, restoration of immediate pre-change backups).

Changes must be tested prior to implementation, reflecting a rational assessment of the potential impacts including any security implications (see 11.1.1 Security Requirements Analysis and Specification).

Change details must be communicated to the relevant people in IT/SIT and in the business and the manual change tracker are placed within shared folder.

Change Management Procedure:

Any change related to information systems shall be requested using MDI's ticketing tool for SIT (Change Management DocGem tool for SIT changes) & IT related changes, are submitted via email, and a manual tracker is maintained for review. For all other changes, the respective managers would be taking approval from Sr. Management on. Once the ticket is raised, approval shall be taken from Sr. Management and the Compliance Lead / ISO. Once the approval is received, IT / SIT shall test the implementation prior to release on production. If the testing is successful, then the same shall be released to production and the ticket shall be closed. In addition, before releasing the change to production, the rollback/fallback procedure shall be documented on the same ticket and the same procedure shall be followed in case if the change has any issue / error post releasing it on the production. MDI shall ensure that the testing is performed on some randomly chosen systems and not on all the systems that are in production. All the changes that are being performed on those systems are detailed in the change ticket. Only after success (no issues observed) in testing, the change shall be released on all other systems. An audit log is maintained of all updates/changes to operational program libraries.

MDI ensures that it uses its configuration control program to maintain control of all implemented software and its system documentation, and archives prior versions of implemented software and associated system documentation. MDI keeps all its software changes in its centralized tool and whenever required, any version of the software can be implemented / rolled back. MDI shall also monitor changes that could affect its internal controls and compliance obligations. Previous versions of application software are retained as a contingency measure. Old versions of software are archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive.

Standard Fallback/Rollback Procedure:

The fallback plan should allow the system to be rolled back in a controlled manner that provides the least disruption possible.

There are two different fallback conditions that MDI shall consider: fallback during the deployment, and fallback after the deployment. During the deployment, we may have to fall back if some environmental or external event occurs. For example, if the client is working (considering both internal/external clients) on the day the deployment is planned, then the deployment may rob our critical time and thus MDI may decide to back out and restart the deployment at a later date.

A fallback after deployment occurs if various tests have missed some critical aspect, and the new system does not perform or behave as the old system did. A post-deployment fallback plan will need to include methods for taking whatever operational updates have occurred to the database back to the older system/application.

9.1.3 Segregation of Duties

Care must be taken to prevent the perpetration of fraud by individuals with excessive access rights. Duties and areas of responsibility must be segregated between individuals to reduce opportunities for unauthorized or unintentional modification or misuse of MDINetworX's information assets.

Systems and processes must require the involvement of at least two people for important transactions, normally by separating the initiation and authorization steps between individuals.

Separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems. Further if segregation of duties is not possible, monitoring of activities, audit trails, management is used to limit the risk of unauthorized or unintentional modification of information assets.

If there is a danger of the primary controls being bypassed (for example, through collusion), additional controls must be designed and implemented, for example, secure logs/records of transactions regularly reviewed, and alarms/alerts on significant security events. Staff performing checks, such as security audits and system acceptance tests, must be independent of the management and operation of the systems and processes being reviewed.

To establish secure and compliant access provisioning framework/procedure, access authorization such as access requests, approvals, and provisioning is segregated among multiple individuals or groups to ensure segregation of duties.

9.1.4 Separation of Development, Test, and Operational Facilities

Pre-production environments (including the systems, networks, and data associated with specification, design, development and testing of computer software) must be fully isolated from production environments to minimize the risk of production incidents, using physically different systems, processors, domains, directories, and networks ("air gaps") or, where physical isolation is not feasible, strong logical controls, such as encryption.

Development and test environments must also be at least logically isolated from each other to ensure their respective integrity. The promotion of new or modified software into production must be controlled through the formal Change Control Process.

MDI shall ensure that it minimizes any testing on production systems. When testing must be performed, a test plan is developed that document all changes to the system and the procedures for undoing any changes made to the system

Test systems should emulate production as closely as possible except that:

- Testers and developers should not have user IDs on production systems (excluding fire-call user IDs which are only enabled for use by authorized IT support workers for specific support purposes through the emergency changes process within the Change Control Process).

- Production data should only be available on production systems. Development and testing should use dummy data wherever possible. If production data must be used, fields containing highly sensitive data (such as credit card numbers and personal data) must first be obfuscated (see also 11.4.2 Protection of System Test Data).
- On-screen messages, screen colors, and so on, should clearly indicate whether a system is in test or production to minimize the risk of someone accidentally submitting test transactions on production systems.

Compilers, editors, and similar powerful system utilities must not be installed on production systems unless absolutely necessary, and then may only be used by authorized users for legitimate purposes under authority of an approved change control record.

MDI shall ensure that level of separation between operational, test, and development environments is identified and controls are implemented to prevent operational issues that includes:

(i) along with removing accounts, a review of all custom code preceding the release to production or to customers must be completed in order to identify any possible coding vulnerability, to include at least the following:
   1. code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices
   2. code reviews ensure code is developed according to secure coding guidelines
   3. appropriate corrections are implemented prior to release
   4. code-review results are reviewed and approved by management prior to release

(ii) test data and accounts is removed completely before the application is placed into a production state

(iii) organizations remove all custom application accounts, user IDs, and passwords before applications go from development to production or are released to customers

(iv) rules for the transfer of software from development to operational status are defined and documented

(v) development and operational software run on different systems or computer processors and in different domains or directories

(vi) compilers, editors, and other development tools or system utilities are not accessible from operational systems when not required

(vii) the test system environment emulates the operational system environment as closely as possible

(viii) users use different user profiles for operational and test systems, and menus display appropriate identification messages to reduce the risk of error

(ix) covered information is not copied into the test system environment

(x) MDI ensures that it performs standard security code review prior to moving code to production

9.2 Third Party Service Delivery Management

9.2.1 Service Delivery

Supplier contracts with third parties for IT-related services must define requirements for information security controls, services, and service levels, including resilience and IT Disaster Recovery requirements.

MDINetworX must be confident that third parties are capable of satisfying requirements prior to entering into such contracts, and that they have the capability and intent to maintain adequate service levels. This is particularly important

where third party services play a significant part in meeting MDINetworX's contractual, legal, or ethical obligations (for example, processing sensitive client data) since MDINetworX remains ultimately accountable.

Supplier contracts should incorporate a 'right of audit' giving MDINetworX the ability to inspect and assess third parties' internal processes relating to the contract, including aspects, such as documented security policies and procedures, change controls, audit trails, and processes for identifying, managing, resolving, and reporting security incidents.

MDI shall ensure that all remote access connections between MDI and all external parties are secured via encrypted channels by using SonicWALL secured VPN. Any covered information shared with an external party is encrypted prior to transmission. However, MDI doesn't have any Third Party from/to whom MDI is exchanging any covered information.

MDI shall ensure that external parties are granted minimum necessary access to the organization's information assets to minimize risks to security. All access granted to external parties is limited in duration and revoked when no longer needed.

MDI identifies and mandates information security controls to specifically address supplier access to the organizations information and information assets.

MDI restricts the location of facilities processing, transmitting, or storing covered information based on its legal, regulatory, contractual, and other security and privacy-related obligations.

MDI monitors security control compliance by external service providers on an ongoing basis. Monitoring involves a service management relationship and process between the organization and the third-party. The organization monitors the network service features and service levels to detect abnormalities and violations.

9.2.2 Monitoring and Review of Third-Party Services

Service Level Agreements (SLAs) with an agreed service arrangement shall address liability, service definitions (e.g., reliability, availability and response times for the provision of services), security controls, and other aspects of services management (e.g., monitoring, auditing, impacts to the organization's resilience, and change management).

Services delivered by third parties must be monitored to ensure they are delivered and maintained by the third parties in accordance with the contracts on an annual basis. More than simply accepting their service level reports, and so on, at face value, actual services provided should be proactively reviewed and any service incidents discussed with them in relation to their contractual obligations. Third-party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to service delivery shall be reviewed. Information about information security incidents are provided to the CIMT. This information is reviewed by the third party that experienced the incident and the organization which the third party provides services to as required by the agreements and any supporting guidelines and procedures. Any identified problems are resolved and reviewed by the organization as noted above.

Responsibilities for managing supplier contracts and relationships must be assigned to specific roles or teams.

Relationship management meetings should take place regularly (monthly for significant relationships, quarterly or six monthly for others) and minutes must be formally documented.

Consideration should be given to auditing third parties. The frequency, scope, and depth of audit should reflect the associated risks to MDINetworX. Audit findings and recommendations should be discussed with the auditors and third parties, and action plans, timescales and ownership should be formally agreed and tracked through to completion.

MDI shall ensure that the review of service-level agreements (SLAs) is conducted at least annually and compared against the monitoring records.

MDI shall ensure that reports produced by the third-parties are reviewed and annual progress meetings are arranged as required by the agreements. Information about information security incidents are provided to the incident response team. This information is reviewed by the third-party that experienced the incident and the organization which the third-party provides services to as required by the agreements and any supporting guidelines and procedures. Any identified problems are resolved and reviewed by the organization as noted above.

MDI shall periodically audit the network services to ensure that network service providers implement the required security features and meet the requirements agreed with management, including new and existing regulations.

9.2.3 Managing Changes to Third Party Services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved.

Risks should be reviewed where changes have been significant, such as those involving networks; use of new technologies, products, versions, development tools or environments; changes to physical location of service facilities, and changes of suppliers.

9.3 System Planning and Acceptance

9.3.1 Capacity Management

Capacity demands and trends must be monitored and future capacity requirements projected to ensure that adequate processing power, memory, disk storage capacity, peripheral devices, and communications systems are available to avoid overloads and failures. The analysis must take account of planned changes in business and system requirements, and trends in our IT needs.

IT managers must use capacity information to identify potential bottlenecks that might present a threat to system security or user services, and take appropriate preventive/remedial action in good time to avoid production impacts.

MDI's capacity requirements take into account current, projected and anticipated, capacity needs for all systems used to provide services to the customer.

9.3.2 System Acceptance

The operational requirements of new systems must be established, documented, and tested prior to their acceptance and use.

Suitable acceptance tests must be performed on “new” information systems (including version upgrades as well as completely new systems) prior to production use. Managers must ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested, taking into consideration:

- Performance and computer capacity requirements
- Error recovery and restart procedures, and contingency plans
- Preparation and testing of routine operating procedures to defined standards
- Agreed set of security controls in place
- Effective manual procedures
- Updated business continuity arrangements (see 13 Business Continuity Management)
- Evidence that installation of the new system must not adversely affect existing IT systems or the infrastructure, particularly at peak processing times
- Evidence that due consideration has been given to the effect the new system has on MDINetworX’s overall information security risk profile
- Training in the operation or use of new systems. For major new developments, IT operations and users must be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design.

The IT Manager is responsible for the quality and security of production IT services as a whole and therefore has the authority to reject new systems that he/she considers will adversely impact the IT infrastructure and other services. Development project managers must not assume that their systems will automatically go into production, no matter how important the systems.

9.4 Protection against Malicious and Mobile Code

9.4.1 Controls against Malicious Code

Appropriate technical and procedural controls (including “antivirus” software, limited system access rights, security awareness, and change management controls) must be in place to minimize the risks relating to malicious and other undesirable software, such as viruses, worms, Trojan horse programs, logic bombs, spam, adware and spyware. The IT Manager is responsible for defining the technical architecture to protect MDINetworX against malware risks subject to practical constraints and cost-effectiveness.

Approved antivirus software must be installed on all applicable IT platforms. The software must be configured for optimum protection and updated promptly when new malware signatures, and so on, are released. Only IT personnel have access to alter or interfere with the antivirus software, its configuration, the update process or its operation.

E-mail messages and attachments must be routinely and automatically checked for malicious software before use. Antivirus controls should be implemented in multiple layers, for example, e-mail gateways, servers, and desktop/portable computers.

Unauthorized software must not be installed on MDINetworX systems. IT Department reviews and approves software, and installation of approved software normally requires explicit authorization by a worker’s manager. This requirement includes all forms of software programs, such as commercial software, operating system software, utilities, shareware and freeware, and evaluation software.

MDI identifies unauthorized software on the information system, including servers, workstations and laptops, employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized software on the information system, and reviews and updates the list of unauthorized software at least once in each year. The organization maintains an up-to-date list of authorized software that is required in the enterprise for any business purpose on any business system

The software and data content of critical information systems must be regularly reviewed by competent and trustworthy persons authorized by the corresponding IAOs, and checked against documented and approved changes. Anomalies, such as the presence of any unapproved files or unauthorized amendments should be notified to the Managers and formally investigated by Information Security or Internal Audit.

Suitable incident reporting, management, and contingency measures must be in place to minimize the impact of, and recover efficiently from, any malware infections.

The Managers are responsible for keeping abreast of and evaluating the malicious software threat using reliable resources, such as trusted websites and professional journals, and disseminating useful information and guidance throughout MDINetworX.

Workers must comply fully with software licenses and must neither install nor use unauthorized or unlicensed software (see also 14.1.2 Intellectual Property Rights).

Automated controls (e.g., browser settings) are in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations). This is achieved by enabling/disabling the settings for individual mobile code components in the Internet explorer browser settings at domain level.

MDI has restricted both the selection and use of mobile code installed on servers and mobile code downloaded and executed on any individual workstations and devices.

MDI has restricted the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

we are fully committed to the protection of our information assets and data against the pervasive threat of phishing attacks. Our comprehensive approach to phishing attack prevention and detection includes multiple measures:

We employ Kaspersky O365 Email Security, a robust email security solution that provides multilayered protection against phishing attacks. This solution includes real-time scanning of emails, attachments, and links to identify malicious content. Additionally, advanced heuristics and machine learning algorithms are utilized to detect and block suspicious emails before they reach our end-users.

To further fortify our defenses, we maintain a strict email policy. This policy ensures that only authorized personnel who have undergone thorough vetting and training have the privilege to send emails to allowed domains, reducing the likelihood of unauthorized personnel attempting to send phishing emails from within the organization.

Email authentication protocols, including SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance), have been implemented. These protocols play a vital role in verifying the authenticity of incoming emails, ensuring that emails are sent from legitimate sources and haven't been tampered with in transit.

As a proactive measure, we conduct user awareness training for all employees. This training equips them with the knowledge to identify various forms of phishing attacks and how to recognize them. Additionally, the training includes simulated phishing exercises to assess employees' ability to spot phishing emails.

We stay informed about emerging phishing threats through automated threat intelligence feeds, which provide real-time information about the latest attack techniques and patterns. This awareness allows us to adapt our defenses promptly.

A well-defined phishing incident response plan is in place, specifying procedures for identifying and reporting potential phishing attacks, containing the threat, and mitigating its impact. Rapid response is of utmost importance in minimizing the damage caused by phishing attacks.

To enhance our defenses, we deploy advanced endpoint protection solutions capable of detecting and blocking phishing attempts at the user's device. These solutions often integrate artificial intelligence and machine learning to identify malicious behavior.

In our effort to safeguard against phishing attacks, we employ URL filtering tools to inspect web links in emails, blocking access to known malicious websites. This proactive measure prevents users from inadvertently visiting phishing sites.

Finally, for the secure sharing of sensitive and confidential information via email, we utilize email encryption solutions. This ensures that only authorized recipients can access the content, further fortifying our defenses against phishing threats.

9.5 Backup

9.5.1 Information Backup

Offline backup copies of essential business information and software, including EPHI, must be taken regularly. Backups must be sufficient to enable essential business information and software to be recovered efficiently following a disaster or media failure affecting the primary data or systems.

Backup schedules must be specifically designed and documented for each system in order to meet legitimate business, legal or regulatory requirements for retention and restoration of data as defined by the Compliance Manager on the basis of risk assessment:

- Suitable types of backups must be taken (for example, full ‘image copy’ weekly backups plus either incremental or differential daily backups)
- Sufficient generations or cycles of backups must be retained to satisfy the minimum backup retention periods (see 14.1.3 Protection of Organizational Records)
- Backups are unlikely to satisfy the requirements for long-term archival of data.

Backup processes should be automated where possible.

MDI uses a backup tool to take the backup of the covered information. All the backups are stored on the NAS device for the tools. Further, the schedule is detailed in “IT004-Backup Policy”.

Backup equipment and processes and information system that are transaction based must be suitably tested prior to implementation. Backup equipment, media, processes, and information system that are transaction based must be regularly tested in production to ensure that they can be relied upon for emergency use when necessary. Testing must include periodic trial restores of data from backups to test systems, avoiding any possibility of overwriting live data in case the backups prove inadequate. Testing must also confirm that backups can be retrieved and restored within agreed service levels for IT data/service recovery.

Both the backups shall have accurate and complete records and must be stored in a remote location chosen to minimize the chances of being affected by a physical disaster affecting the main location (for example, a major fire, earthquake, flood, chemical spill, lightning storm, and so on). This requirement is distinct from and in addition to any local/on-site copies kept in fire safes for rapid restoration of systems or data following less dramatic incidents.

While taking the backups, care shall be taken to segregate different department backups in different folders.

Both the backups shall have accurate and complete records and must be stored in a remote location chosen to minimize the chances of being affected by a physical disaster affecting the main location (for example, a major fire, earthquake, flood, chemical spill, lightning storm, and so on). This requirement is distinct from and in addition to any local/on-site copies kept in fire safes for rapid restoration of systems or data following less dramatic incidents.

Important records, such as contracts, personnel records, financial information, patient records, etc., shall be safeguarded by placing them in a locked cabinet and access to the keys would be restricted with the owner of the records.

MDI shall ensure that Secure site identified by MDI is having reasonable physical and environmental controls so as to protect the backup hard-disks.

The portability and amount of data stored in backups makes them inherently more vulnerable to theft, loss or damage than the primary storage media. Backups must therefore be physically and logically protected to at least the same degree as the original data (see 8 Physical and Environmental Security):

- Backup and archive data must be protected according to the classification level (see 6.2 Information Classification).
- Physical security measures must provide equivalent physical protection at the main site and backup sites against unauthorized access, fire or other physical damage, theft, and so on, (see 9.7.1 Management of Removable Media)
- Backups and archives should be encrypted by default where technically feasible. Where the original data are classified MDI NetworX Restricted or MDI NetworX Secret and are encrypted, the corresponding backups must be similarly encrypted.

Media containing backup and archive data must be stored at a physically separate secure storage facility sufficiently far away from the primary data storage as to be extremely unlikely to experience the same physical incident or disaster. Transportation of media to and from remote storage facilities must be:

- Authorized by management
- Recorded in a secure log or database such that the location of all media can be determined reliably at any point
- Performed by trustworthy people (preferably MDI NetworX associates, otherwise media transportation and storage specialists approved by the Security Committee and bound by contracts specifying suitable security arrangements, responsibilities and liabilities)

In addition, HIPAA specifically requires that if EPHI resides on equipment that is to be moved, a retrievable, exact copy of the EPHI must be made before the move and the same is implemented in MDI as well.

MDI shall ensure that a tracker is maintained to track the inventories of the backup with at least the following details:

- Type of Backup
- Backup Schedule Date/Time
- Backup Status
- Backup Rescheduled (if failed)
- Source Location
- Destination Location

The retention period for essential business information, and also any requirement for archive copies to be permanently retained, must be consistent with MDINetworX policies on records management and records retention.

9.6 Network Security Management

9.6.1 Network Controls

Network and computer management activities must be coordinated to minimize risks to the business and ensure that information security controls are applied consistently across the entire IT infrastructure without unduly compromising service to the business.

Responsibilities and procedures must be established for the secure management of local and remote IT equipment, including computers and networking equipment in user areas. Below are the procedures that is being followed in MDI:

- All the equipment containing, processing or transmitting PHI shall be located in secured area (Operations, Quality and Server room) that is being monitored continuously using CCTV. Further, access to these are only permitted to authorized users only.
- Users are briefed about the security of the assets while they are working remotely and all the precautions the user need to take.

IT Team holds sole responsibility for managing any/all the network equipment. Operational responsibility for networks shall be separated from computer operations.

Special controls are established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications. Special controls may also be required to maintain the availability of the network services and computers connected. MDI shall ensure that time-stamp for logon-logoff activity and other activities shall be captured for all network activities. In addition, MDI shall enable the replay-resistant feature of the firewall.

MDI has trained users on not to work from Public networks like coffee shops or eateries. They are only authorized to work from their residence.

MDI shall ensure that their information systems protect the confidentiality and integrity of transmitted information, including during preparation for transmission and during reception.

MDI formally manages equipment on the network, including equipment in user areas. It will be the responsibility of the IT team to manage all the equipment on the network.

MDI's public facing web-based application DocGem is assessed for vulnerability at least once in each year or if there are any major changes to the application. SIT is responsible for resolving all critical vulnerabilities.

MDI shall ensure that it performs automated vulnerability testing with an emphasis on input validation controls once in each year for its public facing web-based application DocGem/Insight Pro since it stores, processes and transmits covered information. MDI shall ensure that the application's hosted has a firewall which continually checks all the traffic.

Information security controls must safeguard the confidentiality and integrity of data passing over third-party networks and protect the integrity of MDINetworX networks and computer systems against internal and external threats, including the following:

- Networks must be designed with the concepts of 'defense in depth' (multi-layer controls) and 'failsafe operation' (for example, 'default deny') in mind
- Cryptographic controls must ensure confidentiality, integrity, and non- repudiation of messages containing sensitive or critical business transaction data (see 10.4 Network Access Control and 12.3 Cryptographic Controls)
- The network perimeter and, where relevant, discrete internal domains must use firewalls to monitor and control access and use of the networks and attached systems
- Networks must be designed and managed to deliver a level of availability, capacity and performance equivalent to the connected computer systems and sufficient to meet legitimate business requirements. Arrangements must also be prepared to enable the recovery of essential network services in accordance with legitimate business requirements in the event of a contingency situation.
- Gateways, firewalls, and servers must monitor network traffic, log security- relevant information and raise alerts for significant events.
- The IDS shall be integrated with the Firewall and the network administrator shall monitor the activity on real-time basis. If any suspicious activity is noted during the monitoring then action shall be taken by IT Team immediately without waiting for any approval.

- On a weekly basis, an automated firewall report is generated and is published to the Compliance team. The Compliance team reviews the report for any unauthorized attack/traffic and if any deviation/suspicious activity is observed the same shall be highlighted to the Compliance Manager and IT Team for action.
- Teleworking activities are formally managed/controlled and only authorized if suitable security arrangements and security controls that comply with relevant security policies and organizational requirements are in place
- The communications security requirements are addressed and take into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system
- MDI shall communicate with each user that the wireless network they connect shall have a minimum of AES WPA2 encryption enabled.
- MDI shall communicate the users regarding the return of assets once the regular office is being started.
- MDI shall ensure that each user logins with their own domain credentials
- MDI shall ensure that cryptography is used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems. MDI's remote working user connects to MDI's network either by using SonicWall VPN or using terminal server. Both of the connections are secured and encrypted.
- MDI shall ensure that the users connect to MDI's network either by using secured VPN or using Terminal Server.
- MDI shall define the ownership of the assets provided for each user in its Asset Inventory.

9.6.2 Security of Network Services

Security features, service levels, and management requirements of all network services (such as the provision of connections, private network services, and value-added networks, and managed network security solutions, such as firewalls and intrusion detection systems, whether provided in house or outsourced) should be identified and included in Network Services Agreements.

MDI provides both dedicated database or dedicated instance of databases to each of its customer. Its customer's decision to choose the right kind of database.

The security arrangements necessary for particular services (including technical and procedural security controls, service levels and management requirements) should be identified in the agreement. The ability of network service providers to secure the network services should be determined before entering into the agreement and regularly monitored thereafter. A 'right of audit' should therefore be included in the agreement.

SonicWall Firewall shall be used between the internal network, external networks (Internet and third-party networks). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two (2) interconnected networks to control access and information flow between the two (2) domains. This gateway shall be capable of enforcing security policies, shall be configured to filter traffic between these domains, and block unauthorized access in accordance with the organization's access control policy.

Wireless networks are segregated from internal and private networks. MDI has a separate VLAN configured for wireless network and other internal networks. All the traffic passing through the wireless network shall be passed through the firewall. Further, in US office VLAN segregation is not available as there is only one process of scanning the physical images and uploading the same on the SFTP.

Network traffic shall be denied by default and allowed by exception (i.e., deny all, permit by exception). MDI shall restrict the ability of users to connect to the internal network in accordance with the access control policy and if required for business application.

MDI shall ensure that routing controls are implemented through firewalls used between internal and external networks. In addition, the IT Team reviews all the firewall rules at least once in each year.

MDI owns two applications, DocGem (PMS) & Golem and has already identified the sensitivity as high as both the applications are processing PHI/PII. In addition, all the systems servers handling PHI will be treated as high sensitivity. The systems and servers containing or processing PHI can be identified using the information asset log.

MDI shall document and review every six months the network diagram that shall at least consist of the below:

- high-risk environments
- data flows
- connections to systems storing, processing or transmitting covered information (VLAN1, VLAN3 & VLAN4), including any wireless networks that may have legal compliance impacts

MDI shall ensure that the network diagram is updated based on changes to the network, or is updated no less than every six months.

MDI shall monitor for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAP) unless explicitly authorized by the ISO and Sr. Management on an email.

MDI shall address new threats and vulnerabilities on an ongoing basis and ensure that DocGem/Insight Pro (which is the only web-based public facing application) is protected against known attacks by performing penetration testing and vulnerability assessment with the help of Valency Networks at least once in a year. Any vulnerabilities or threats identified as part of the assessment performed by the team are tracked to closure and mitigated to ensure security.

MDI shall segregate the networks into separate logical network domains (VLANs) each protected by a defined security perimeter. IP address of the equipment is used to indicate whether the equipment is permitted to connect to the VLAN network and to which VLAN network the equipment is permitted to connect. MDI has different VLANs created for different departments due to the difference in the work and sensitivity of the work.

MDI shall ensure that separate domains are implanted by controlling the network data flows using routing/switching capabilities, including access control lists.

The domains are defined based on risk assessment and the different security requirements within each of the domains. A graduated set of controls is applied to segregate the network security environment.

To ensure proper separation, the organization verifies any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, moves it to an internal VLAN and gives it a private address. The criteria for segregation of networks into domains is based on the access control policy and access requirements,

and also takes account of the relative cost and performance impact of incorporating suitable network routing or gateway technology. In addition, segregation of networks is based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

Networks shall be segregated from production-level networks when migrating physical servers, applications or data to virtualized servers. While migrating the physical server, MDI ensures that the network is disconnected and the data from the previous server is copied to the new server and then the new server is activated.

The organization only authorizes connections of mobile devices meeting organizational usage restrictions, configuration requirements, connection requirements, and implementation guidance. Also enforce requirements for the connection of mobile devices to sensitive information systems

MDI has also restricted it users from storing any data related to its customer on any of the mobile device including laptop or mobile.

MDI has blocked the external remote storage so that none of the users can store and access the data outside network.

9.7 Media Handling

9.7.1 Management of Removable Media

Procedures must be implemented to ensure that removable storage media used to store sensitive MDINetworX information (including EPHI) are appropriately secure during handling, storage, and destruction. Procedures must consider the following guidelines:

- If no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable.
- Where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail.

MDINetworX shall ensure the below for management of removable media and laptops -

- Security shall be maintained on restrictions and usages of media by implementing access controls, password policy, endpoint security software, data loss prevention mechanism, encryption etc.
- Media and laptops will be registered by enforcing MDI hardening guidelines. Further inventories shall be updated as and when required.
- All laptops or external storage devices shall be properly encrypted
- Physical security to removable media shall be restricted only to IT team

9.7.2 Disposal of Media

The secure sanitation of computing devices that contain storage media must occur prior to disposal or reuse. This must be facilitated in a manner that ensures information and software cannot be restored or re-constructed from storage media or system memory.

There are three acceptable methods to be used for the sanitization of hard drives:

- Overwriting with a predetermined pattern of meaningless information (using a software product or application)
- Erasing magnetic media by degaussing (hard drives seldom can be used after degaussing)
- Physical Destruction (pounding with a sledge hammer, incineration, drilling, and so on)

The method used for sanitization, depends upon the operability of the hard drive:

- Operable hard drives that will be reused must be overwritten prior to disposition.
- If the hard drive is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing MDINetworX owned or leased hard disk storage media.

Surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required.

The following paragraphs pertain to the use of hard drives, storage systems, removable storage media, printed materials and all other forms of storage devices. This policy includes, but is not limited to, the below sub-policies and procedures.

MDI shall ensure that the risk of information leakage to unauthorized persons during secure media disposal is minimized by limiting the disposal activity to Admin personnel and to shredding vendor (for papers only in USA).

Requirements from Third-party companies to whom the disposal activity is outsourced:

- MDI shall ensure that it collect the NAID certificate from the third party to whom the paper shredding activity will be outsourced.
- MDI shall ensure that a shredder is placed in MDI India office so as to shred the papers when no longer required
- MDI shall use internal team to shred the electronic data and this activity is not being outsourced

MDI outsources shredding of physical papers from its mailroom from a well-known shredding vendor Shred Instead which is NAID certified.

MDI shall ensure that:

- the use of generally accepted, secure disposal or erasure methods for use by another application within the organization, for all its media
- all the data that is received from the client shall be considered as covered information.

Destroying or Disposing

- Prior to destroying or disposing of any storage device or removable storage media, care must be taken to ensure that the device or media does not contain EPHI.
- If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to disposal.
- If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data.

Media used for System Backups and Disaster Recovery

- If using removable storage media for the purpose of system backups and disaster recovery and the aforementioned removable storage media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.
- When using storage devices and removable storage media to transport EPHI a procedure must be implemented to track and maintain records of the movement of those devices and media and the parties responsible for the device and media during its movement.

9.7.3 Information Handling Procedures

Procedures for handling and storing classified information must be established in order to protect such information from unauthorized disclosure or misuse, in accordance with the information classification (see 6.2 Information Classification).

Information must be classified and labeled according to risk using MDINetworX's information classification process. MDINetworX Restricted and MDINetworX Secret information must be protected by suitable security measures including encryption, system/file access controls, physical protection, and so on.

Information handling procedures apply to all forms of information, such as computer data, documents, computer systems, networks, mobile computing and communications, electronic mail and postal services, voice mail and voice communications, multimedia, facsimile machines, and items, such as MDINetworX checks and invoices.

In accordance with the MDINetworX information classification process (see 6.2 Information Classification), information handling procedures must include the following:

- Media handling and classification labeling
- Physical, logical and/or procedural controls to prevent access by unauthorized personnel, including appropriate protection of spooled data awaiting output and hardcopy output awaiting collection, and other protection requirements for classified data
- Maintenance of a formal record of the authorized recipients of MDINetworX Secret data, clear marking of all copies of data for the attention of the authorized recipient, and regular review of distribution lists, and so on
- Validation and other controls to achieve and maintain data and systems integrity
- Storage of media in accordance with manufacturers' specifications

- Minimizing the distribution of sensitive data, especially to third parties

9.7.4 Security of System Documentation

Documentation describing system, network, and application designs, security parameters, operating and management processes, data structures, user authorization processes, and so on, must be classified according to the MDINetworX information classification guidelines (see 6.2 Information Classification).

Such documentation must be stored and communicated securely in accordance with its classification, reflecting the risk of unauthorized disclosure or modification (for example, encrypted if sent over public networks).

9.8 Exchange of Information

9.8.1 Information Exchange Policies and Procedures

This Information Security Policy Manual in general, and the following security policies specifically, apply to all forms of communications and information exchange including voice conversations in person or by telephone, video and e-mail communications, Instant Messaging, and so on.

Exchanged information must be suitably protected from interception, copying, modification, misrouting, and destruction according to the classification level and risk of compromise.

Based upon standards from the Sr. Management, suitable security controls (such as egress filtering on firewalls) must be implemented to minimize the risk of transmission of malicious code (see 9.4.1 Controls against Malicious Code).

Electronic communication facilities must be used in accordance with applicable guidelines and acceptable use policies (see 6.1.3 Acceptable Use of Assets).

Workers must not compromise or disadvantage MDINetworX or bypass other controls through particular types of communication, for example by e-mail defamation, harassment, impersonation, forwarding of chain letters, making unauthorized purchases or contractual agreements, and so on.

Suitable cryptographic techniques must be used to protect the confidentiality, integrity, and authenticity of information in accordance with the information classification policies (see 11.3 Cryptographic Controls).

Workers must comply with retention and disposal requirements for all business correspondence, including e-mail messages, in accordance with relevant policies, laws and regulations.

Workers should avoid supplying their own personal data, such as e-mail addresses to third parties unless there is a legitimate need to do so, and the third parties are deemed trustworthy. Extra care must be taken when providing personal data belonging to clients, other workers, and so on. Workers must comply with legal and regulatory requirements to protect personal privacy and secure personal data.

Indeed, information exchange facilities and procedures must comply with all relevant legal requirements (see 14 Compliance).

9.8.2 Exchange Agreements

The exchange of information and software between MDINetworX and other organizations must be governed by agreements reflecting the sensitivity and value of the information involved and defining necessary controls, such as the following:

- Confidentiality and liability clauses in contractual agreements to limit any impacts on MDINetworX caused by security failures at third parties
- Management responsibilities and procedures including the maintenance of formal records showing the location of all media at any point, separate communications between senders and receivers to confirm dispatch and receipt, and so on
- Standards for media packaging and transportation (see 9.8.3 Physical Media in Transit)
- Positive identification of authorized couriers (for example, by photographic identity cards) and receipting of media handed to couriers
- Responsibilities to protect media from loss or damage, including explicit accountability and liabilities when media are entrusted to couriers, and so on
- Labeling and protection of information according to its information security classification, including any special controls that may be required to protect MDINetworX Secret information, such as encryption and digital signatures (see also 6.2 Information Classification)
- Information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations
- Technical standards for recording and reading information and software
- Physical, logical and/or procedural security controls to protect extremely sensitive MDINetworX Secret items, such as cryptographic keys

9.8.3 Physical Media in Transit

Computer media must be transported securely between MDINetworX sites or to off-site locations, that is:

- Reliable transport or couriers must be used. A list of authorized couriers must be agreed with management and a procedure to check the identification of couriers implemented.
- Media packaging must be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications (for example, purpose-made lockable tape carriers).
- Special controls must be adopted, where necessary, to protect media containing MDINetworX Secret and other especially sensitive or critical information from unauthorized disclosure or modification (for example, through the use of encryption, locked containers, delivery by hand, tamper-evident packaging, splitting of the consignment into more than one delivery for dispatch by different routes).

9.8.4 Electronic Messaging

Information involved in electronic messaging must be appropriately protected according to the information security risks and classification.

Messages should be protected against unauthorized access, modification, or denial of service. Correct addressing and transportation of Electronic Messaging messages must be ensured, along with the general reliability and availability of messaging services.

Legal considerations (such as requirements for electronic signatures) must be satisfied (see 9.9.1 Electronic Commerce and 14 Compliance).

Explicit approval by the Sr. Management is required prior to using external/public messaging services, such as Instant Messaging or file sharing.

MDI shall ensure that the communication protection requirements, including the security of exchanges of information, are the subject of policy development and compliance audits.

MDI shall ensure that none of its users are sending any sensitive information over emails. If there is any need to send the same, then the same can be performed by using the client provided secured email service or users can encrypt the data using password protection option of the zip file. In addition, MDI ensures that no user sends unencrypted sensitive information over email or other electronic medium.

Further, MDI's emails are encrypted using Microsoft O365 default encryption techniques.

Where required by legislation, consent is obtained before any PHI/PII (e.g., about a client/customer) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization.

MDI shall ensure that stronger levels of authentication are implemented to control access from publicly accessible networks by having:

- Two Factor Authentication implemented for all the users connecting to MDI using VPN
- Complex password shall be maintained for the passwords of the users connecting to MDI using Terminal Servers

When using electronic communication applications or systems for information exchange, the following items shall be addressed:

i. requirements (e.g., policies, standards) or guidelines shall be defined outlining acceptable use of electronic communication applications or systems;
ii. the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications;
iii. procedures shall be implemented for the use of wireless communications including an appropriate level of encryption;
iv. employee, contractor and any other user's responsibilities shall be defined to not compromise the organization (e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.);
v. the required use of cryptographic techniques to protect the confidentiality, integrity and authenticity of covered information;

vi. the retention and disposal guidelines shall be defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and

vii. controls and restrictions shall be implemented associated with the forwarding of communications (e.g. automatic forwarding of electronic mail to external mail addresses).

9.8.5 Business Information Systems

Information security must be taken into account in the design and use of internal business information systems, such as administrative and accounting systems.

Known/inherent security vulnerabilities in the systems must be addressed through suitable compensating controls and appropriate access rights must be configured. MDINetworX Secret information must only be communicated by secure, encrypted, mechanisms. Systems and data must be backed up regularly (see 10.5.1 Information Backup) and suitable resilience and disaster recovery arrangements must be made.

9.9 Electronic Commerce Services

9.9.1 Electronic Commerce

This section is not applicable to MDI as MDI doesn't deal with any online transactions. The only online transaction that happens is to release the payment to the employees.

9.9.2 Online Transactions

This section is not applicable to MDI as MDI doesn't deal with any online transactions. The only online transaction that happens is to release the payment to the employees.

9.9.3 Publicly Available Systems

The integrity of information made available on Internet websites, associated written media, and so on, should be protected using information security controls, such as access controls and digital signatures, depending on the nature of MDINetworX's business requirements and applicable legal obligations.

Information to be published by workers on behalf of MDINetworX in any public forum must comply with applicable laws, rules, and regulations and must be explicitly approved for publication by an authorized management body.

Interactive Internet websites, and so on, must be controlled so that:

- Any personal information is obtained and secured in compliance with applicable privacy/data protection legislation
- All data inputs are validated to ensure their integrity and to minimize the possibility of malicious attacks
- Legitimate information input to the system is processed completely and accurately in a timely manner
- Sensitive information is protected against unauthorized disclosure during collection, processing, storage and output
- Unauthorized user access to other networks and systems is prevented

9.10 Monitoring

9.10.1 Audit Logging

MDINetworX ensure plans for monitoring activities are developed, implemented, maintained, and reviewed for consistency with the risk management strategy and response priorities.

The Compliance Team shall review the event log on a daily basis. The event logs shall be auto generated daily by using the Desktop Central feature and shall be emailed to the ISO. Any deviation/observations shall be highlighted to the Sr. Management. The Compliance Team shall acknowledge to the email even if there are no deviations observed. The audit logs shall be retained at least for 180 days and after that it is retained for 1 year.

The ISO who is responsible for reviewing the log shall at least be graduated in Computer Science domain. In addition, the ISO who is performing this activity shall have an experience of 2+ years in Compliance.

All the reviews shall be documented in the “Review Tracker” and the same shall be circulated to the Sr. Management once in each year. The ISO shall capture the below details in the review tracker:

- Document Name
- Date of review
- Individual name who highlighted the observation
- Description of the observation (if any)
- Corrective Actions taken
- CA Taken by (name)
- The CA Date
- Final Status of the observation (Open/Closed/Hold)
- How the action plan is working post performing the CA

The ISO shall review the following:

- The Active User List – Compliance Team reviews the Domain active user reports on a weekly basis. The report contains the list of users currently active on the domain. Once the report is received, Compliance Team verifies whether all the individuals listed in the report are actually active by comparing the list along with the HR user report. If any deviation is observed, then it shall be highlighted to the IT team asking for resolution on the same on priority.
- Traffic Report – Compliance Team reviews the traffic report on a daily basis. The report contains the bandwidth usage of the internet. Compliance Team verifies the bandwidth utilization. If the utilization goes beyond 200% of the daily average then the same shall be highlighted to IT team asking for the reason for the spike in the bandwidth utilization. Based on the utilization, the ISO shall recommend the Sr. Management if procurement of any new ISP would be required.
- EventLog Analyzer Report –
    - Need to verify any suspicious activity being performed on any of the information systems.
    - User unsuccessful logon attempts (if any defaulters, the same shall be highlighted)
    - Any policy changes in the system, if yes then whether it was authorized.

  - Account management report – The number of new hires and the number of account created. The number of terminated users vs. the number of accounts deleted.
  - Any suspicious activity shall be initially enquired with the IT team, if the suspicious activity is actually an incident then proper decision shall be taken post conducting the meeting with the Sr. Management and the decision shall be taken on the same day the observation was made without much delay.
- Firewall report –
  - VPN users login details (verify whether only the authorized users are logging in)
  - IDS Report – Attack Reports (Verify whether only the authorized domains are hitting the servers)
  - Admin Reports – Verify whether there are any changes in the configuration of the firewall
  - Any suspicious activity shall be initially enquired with the IT team, if the suspicious activity is actually an incident then proper decision shall be taken post conducting the meeting with the Sr. Management and the decision shall be taken on the same day the observation was made without much delay.

All the above-mentioned report/logs are deemed adequate to support after-the-fact investigations of security incidents as they provide enough information about operating system, traffic in/out and other information so as to reach to the root cause analysis.

MDI shall ensure that information collected from multiple sources is aggregated for review.

MDI shall comply with all legal requirements for monitoring of system use including authorized and unauthorized access attempts.

MDI shall test its monitoring and detection processes annually. If any deficiency is observed then the same shall be remediated on priority with the approval of the Sr. Management. In addition, reviews shall be performed annually so as to identify the improvement areas.

Acceptable use agreements stating that the actions performed on all the MDI owned information system is monitored by means of CCTV, Domain Logs, Firewall Logs etc., shall be signed by all employees, contractors, and third-party users indicating that they have read, understand, and agree to abide by the rules of behavior before management authorizes access to the information system and its resident information and are retained by the organization.

The organization reviews and updates the rules of behavior every year and requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated.

MDI shall ensure that it reviews the failed log-in attempts and follow-up on any anomalies observed. The Compliance team is responsible for reviewing and highlighting the failed log-in attempts to the compliance

MDI shall create a secure audit record each time a user accesses the covered information via the system. Further, MDI doesn't have access/authority to create/modify/archive the covered information. Audit logs recording exceptions and other security-relevant events must be produced and retained securely to assist with the investigation of security incidents and routine security monitoring.

Audit logs must also include the following items:

- User IDs
- Event ID's
- Function performed
- Date/Time of the event
- Terminal identity or location if possible
- Records of rejected system access attempts
- Changes to system configuration
- Network addresses and protocols
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems

The audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken. Where possible, System Administrators should not have permission to erase or de-activate logs of their own activities (see 9.1.3 Segregation of Duties).

MDI shall ensure that an intrusion detection system is managed outside of the control of system and network administrators be used to monitor system and network administration activities for compliance.

A separate log shall be maintained for messages sent/received containing PHI/PII. The log shall contain the following:

- Date/Time the message was sent/received
- Origin of the message
- Destination of the message

Note: For security reasons, the data sent/received shall not be captured in the log.

MDI shall ensure that auditing is made available at all times while the system is active and audit logs are maintained for:

i. dates, times, and details of key events (e.g. log-on and log-off);
ii. records of successful and rejected system access attempts;
iii. records of successful and rejected data and other resource access attempts;
iv. changes to system configuration and procedures for managing configuration changes;
v. use of privileges;
vi. use of system utilities and applications;
vii. files accessed;
viii. network addresses and protocols;
ix. alarms raised by the access control system;
x. activation and de-activation of protection systems, including anti-virus systems and intrusion detection systems, and identification and authentication mechanisms; and
xi. creation and deletion of system level objects.

Monitoring of unauthorized access attempts include failed or rejected user actions, including attempts to access deactivated accounts and actions involving data and other resources, access policy violations and notification for network gateways and firewalls, and alerts from proprietary intrusion detection/protection systems (IDS/IPS).

MDI shall ensure that it has implemented IDS/IPS (Intrusion Detection/Protection System) on its network and the same is updated promptly whenever it is required.

Monitoring of the privileged operations include the use of privilege accounts, system start-up and stop, and I/O device attachment/detachment.

Monitoring of authorized access includes the user ID, date and time of key events, types of events, files accessed and the programs/utilities used.

Monitoring of system alerts or failures include console alerts or messages, system log exceptions, network management alarms, alarms raised by the access control system (e.g., IDS/IPS or network monitoring software), and changes or attempts to change system security settings and controls.

Audit records are retained for a period of 180 days (then archive for 1 year) and then once the retention period is completed, it will be deleted by the script prepared by MDI's IT Team.

MDI shall have Data Loss Prevention (DLP) installed on all the systems and monitor the domain activities using Desktop Central tool to identify irregularities or anomalies that are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient and secure state.

MDI shall use Desktop Central tool for monitoring system events, detecting attacks and analyzing logs and audit trails to allow the identification of all access or modification of any given record by any given system user over a given period of time. Monitoring devices are deployed at strategic and ad hoc locations to track specific transactions and the impact of security changes to information systems.

MDI shall review physical access logs for Main Door, Operations, QA & SIT weekly and upon occurrence of security incidents involving physical security.

MDI shall respond to physical security incidents and coordinate results of reviews and investigations with the organization's incident response capability.

MDI shall review the IDS/IPS logs once in a month. In addition, MDI shall ensure that its IDS/IPS signatures are up-to-date.

MDI shall include elements for access control to MDI auditing tools (e.g., AD Audit Plus, Log 360, Event Log Analyzer, etc.) to prevent any possible misuse, compromise, or unauthorized access.

9.10.2 Monitoring System Use

Procedures and Areas of Risk

Procedures for monitoring use of information processing facilities must be established and the results of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The compliance manager shall review the log once in a week.

Changes to, or Attempts to Change, Security Settings and Controls Risk Factors

The result of the monitoring activities must be reviewed regularly. The frequency of the review should depend on the risks involved. The following risk factors must be considered:

- The criticality of the application processes
- The value, sensitivity, and criticality of the information involved
- The past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited
- The extent of system interconnection (particularly public networks)
- Logging facility being de-activated

9.10.3 Protection of Log Information

As far as is practicable, logging systems and log files must be secured against unauthorized changes and operational problems, such as:

- The security logging facility being de-activated or suspended
- Alterations to log file contents, or to dates and times of log files or individual entries
- Deletion or renaming of log files
- Exhaustion of log file space, thereby causing records to be discarded or overwritten

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

MDI's Information systems support audit reduction and report generation that supports expeditious, on-demand review, analysis, reporting and after-the-fact incident investigations of security incidents and does not alter the original content or time marking of audit records.

The logs that require auditing on a continuous basis in response to specific situations are listed in "9.10.1 Audit Logging". In addition, the listing of auditable events and supporting rational are reviewed and updated once in each year.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

This process outlines the steps for granting both temporary and permanent access to MDI auditing tools, including but not limited to AD Audit Plus, Log 360, Event Log Analyzer, and other enterprise tools. It defines the roles and responsibilities of the teams involved, including IT administrators, access control administrators, and compliance teams.

Additionally, it details the workflow of access grant tickets, specifying the required information for such tickets and the approval process for access requests.

Process

- Access Request Initiation:

Initiator: IT Personnel

Action: IT personnel send an access request email to the IT Head specifying the purpose, type of access needed (Admin, Technician, Read-only, Contributor), and their job role.

- Initial Review by IT Manager:

Initiator: IT Manager

Action: IT Head reviews the access request, considering the requester's job role and the necessity of the requested access.

- Approval Decision:

Initiator: IT Head

Action: IT Head approves the access request if it aligns with the job responsibilities and is in compliance with policies and regulations.

- Access Control Administrator Review:

Initiator: IT Manager

Action: IT Manager review the approved request, verifying the appropriateness of the access level (Admin, Technician, Read-only, Contributor) and checking tool-specific requirements.

- Access Provisioning:

Initiator: IT Manager Access Control Administrators

Action: Upon successful reviews and approvals, access control administrators provision the approved access levels to the requester. This involves configuring permissions and settings in the respective tools (E.g. AD Audit Plus, Log 360, Event Log Analyzer, etc.).

- Notification to Requester:

Initiator: Access Control Administrators

Action: The requester receives a notification indicating that their access has been provisioned. The notification may include details about the granted access level and any relevant guidelines.

- Continuous Monitoring:

Initiator: Access Control Administrators,

Action: Continuous monitoring of access is conducted to ensure ongoing compliance. Regular audits may be performed to verify that access levels remain appropriate.

- Access Review and Renewal:

Initiator: IT Head, Access Control Administrators

Action: Periodic reviews of access rights are conducted to assess ongoing necessity. If access is no longer required or needs adjustment, the IT Head and access control administrators take appropriate actions.

This structured workflow ensures a comprehensive and controlled process for granting access to MDI auditing tools, promoting security, compliance, and efficiency in managing IT access within the organization.

9.10.4 Administrator and Operator Logs

IT operations staff, system administrators, and so on, must maintain “Operator Logs” recording important activities on production systems in accordance with Operations and related procedures.

MDI shall ensure that audit logging is enabled and is enforced via group policy through active directory. Further, group policies shall be pushed every 24 hours.

Operator logs & Administrator logs must be regularly reviewed by ISO for compliance with stated procedures and any anomalies. They may also be audited at any time.

The Administrator logs shall include but are not limited to:

- Success/Failure of the Event
- Date/Time of the Event
- Detailed Information about the event or failure
- The account or Administrator involved (or the IP address)
- Processes involved
- system start-up and stop
- I/O device attachment/detachment

9.10.5 Fault Logging

Faults (that is, problems with IT or communications systems including definite or suspected security breaches, system failures, program errors/bugs, viruses, and other undesirable system operation) must be reported and logged, using automated functions where available.

Appropriate corrective actions must be taken promptly. There must be clear rules for handling reported faults including management reviews of the following:

- Fault logs to ensure that faults have been satisfactorily resolved
- Corrective measures to ensure that controls have not been compromised and that actions taken were fully authorized
- Error logging configuration parameters

9.10.6 Clock Synchronization

To facilitate forensic analysis, IT operations staff must synchronize system clocks against an agreed reference, such as Universal Coordinated Time (UTC), and monitor their accuracy.

Technical facilities (such as Network Time Protocol) or processes (manual review and correction) must ensure that system clocks remain within a few seconds at most of the true time, especially on critical systems.

9.11 Client Communication Handling

MDI understands the seriousness and impact of client communication. Thus, MDI has a policy wherein only authorized users would communicate with the customers in case of any additional question / query from the question that the agent is not aware about. In addition, MDI has explained its agents not to reply on any of the customer complaints as MDI want them to be analyzed and find the RCA so that the same issue is not repeated.

MDI shall ensure that the client is well aware about the MDI’s escalation matrix.

10. Access Control

10.1 Business Requirement for Access Control

10.1.1 Access Control Policy

Based on information security risk assessments, business requirements to control access to Significant Information Assets must be defined and documented by IAOs in the form of User Roles relating functions or components of the system to process, types of jobs or activities, taking account of:

- Information security requirements for specific business applications (distinguishing mandatory from recommended, optional or conditional requirements)
- Relevant fundamental information security principles summed up by phrases, such as 'default deny' and 'least privilege' (see 4 Security Policy)
- Identification and classification of information assets relating to the business processes and systems (see 6.2 Information Classification)
- Relevant legal and contractual obligations regarding protection of access to data or services (see 14.1 Compliance with Legal Requirements)
- Mandatory, recommended or conditional rules, and aspects which require explicit approval of the IAO (for example, use of privileged user IDs)
- Access rights assigned and managed using User Roles in preference to customized rights for individuals
- Segregation of duties where applicable (for example, the request, formal authorization and administration of user rights should be performed by different people)

MDI shall ensure that the requirements for controlling access to applications and application functions are addressed, by following the below:

- providing menus to control access to application system functions
- controlling which data can be accessed by a particular user
- controlling the access rights of users, e.g. read, write, delete and execute
- controlling the access rights of other applications
- limiting the information contained in outputs
- providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.
- enabling authorized users to determine whether access authorizations assigned to business partners match the access restrictions on information for specific circumstances in which user discretion is allowed
- employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions

IAOs must specify and authorize User Roles prior to the implementation of new IT systems, and review and re-approve them:

- Whenever significant changes occur in the IT systems, organization or business processes
- Routinely at least once a year

- At any other times when there is reason for management to suspect that inappropriate access rights might be in effect

The Compliance Manager will work with the IT and Sr. Management to ensure that all members of MDINetworX's workforce have appropriate access to EPHI and to prevent those who do not need access from obtaining it. These procedures must ensure that all personnel with access to EPHI have proper authorization and appropriate clearances.

MDINetworX has implemented administrative procedures to control access to systems containing EPHI as required by the HIPAA Security Rules. Such controls include procedures to provide for authorization, establishment and modification of user access to MDINetworX's systems.

To protect the confidentiality, integrity, and availability of EPHI, all members of the MDINetworX workforce are expected to comply with MDINetworX's access controls.

All the above said access policies applied to all system and/or application for which MDI is providing access that includes but are not limited to access granted to client for DocGem application.

The access list for system documentation is kept to a minimum and is authorized by the application owner

Data which is stored in information systems is protected with appropriate system access controls and security measures for the security of data. Periodic reviews of such output are performed to ensure that redundant information is removed.

10.2 User Access Management

10.2.1 User Registration

The following controls and procedures must be implemented in order to comply with this policy. It will then be possible to uniquely identify, differentiate, and monitor one user or workforce member from all others for the purpose of access control to all networks and application systems.

- Any user or workforce member that requires access to any network or application system, including those that access, transmit, receive, or store EPHI, must be provided with a unique user identification string.
- Requests for access must be approved by the user's manager, documented, and retained for audit purposes
- Access must be granted only when it is appropriate for the user's job responsibilities and it does not compromise segregation of duties (see 9.1.3 Segregation of Duties)
- The unique user identification in conjunction with a secure password (for a complete description of secure passwords, see the 10.3.1 Password Use) is required to gain access to any network, system, or application.
- The unique user identification must not give any indication of the user's privilege level (see 10.2.2 Privilege Management), for example, manager, supervisor, or system administrator.
- Users or workforce members must not allow another user or workforce member to use their unique User Identification or Password.
- Users or workforce members must ensure that their User Identification is not documented, written, or otherwise exposed in an insecure manner.
- Physical access to any supplier shall not be provided.

- Logical access may be provided to suppliers only when necessary and after approval from the Directors. In addition, the logical access shall be monitored by the compliance lead at least once in a week.
- Unique IDs that can be used to trace activities to the responsible individual are required for all types of organizational and non-organizational users.
- Communicate password procedures and policies to all users who have information system access
- Access to the information systems is granted based on minimum necessary for assigned duties, intended system usage and personnel security criteria such that access is granular enough to support an individual's consent that has been captured by the organization and limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function
- MDI IT team and Compliance team shall ensure that the user has authorization from the system owner or the manager for the use of the information system or service
- Separate approval for access rights from managers
- MDI shall give users a written statement of their access rights
- MDI ensure that users sign statements indicating that they understand the conditions of the access granted and the seriousness about the same.
- MDI shall ensure that no access is granted until authorization procedures have been completed
- If the user's manager is sending out a request for the user's access, then the same shall be considered as authorization and no further authorization is required
- MDI shall ensure that default accounts are removed and/or renamed
- MDI shall maintain a formal record of all persons registered to use the service
- MDI shall ensure to remove or block critical access rights of users who have changed roles or jobs or left the organization on their release day and remove or block non-critical access within twenty-four (24) hours
- MDI shall ensure that account inactive for more than 60 days shall be deactivated
- The Compliance reviews the user registered in DocGem (once the DocGem user billing is prepared) and verify whether they need to have access to the DocGem application. If there is any deviation, Compliance team will notify the Sr. Management about the same and the access is terminated on priority.
- MDI is currently employing manual processes to assist users in making information sharing/collaboration decisions.
- MDI requires verifiable unique ID's for all types of users including, but not limited to: technical support personnel, operators, network administrators, system programmers and database administrators.
- For unique Domain ID generation, MDI follows the below as the user name:
    - <<User's First Name>>.<<User's Last Name>>
    - If the user name is conflicting with other user's login name, IT personnel will verify if the user has middle initial so that the same can be added else, the IT personnel adds letter to the user name to make it unique
    - IT personnel shall ensure that the same user name is not provided to any other user even if the previous user is terminated
    - The same user name is being used by PMS & Golem as they are synced with Domain
- For unique email ID generation, MDI follows the below as the user name:
    - <<User's First Name>><<First letter of user's last name>> @ mdinetworx.com
    - If the user name is conflicting with other user's email ID, IT personnel will take suitable action to make the email ID unique either by adding the second letter of the last name or some numerical value so that the ID is unique.

- The above-mentioned process is also applicable to Third-Party/Temporary access provisioning. The only difference is that the access to Third-Party/Temporary access shall only be granted post receiving approval from the Sr. Management.
- MDI is currently using Manage Engine's AD Manager tool for creation of the domain ID's.
    - The initial ticket to create the domain ID is raised by a Compliance team member
    - The ticket is then allocated to Compliance Lead for approval
    - The compliance Lead approves the ticket post completing HIPAA & ISMS training and post reviewing the BG check report.
    - Once the ticket is approved by the compliance lead, it is then executed by the IT Team personnel and the domain ID is created.

It is the responsibility of users and workforce members to ensure that their assigned user identification is appropriately protected and only used for legitimate access to networks, systems, or applications. If a user or workforce member believes their user identification has been compromised, they must report the security incident to the ISO immediately.

The IT team is responsible for receiving and processing requests for access by individuals for PII/PHI records/folder as organizational records for a period of six years.

The organization ensures that the use of system utilities is controlled by implementing, identification, authentication, and authorization procedures, segregating of system utilities from applications software and limiting the of the use of system utilities to the trusted and authorized users to ensure appropriate access.

Terminated Users' Accounts

- Accounts inactive for 90 days must be disabled by the system administrator.
- Accounts of users that were terminated or have resigned must be disabled on the date of departure.
- Accounts for users that will be on extended leaves, for example, Maternity have no business reason for accessing the above resources, must be disabled on the first day of leave.

10.2.2 Privilege Management

Additional security measures are often necessary to restrict use of powerful system functions and access rights. IAOs may therefore reserve the right to approve personally the allocation of Privileged User Roles to highly trustworthy and competent users, rather than delegate this to other managers. The requirements for privileged users supplements the generic obligations on workers noted above.

Privileges must only be allocated to and used by authorized individuals for legitimate business purposes. Privileged User IDs must not be used for routine office activities.

In conjunction with the ESO, IAOs must define any special security controls as part of the definition of Privileged User Roles. The privileges associated with each system product (for example, operating system, database management system) or application, plus the user Roles which require those privileges, must be identified. Where possible,

privileged programs/routines should be used to avoid the need to grant privileges to users provided these are appropriately controlled against unauthorized access.

Privileged users must be given written statements of their access rights and conditions of use of the systems (as defined by the IAOs) and must sign to confirm that they accept the conditions of use before being given access (see the following Privileged User Code of Conduct). Until the authorization process is complete, privileged access must not be granted.

MDI documents access agreements for information systems, and privileges are granted only after the employee accepts the agreement AND the terms and conditions have been satisfied.

MDI shall ensure that elevated privileges are assigned to a different user ID and shall only be provided to IT personnel and the IT personnel shall not use the same for normal business use. All users access privileged services in a single role, and such privileged access is minimized. Users who perform privileged functions (e.g., system administration) use separate accounts when performing those privileged functions. IT personnel in MDI are performing only administrative roles and thus they have privilege access. They do not carry any other account as it is not required for our business.

MDI shall ensure to restrict access to privileged functions and all security-relevant information. Access to privilege functions if provided shall only be limited to IT personnel.

MDI shall ensure that it authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information:

- Setting/modifying audit logs and auditing behavior
- Setting/modifying boundary protection system rules
- Configuring/modifying access authorizations (e.g., permissions, privileges)
- Setting/modifying authentication parameters
- Setting/modifying system configurations and parameters.

Privileged User Code of Conduct

Privileged Users and all other persons given broader-than-normal access privileges on MDINetworX computer systems agree:

- Not to "browse" through the computer information of applications, systems, or system users while using the powers of privileged access unless such browsing meets one or more of the following criteria:
    - is a specific part of their job description (for example, an ESO auditor)
    - is required during file system repair, management, or
    - is necessary to investigate suspicious or system-impairing behavior
    - is specifically requested by, or has the approval of the person who authorized their privileged access
- Not to amend users' files without their consent. Files may only be deleted in an emergency, and the Privileged User must inform the user of the action and the reason for it (e-mail is an acceptable form of notification).

- Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.
- Not to copy any computer information for any purpose other than those authorized under their defined job responsibilities.
- Not to intentionally or recklessly damage or destroy any MDINetworX computing resources.
- Not to accept favors or gifts from any user or other person potentially interested in gaining access to MDINetworX computer systems.
- Not to do any special favors for any user, member of management, friend, or any other person regarding access to MDINetworX computers. Such a favor would be anything that circumvents prevailing information security policies. Not to tell or disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.
- Not to attempt to gain or use privileged access outside of assigned responsibility (for example, on other machines) or beyond the time when such access is no longer required in assigned job functions.
- Not to change or develop any computer software in a way that would disclose computer information to persons not authorized to have it, or make it possible to retain any special access privilege once that authorized privilege has been terminated by management.
- Not to make arrangements on computer systems under their charge that will impair the security of other systems. In order to comply with this restriction, a Privileged User setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.
- Furthermore, Privileged Users and all other persons given broader-than-normal access privileges on MDINetworX computer systems agree that they will do the following:
    - Use good judgment in the execution of their responsibilities.
    - Report all suspicious requests, incidents, and situations regarding a MDINetworX computer to the ESO.
    - Use all available protections to safeguard computer systems under their charge from unauthorized access by any person or another computer.
    - Take steps to the best of their ability to comply with all MDINetworX established computer security policies, standards and procedures while managing technology assets, and furthermore, advise management and/or the ESO of deficiencies in these standards.
    - Privileged Users should only access or review the minimum amount of EPHI necessary to complete the required function.

10.2.3 User Password Management

The allocation of passwords must be controlled through a formal management process. The process must include the following requirements:

- Users are required to maintain their own passwords and are provided initially with a secure temporary password (see 10.3.1 Password Use), which they are forced to change immediately. Once the user's domain account is created, the initial password is sent to the user's WhatsApp account by the IT team personnel.
- MDI has launched AD Self Service Tool effective Jan'19 which will help the users to reset/unlock their passwords after answering three security questions (two pre-defined security questions and one security question which the user shall enter manually). Only after answering all the three security questions correctly the user would be allowed to change his/her password or to unlock his/her windows account.
- Passwords should never be stored on computer systems in an unprotected form.
- Default vendor passwords should be altered following installation of systems or software.
- Passwords shall not be displayed when entered in Windows OS / DocGem / PMS / Golem / SonicWall VPN

- MDI shall maintain a list of commonly-used, expected or compromised passwords which shall be updated and reviewed once in every 180 days and when organizational passwords are suspected to have been compromised, either directly or indirectly
- MDI shall create awareness during ISMS trainings that all employees should choose strong, unique passwords and avoid using commonly-used or easily guessable passwords. Passwords must meet the organization's defined security criteria to enhance the overall security posture
- MDI shall ensure that the users are made aware of the organization's password policies and requirements
- It will be the user's responsibility to keep the password confidential
- None of the users shall write their passwords in any of the documents/papers/file in a system or on mobile devices
- MDI shall ensure that users are made aware to keep passwords confidential, avoid keeping a record of passwords (whether on paper or electronically), unless this can be stored securely and the method of storing has been approved.
- Users shall change passwords whenever there is any indication of possible system or password compromise.
- Users shall not share individual user accounts or passwords and not provide their password to anyone for any reason.
- Users shall not use the same password for business and non-business purposes, and select quality passwords
- The Compliance team approves to save the passwords in a Microsoft excel worksheet, provided that the worksheet is password protected and no individual can open the file without the password of the file.
- IT is the user's responsibility to change passwords whenever there is any indication of possible system or password compromise
- The users shall never share their login credentials of any application or domain to anyone
- MDI shall enable the strong password complexity feature for all the users and for all its applications and password must be set as per the instructions provided in Section 10.3.3.
- MDI shall ensure that all the application passwords are encrypted
- MDI users shall not use the same password for business and non-business purposes. i.e., keep your passwords used for your office purpose completely different and should not match with any of your personal account passwords.
- MDI shall ensure that users are forced to select complex passwords that matches MDI's password policy.
- MDI shall ensure that each employee signs the Acceptable use policy that specifies that each employee has to safeguard the passwords provided to them. HR asks the user to sign on the acceptable use policy and explains them about the same in detail during the induction of the employee.
- MDI shall ensure that users get a message about the password criteria, if the users try to select the password that doesn't satisfy the MDI's password requirement.
- MDI allows users to select and change their own passwords and include a confirmation procedures to allow for input errors.

10.2.4 Review of User Access Rights

If access requirements have changed as a result of the associate changing positions or leaving the company, the user's access privileges should have been modified accordingly.

Additional interim reviews should be conducted periodically on high risk/business- critical systems as specified by the IAOs. Ad hoc access rights reviews may be conducted at any time at the request of management, IAOs, Information Security or auditors. User access rights are reviewed after any changes and reallocated as necessary.

MDI shall ensure to review critical system accounts and privileged access rights at least on monthly; all other accounts, including user access and changes to access authorizations, are reviewed at least on monthly.

All reviews of access rights and privileges must be documented and the documentation retained for at least a year in a form suitable for audit.

DocGem/Golem/PMS Active User Review - The DocGem/Golem/PMS active user report shall be reviewed once in a month.

System Accounts Review – On a monthly basis, automated mail is generated from HRMS which has the list of inactive and active user accounts and shared with compliance team. Compliance team shall review, and unnecessary accounts are removed, disabled or otherwise secured. The review shall include Guest/anonymous, shared/group/generic, emergency and temporary accounts as well.

10.2.5 Mobile Device Usage Policy

- MDI recognizes the role of information security to ensure the same, use of mobiles phone or any removable Media device on the Operations and Quality floor shall be prohibited.
- All employees who works on PHI shall keep their mobile phones or any removable Media device in their respective lockers.
- If any employee is found carrying mobile phone or any removable Media device on the production floor disciplinary action will be taken against him/her which may even lead to termination from job.
- All supervisors have the rights to check any employee at any time on the production floor to ensure if he /she is carrying the mobile phone or any removable Media device.
- Employees with Team Lead or above are only allowed to use the mobile phone on the floor. Although, discussing/sharing the PHI through mobile phone is prohibited irrespective of the designation or grade.
- Employees who are working under IT department are only allowed to use removable Media device on the floor.
- Mobile phones are allowed to use in Software, HR and Admin associates. However, the same shall be controlled while they are on the Operations/Quality zone.
- Any user who notices associate using their mobile phone on either the Operations/Quality zones may report the incident to the compliance manager.
- All the company provided mobiles wherein the organization's email has been configured shall have ManageEngine MDM installed and running.
- No employee is permitted to change the setting or install/delete any app without the permission of the IT head.

10.3 User Responsibilities

10.3.1 Password Use

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MDINetworX's entire operation. As such, all MDINetworX associates (including clients, contractors and vendors with access to MDINetworX systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

10.3.2 General

- All user-level passwords, such as, windows and MDI hosted applications shall be changed every 30 days.
- All privilege account for OS as well as all the application passwords shall be changed once every 30 days.
- The password history shall be configured to remember past 24 passwords.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication unless a secure transmission platform is used, such as MDINetworX Secure E-Mail.
- Initial passwords are temporary and must be changed during first log in.
- Passwords shall not be stored in any macro, function key or any auto-scripts.
- MDI shall ensure that passwords are transmitted only when cryptographically protected and stored using an approved hash algorithm and salt. For the internal applications, MDI has configured LDAP and thus transmitting the passwords is not required. For DocGem, a hyperlink is shared on the user's email which is valid for 24 hours. Once the user clicks the hyperlink, DocGem prompts to enter the password of user's choice, but it should be a complex password as per our password policy.
- MDI's IT team shall ensure that the user's password is not reset unless it is requested by the user's manager. When setting the password for the first time, IT team shall request the user to input the new password in front of them after verifying their identify by looking at the badge of the user. If the user has not received the badge or has forgotten the badge, then a temporary password shall be shared with the user's manager. The temporary password shall be mandatorily changed upon first login.
- Once the password has been set by the user successfully, they acknowledge that they received and have changed the temporary passwords verbally either to their reporting supervisor or to the IT personnel directly.
- MDI shall ensure that the temporary passwords are unique and not guessable. MDI IT personnel set the password manually by choosing random letters, numbers and special characters. In addition, IT personnel shall ensure that he selects the option to change the password on first logon shall always be selected.

MDI shall maintain a list of commonly-used, expected or compromised passwords, and updates the list at least every 180 days and when organizational passwords are suspected to have been compromised, either directly or indirectly.

10.3.3 Password Construction

All user and system level passwords must meet the strong password characteristics defined in the following:

- Contain both upper- and lower-case characters, for example, a-z, A-Z
- Have digits and punctuation characters as well as letters, for example, 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters' long
- Are not a word in any language, slang, dialect, jargon, and so on
- Are not based on personal information, names of family, and so on

10.3.4 Wireless Password Construction

MDI NetworX provided WIFI shall follow the below complexity and shall follow the AES WPA2 encryption method.

- Contain both upper- and lower-case characters, for example, a-z, A-Z
- Have digits and punctuation characters as well as letters, for example, 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fourteen alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, and so on
- Are not based on personal information, names of family, and so on

10.3.5 Unattended User Equipment

Employees should protect unattended IT equipment from avoidable harm, loss, theft or unauthorized access, taking into account the value of the data as well as the hardware.

Particularly valuable or vulnerable equipment, such as servers and portable PCs must be physically protected to a suitable degree (for example, using cable locks, tamper-resistant labels/disfiguring paint and/or covert marking, and

All Employees should be informed of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Employees must:

- Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, such as a password protected screen saver
- Log-off computers when the session is finished (that is, not just switch off the PC screen or terminal)
- Secure PCs or terminals from unauthorized use by a key lock or an equivalent control, such as password access when not in use (see the following 10.3.5 Clear Desk and Clear Screen Policy).

Significant quantities of IT equipment must be stored securely.

10.3.6 Clear Desk and Clear Screen Policy

All MDINetworX information processing facilities must adopt a clear desk policy for papers and removable storage media and a clear screen policy. The purpose is to reduce the risks of unauthorized access, loss of, and damage to information, including EPHI during and outside normal working hours. Information (papers and removable storage media) left out on desks is also likely to be damaged or destroyed in a disaster such as a fire, flood or explosion.

Information security classifications must be considered (for more detailed information, see 6.2.1 Classification Guidelines).

The following controls are required:

- Sensitive or critical business information must be locked away (ideally in a fire- resistant safe or cabinet) when not required, especially when the office is vacated.

- Personal computers and computer terminals and printers must not be left logged on when unattended and should be protected by key locks, passwords or other controls when not in use (for more detailed information, see 10.5.5 Session Time-Out).
- Incoming and outgoing mail points and unattended fax machines must be protected.
- Photocopiers and scanners must be locked (or protected from unauthorized use in some other way) outside normal working hours.
- Sensitive or classified information, when printed, must be cleared from printers immediately.
- Transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit to ensure no leak of information.

10.4 Network Access Control

10.4.1 Policy on Use of Network Services

Physical, logical, and procedural controls must limit access to the MDINetworX network comprising the network links/connections, network nodes (including routers, firewalls, application servers, workstations, and various other network-attached devices) and/or network services (such as file and print, HTTP/web and e-mail services).

Network access must be limited according to a combination of business requirements (see 10.1 Business Requirement for Access Control) and information security policy requirements (see 4 Security Policy):

- The ‘default deny’ principle applies to network access, in other words users must only be provided with access to networks and networked systems that they have been specifically authorized to use
- Physical access to networking equipment and cabling (except for LAN tails) must be limited to authorized support persons (see 8.2 Equipment Security)
- Logical access to networks must be limited to authorized and authenticated people or systems using access controls applied at the servers, routers, firewalls, and so on, (see 10.4.6 Network Connection Control)
- Firewalls must control both inbound and outbound access (see 10.4.3 Equipment Identification in Networks and 10.4.6 Network Connection Control)
- Procedures for managing, monitoring and using networks must be documented and followed (see 9.6 Network Security Management)

Interconnections between MDINetworX and third-party networks must be explicitly authorized by the ESO. Following an information security risk assessment, network access control requirements for such connections must be specified as part of the security design documentation, implemented and maintained.

Note: Interconnections here means persistent point-to-point network links, such as leased lines and Virtual Private Networks, excluding temporary connections made by Internet browsers.

Worker access to Internet–based services must be logged and restricted to legitimate business purposes. All Internet connections to MDINetworX equipment must be explicitly authorized by the ESO due to the need to incorporate strong security controls counteracting the high level of threats.

Network security incidents and parameters must be monitored routinely by relevant internal functions (such as Service Desk and Internal IS Support) and third-party service providers, each focusing on their respective areas of responsibility

but sharing information where relevant. Network security incidents must be logged securely and, where applicable, promptly trigger the escalation and incident response processes (see 12 Information Security Incident Management).

Network security vulnerabilities must be monitored routinely by Information Security. Risks to MDINetworX networks and devices must be assessed and prioritized. Vulnerable systems must be patched promptly if there are significant threats. If patches are not available or cannot safely be applied, alternative compensating controls (such as additional monitoring) must be implemented to minimize the risks.

Security configuration parameters of network control components (such as firewall filtering rules, protocols in use, open ports, and so on) must be documented, maintained under change control (see 11.5.1 Change Control Procedures) and periodically tested for accuracy and suitability (see 14.2 Compliance with Security Policies and Standards and Technical Compliance).

Network operating procedures must be documented and incorporate suitable information security management controls (see 9.6 Network Security Management).

10.4.2 User Authentication for External Connections

Procedures must be published to address user authentication for connections to MDINetworX information systems (including those that contain EPHI) from external connections. Procedures must address the following controls:

- Users seeking access to MDINetworX networks must be authenticated at the initial point of entry into the network using unique user IDs and multi-factor authentication (for example, cryptographic security tokens or smartcards coupled with passwords, PINs and/or biometrics), according to the risks of unauthorized access. Unauthorized connections must be dropped (‘default deny’).
- User authentication devices (access control gateways, remote access tokens, and so on) must be risk assessed and explicitly authorized by the ESO. Connections between MDINetworX and third-party networks or systems must traverse authorized gateways.
- Access through gateways must be logged and monitored. Unauthorized access attempts must generate security alarms and, where relevant, trigger the incident response procedures (see 12 Information Security Incident Management).
- Gateways must be managed and supported by authorized support staff through secure access mechanisms authorized by the ESO. Management ports and services must not be exposed on insecure networks without strong multifactor user authentication controls (see 10.4.4 Remote Diagnostic and Configuration Port Protection).
- Dial-up and wireless modems must not be used on MDINetworX networks or systems unless explicitly authorized by the ESO.

IAOs may permit or deny remote access to their systems according to the business security requirements (see 10.1 Business Requirement for Access Control).

10.4.3 Equipment Identification in Networks

Connections between computer systems must be authenticated using secure methods approved by the ESO according to the level of security risk.

The risk level depends on factors, such as:

- The types of usage involved, ranging from simple data presentation (for example, a Web server), through end user access to an application system (for example, a mail server) or transaction processing system, to privileged systems management access
- The level of threats (for example, security threats are generally greater on Internet connections than those on trusted internal networks)
- Potential impacts of unauthorized connections (for example, whether business- critical systems might be affected)
- Other access controls already in place (for example, strong physical access controls within a data center reduce the probability of unauthorized systems being connected locally)

Potential node authentication methods range from MAC/Ethernet/IP addresses (for low risk situations) to mutual cryptographic authentication using tokens or digital certificates. The methods chosen to satisfy the business and security requirements must be professionally designed, documented, tested, implemented, operated, maintained and reviewed, with the frequency and extent of review reflecting the security risk level.

10.4.4 Remote Diagnostic and Configuration Port Protection

Access to remote diagnostics, configuration/management or console ports and modems permitting privileged access for technical support on devices, such as telephone exchanges, servers, disk subsystems, routers, firewalls, and gateways, must be restricted to authorized support staff using strong user authentication and access control mechanisms specifically authorized for this purpose by the ESO (see 10.4.2 User Authentication for External Connections).

Where possible, privileged ports/modems should only have enabled as and when required for specific authorized remote support activities.

10.4.5 Segregation in Networks

Security factors must be considered when designing, configuring or altering the network architecture. In addition to the perimeter controls noted elsewhere, internal MDINetworX systems and networks should be segregated according to the respective information security risks into separate categories, groups, partitions or domains, such as:

- Ordinary business applications (without high confidentiality, integrity or availability requirements) versus especially critical, valuable, or sensitive business applications (with high confidentiality, integrity, or availability requirements)
- Third party networks (such as the Internet) versus purely internal networks
- Systems owned or managed by third parties versus MDINetworX
- Development versus test versus production systems
- Wired versus wireless networks
- Ordinary user traffic versus systems/network/security management traffic

Segregation should use appropriate control mechanisms, such as firewalls/gateways, physical isolation (air gaps), encryption (for example, VPNs), and so on, reflecting the security requirements arising from business needs, assessed

information security risks and these information security policies (see also 10.1 Business Requirement for Access Control, 10.4.6 Network Connection Control, and 10.4.7 Network Routing Control).

10.4.6 Network Connection Control

Connections between networks must be controlled using firewalls (specialized routers or gateways dedicated to network access control) authorized for this purpose by the ESO. Firewalls must:

- Be designed into the network security architecture to satisfy business requirements, minimize risks identified by security risk assessments and comply with these policies
- Apply packet filtering rules based on criteria, such as packet integrity, network ports, protocols, services or applications, device addresses, connection state, and so on
- Permit access only by authorized users to authorized network services, blocking all others ('default deny') (see 10.1 Business Requirement for Access Control)
- Have sufficient capacity and resilience to satisfy business requirements for network availability and performance (see 9.6.1 Network Controls)
- Be managed by Network Operations using strong authentication and access mechanisms approved by the ESO (see 10.4.2 User Authentication for External Connections)
- Be kept up-to-date in respect of software versions, configurations and filtering rules to address current security threats through change control procedures (see 11.5.1 Change Control Procedures)
- Log security messages (including configuration changes and unauthorized access attempts) to secured log files and raise real-time security alarms in the event of potentially serious security incidents requiring urgent action (see below)

Firewall security alarms and logs must be monitored (alarms must be monitored in real-time and logs must be reviewed daily). Logs and/or alarms on critical firewalls should be distributed to additional functions (such as the ESO) for independent analysis. The incident response process must be initiated promptly whenever significant security incidents are identified (see 12.1 Reporting Information Security Events and Weaknesses).

Firewall filtering and logging rules must be documented for review and approval by the ESO according to an assessment of the information security risks. Configuration changes must be controlled (see 9.1.2 Change Management). Filtering and logging rules must be applied consistently, for example, network perimeter firewalls throughout MDINetworX must apply the same or equivalent rule sets.

10.4.7 Network Routing Control

In addition to the use of firewalls (see 11.4.6 Network Connection Control), other traffic routing controls (such as source and destination address-checking mechanisms, designated internal IP address ranges and Network Address Translation) must be used to govern information flowing within or between networks where this is deemed necessary for business purposes, to address control requirements arising from security risk assessments, and to comply with these security policies (see 11.1 Business Requirement for Access Control).

Network traffic should normally be controlled in both directions, for example to limit the misuse of MDINetworX systems for outbound Denial of Service attacks against third parties as well as to limit inbound attacks.

10.5 Operating System Access Control

10.5.1 Secure Logon Procedures

MDINetworX systems must use secure logon processes where available:

- PCs must use the control-alt-delete secure user log in initiator sequence
- Prior to a user logging on, systems should display a standard notice warning against access by unauthorized users and must not provide help messages or unnecessary information about the system or technology that might aid an unauthorized user
- Passwords, PINs, private keys, and so on, are classified MDINetworX Secret and so must not be displayed on the screen, sent unencrypted over the network, nor stored unencrypted
- If invalid user credentials and passwords, PINs, token values, and so on, are entered, systems should not indicate which elements were incorrect
- Systems should allow a defined number of unsuccessful logon or connection attempts at which point the corresponding user IDs should be suspended indefinitely. Such events must be recorded in the security event log and should generate security alarms in the case of privileged or enhanced access user IDs
- Once users are logged on, systems should display the dates and times of previous successful logons plus details of any intervening unsuccessful log on attempts
- MDI to limit the number of unsuccessful log-on attempts allowed to three attempts, and enforce:
    - disconnecting data link connections
    - sending an alarm message to the system console if the maximum number of log-on attempts is reached
    - setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected
    - limit the maximum and minimum time allowed for the log-on procedure, if exceeded, the system terminates the log-on
    - not transmit usernames and passwords in clear text over the network
    - not display system or application identifiers until the log-on process has been successfully completed
    - not provide help messages during the log-on procedure that would aid an unauthorized user
    - validate the log-on information only on completion of all input data. If an error condition arises, the system does not indicate which part of the data is correct or incorrect.

10.5.2 User Identification and Authentication

Users must be identified and authenticated using mechanisms that meet the security requirements of specific systems:

- Low-risk systems may use user IDs and passwords/PINs
- Medium-risk systems (including network and local access to privileged accounts) may use multi-factor authentication using digital certificates or other tokens in addition to user ID and passwords/PINs
- High-risk systems may require the use of even stronger authentication methods, such as cryptographic tokens/smartcards or biometrics.

Every authorized user must have a unique identifier (user ID) for their personal use in order to be able to trace activities logged by systems to the corresponding individual users. User IDs must conform to naming standards and must not give any indication of the users' access rights, for example, contain words, such as manager, supervisor or privileged.

User IDs required for non-interactive automated system-to-system logons should be configured to block interactive use.

Actions that can be performed without identification and authentication are permitted by exception.

Help desk support requires user identification for any transaction that has information security implications. For example, the user has to mandatorily use the AD Self-service portal in order to get his/her password reset/unlock. During the password reset/unlock process the tool asks for some security questions which can only be answered by the user. In addition, if the user is unable to use the AD self-service portal for any reason, then the IT personnel shall confirm his personal details and only share the account details to his manager via official email if the IT personnel is not confident about the user's identification.

The organization requires multi-factor authentication for access to non-privileged accounts when accessing from remote networks (which includes accounts in Web applications and in remote access solutions such as VPNs)

The information system uses replay-resistant authentication mechanisms such as one-time passwords for network access to privileged accounts. The organization employs multifactor authentication for remote network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The organization ensures that multifactor authentication is used for local access to privileged accounts wherever it is necessary to enhance security and authorization of individuals to critical information systems and processes.

10.5.3 Password Management System

Systems must allow users to select and change their own passwords and PINs, provided they first enter the original password/PIN (to prevent unauthorized changes) and confirm the new password/PIN (to trap data entry errors).

Wherever technically feasible, systems must automatically ensure that users choose strong (that is, difficult to guess) new passwords and change them regularly (see 10.3.1 Password Use).

MDI shall ensure that this Password Policy is applicable to all MDI systems including mobile devices. Users shall not have any permission to change the settings of the systems so that they cannot change the password complexity or any other setting related to password. In addition, MDI IT team shall immediately change the passwords for an account whenever there is any indication of possible system or password compromise.

MDI shall ensure that no user has authority to change the password length or other password configuration and change the authentication requirements for email or any other internet settings.

Systems must not display passwords on the screen. In addition, passwords shall never be sent on email in an unencrypted manner. MDI shall not use any third-party or unprotected (clear text) electronic mail messages for the distribution of passwords. MDI has encrypted all its password whether during transmission or during rest and on all its system components.

MDI IT team shall ensure that they are forcing the users to change the temporary password at the first log-on. In addition, requires immediate selection of a new password upon account recovery.

Passwords for Windows OS or any application used by MDI for its processing must be stored securely (that is, using one-way encryption/hashing) and separately from application system data.

MDI's IT team is responsible for changing any default vendor-supplied passwords. Also, they must be changed immediately following installation of software.

Procedures for resetting forgotten passwords must require positive authentication of the corresponding users, and reset passwords must expire following the first successful logon (see 10.2.3 User Password Management).

10.5.4 Use of System Utilities

Powerful system utilities and privileges that are capable of overriding system and application security controls must be tightly controlled:

- Routine and ad hoc access to system utilities and privileges must both be controlled using user authentication and access controls in order to limit access to the minimum practical number of trusted, competent users for authorized business purposes according to the 'default-deny' principle (see 10.2.2 Privilege Management).
- System utilities must be logically segregated from application software, for example, in separate directories with different access rights or Access Control Lists.
- All use of powerful system utilities and privileges must be logged securely.
- Unnecessary system utilities and systems software should either be removed from systems or disabled, especially in the case of important production systems.
  - disabling of public "read" access to files, objects, and directories
  - logging of all use of system utilities
  - defining and documenting authorization levels for system utilities
  - deletion of, or file system file execution permission denial of, all unnecessary software-based utilities and system software
  - denial of system utilities availability to users who have access to applications on systems where segregation of duties is required.

The information system owner regularly reviews the system utilities available to identify and eliminate unnecessary functions, such as scripts, drivers, features, subsystems, file systems, and unnecessary Web servers.

Ad hoc or temporary access to additional systems utilities or privileges must require explicit management authorization through the conventional change management process. Such access must be limited as far as practicable, for example, granted for the duration of authorized changes or support sessions for specified legitimate support purposes.

10.5.5 Session Time-Out

The following procedures must be followed to ensure that access is appropriately controlled to all servers and workstations that access, transmit, receive, or store EPHI.

- Servers, workstations, or other computer systems containing or accessing EPHI repositories must employ inactivity timers or automatic log off mechanisms. The aforementioned systems must terminate a user session after a maximum of 1 minutes or less of inactivity. This has been configured and pushed to all the devices using MDI's default group policy.
- Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms, such as a Password protected screen saver that blacks out screen activity. The aforementioned systems must terminate a user session after a maximum of 1 minutes, or less of inactivity. This has been configured and pushed to all the devices using MDI's default group policy.
- Applications and databases using EPHI must employ inactivity timers or automatic session log off mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 30 minutes. This is configured using the applications API configuration.
-
- If a system requires the use of an inactivity timer or automatic log off mechanism as detailed in the aforementioned procedures, but does not support an inactivity timer or automatic log off mechanism, one of the following procedures must be implemented:
  - The system must be upgraded or moved to support the aforementioned Automatic Log Off procedures.
  - The system must be moved into a secure environment.
  - All EPHI must be removed and relocated to a system that supports the aforementioned Security Automatic Log Off procedures.
- When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the systems' Automatic Logoff Mechanism.
- MDI cannot implement the session time-out for its network as the feature is not available in the SonicWall firewall
- Connection time controls are implemented for sensitive computer applications, especially from high-risk locations (e.g., public, or external areas that are outside the organization's security management). Connection time controls include using predetermined time slots restricting the connection times to normal office hours if there is no requirement for overtime or extended-hours operation, and re-authentication at timed intervals.

10.6 Application and Information Access Control

10.6.1 Information Access Restriction

Users of application systems, including support staff, must be granted restricted access to data and application functions in accordance with User Roles approved by the respective IAOs.

User Roles must be developed to reflect security requirements identified by risk assessment (taking into account the classification of data being processed by the systems and MDINetworX's access control policies (see 11.1 Business Requirement for Access Control) and incorporated into system security designs.

Changes to User Roles must be controlled in order to prevent unsuitable or unauthorized changes not specifically approved by the IAOs.

When application systems are designed, built, and operated, the following controls must be considered in order restrict information access under the 'default deny' principle:

- Menus and other workflow controls should govern access to application system functions, especially in the case transaction approval/authorization and security management functions. Systems must incorporate controls to prevent users gaining unauthorized access or skipping key parts of the process flow by bypassing the menus, manipulating URLs, and so on.
- The ways that users are permitted to access data items or collections (for example, read, write, delete, execute, create) must be controlled by the applications in conjunction with the operating systems and/or middleware, based on the user roles.
- Access controls must be tested against the application design documentation prior to systems being released for production. Access rights assigned to sample user IDs must be validated against those required for the corresponding user roles. Similar checks must be repeated as necessary thereafter, for example, following application changes, periodically through routine system/application security reviews, and occasionally through management reviews or audits.

10.6.2 Sensitive System Isolation

The sensitivity of an application system must be explicitly identified and documented in the security design through an information security risk assessment conducted by the IAO in conjunction with Information Security.

The risk assessment must take into account the shared nature of the IT infrastructure. For example, systems processing MDINetworX Secret information are likely to require special security measures, such as dedicated/isolated computing environments and data encryption to prevent data being compromised through the shared infrastructure.

11. Information Systems Acquisition, Development, and Maintenance

11.1 Security Requirements of Information Systems

11.1.1 Security Requirements Analysis and Specification

IT governance requires that MDINetworX must assess information security risks relating to proposed IT systems and specify suitable information security control requirements (see 3 Risk Assessment and Treatment).

MDI shall address information security and other business considerations when acquiring systems or services; including maintaining security during transitions and continuity following a failure or disaster. The organization ensures that the third-party maintains sufficient service capabilities together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

Information security must be taken into account from early in the systems development lifecycle in business cases, budget proposals, work requests, and so on, to minimize the overall security costs and ensure that sufficient resources are allocated to complete the necessary information security tasks. This applies to custom software developed in-house or externally and commercial off the shelf packages, both new systems and changes to existing systems.

Business cases should be reviewed and if necessary updated regularly by Project Governance Committees throughout the development process to ensure that any changes to scope, costs and benefits (including information security elements) are duly considered.

IAOs represent the interests of the business department/s who are the primary users of systems. IAOs must be identified at the earliest opportunity and guided where necessary to understand and accept their responsibilities towards information security controls and risk management. They must formally approve initial business cases plus, any subsequent changes.

Note: IAOs are typically the business sponsors of software development projects. Information Security, Risk Management, and the IS department represent the greater interests of the organization and are responsible for maintaining and protecting the security of the IT infrastructure as a whole. They must therefore be consulted at the earliest opportunity when developing or acquiring new IT systems or changes to existing systems. Consensus must be reached between all parties because they have the management authority and obligation to block implementation of IT systems following Production Acceptance Testing if they would adversely impact MDINetworX's IT risk profile.

Once development or system change projects are approved, Project Managers (working in conjunction with Information Security, Risk Management, and other specialists where necessary) are responsible for following MDINetworX's approved software development and acquisition methods including the following specific information security tasks:

- Conducting high level information security risk assessments and, if necessary, detailed risk analyses to clarify the security control requirements, reflecting the value of the information assets and the potential impacts of security incidents

- Preparing architectural/design documentation describing controls that address the identified information security risks and comply with this information security policy manual plus applicable standards, guidelines, and so on, and other requirements, such as legal and regulatory obligations
- Developing technical, procedural and managerial information security controls comprising an appropriate mix of preventive, detective and corrective controls
- Evaluating/testing systems against the requirements specifications, including security elements, and completing any modifications necessary to achieve compliance
- 'Packaging' systems ready for Production Acceptance Testing (see below)
- Obtaining IAO approvals for requirements specifications, as-built designs and evaluation/test reports

Any non-compliance with security requirements, policies, standards, and so on, must be brought to the attention of both the IAO and the ESO who may, if necessary, escalate the issue to the Security Committee as appropriate. Justifiable security policy exemptions will be granted, provided that the associated risks are acceptable to MDINetworX and that the IAO accepts personal accountability for any impacts pending their resolution (see 1.4 Policy Exceptions).

Individual development teams are responsible for conducting Production acceptance testing against MDINetworX's general requirements for IT systems, including information security policies, standards, and so on. The handover of software from development teams to IT operations is a critical control point in the development process. Entry criteria for Production acceptance testing include:

- Completion of business testing as evidenced by the IAOs' sign-off
- Delivery of complete installation packages comprising the final signed-off source code and object code, plus user and technical documentation, scripts/instructions for implementation and tools, documentation, and so on, required for operations, support and maintenance

11.2 Correct Processing in Applications

11.2.1 Input Data Validation

According to their security designs, application systems must incorporate suitable technical and procedural controls necessary to ensure the integrity (correctness, completeness, and accuracy) of data input manually or automatically. Validation checks must be applied to transaction data, standing data (for example, names and addresses, credit limits, client numbers) and parameter tables (for example, prices, currency conversion, tax rates) at the point of entry into the system or shortly thereafter.

In addition to automated validation (see below), validation of manually-input data may include manual procedures for checking the authenticity and completeness of source documents, and so on, by data entry personnel, by peer review or by managers who review and confirm or authorize data entry. Such checks may be routine (for example, individual lines on an input form are ticked off as they are entered and the finished screen or a data entry printout is visually checked against the form for completeness and accuracy) and/or ad hoc (for example, spot-checks confirm whether all source documentation is filed in sequence, is complete, appears authentic and contains no unauthorized changes).

Both manually- and automatically-input data may be validated by automatic or systematic validation functions. According to the security requirements of the application, the following checks may be necessary to detect and correct errors:

- Out-of-range values (such as excessively long strings)
- Invalid characters (such as quotes or other terminators in input data used to form SQL queries)
- Missing or incomplete data (such as key fields not entered or missing values in a sequence)
- Exceeding upper or lower volume limits (for example, if 10 data items or messages are expected but 9 or 11 are supplied)
- Unauthorized or inconsistent control data (for example, invalid or missing digital signature; column totals not matching row totals)
- Implausible data, meaning the use of business logic and correlation techniques to identify invalid or suspicious data values, combinations, timing, volumes, and so on
- Invalid batches (for example, incorrect file format or date, unexpected number of records, out-of-sequence, and so on)

The content of critical fields and data files (for example, bank account numbers, digital signatures) may be periodically reviewed and cross-checked by manual and/or automated processes to confirm their validity and integrity.

Requirements for data validation and related integrity controls should be determined by assessing information security risks in application systems. Stricter and more comprehensive data and system validation rules apply to applications processing data classified as having high integrity requirements compared to medium or low integrity systems.

Automated procedures should normally involve:

- Identification and/or rejection of invalid values (for example, using error flags or placing them in a ‘hold’ file)
- Creation of audit trail information about the identified errors in log files, alarms or reports
- No further processing of invalid entries unless the blockage is manually overridden either by re-entering the data or by special system override functions (access to which must be strictly controlled and recorded in the audit trail)

Procedures and responsibilities for handling and resolving validation errors must be defined. Manual processes should normally involve the following:

- Documentation and analysis relating to the errors including decisions about how they should be resolved (for example, tracing back along the audit trail to identify the sources or causes of the problems)
- Authorization to make any necessary corrections to data or systems through the standard access controls (see 10.1 Business Requirement for Access Control) and/or change control procedures (see 11.5.1 Change Control Procedures)

Correct operation of the integrity and other information security controls must be tested prior to implementing new systems or changes.

The above procedures/policy and any update to it shall be intimated to the respective person/team within the organization through email by IT Team/Operations manager (IT Team for IT related information and Operations Manager for any operational information).

MDI shall review procedures, guidelines and standards for the development of applications annually. The same shall be assessed and updated as necessary by the ISO.

MDI's Information system shall check the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. For the software developed by MDI (Golem, PMS & DocGem), MDI shall ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

MDI shall ensure that its application DocGem which is hosted on AWS shall undergo automated application vulnerability testing with an emphasis on input validation control by a qualified party on an annual basis. Further, for its internal application PMS and Golem which are internally hosted shall undergo automated application vulnerability testing by internal IT team on an annual basis.

11.2.2 Control of Internal Processing

According to their security designs, application systems must incorporate reasonable controls necessary to aid in the integrity of internal processing, such as:

- Recording relevant audit trail information in secure log files for subsequent analysis
- Referential integrity controls in database systems (for example, controlling changes to values in key fields used to link related data tables)
- Run-to-run and program-to-program controls, such as checking opening balances against previous closing balances, file update totals, transaction sequence numbers, and so on
- Validation of system-generated data, for example, input validation (see 11.2.1 Input Data Validation) and checking that interim calculations do not yield out of range or otherwise invalid temporary values
- Checkpoint and rollback processes to reverse invalid transactions gracefully
- Run-time, periodic or ad hoc validation of the integrity and authenticity of programs, records and/or files typically by comparing current hash values/digital signatures against trustworthy stored values (see 11.3 Cryptographic Controls) and malware scanning (see 9.4 Protection against Malicious and Mobile Code)
- Checks to ensure that application programs are run at the correct time and in the correct sequence where relevant (for example, batch systems)
- Checks for processing delays, long queues, excessive processing volumes, excessive memory or CPU utilization or other possible symptoms of processing errors, infinite loops, and so on, triggering appropriate error handling routines and exception procedures

11.2.3 Message Integrity

Message authentication techniques, such as digital signatures and cryptographic hash codes (see 11.3 Cryptographic Controls) should be used to protect the integrity of message contents where this requirement has been identified by the risk assessment process.

11.2.4 Output Data Validation

According to their security designs, output from application systems must be checked to ensure that processing has completed correctly and accurately, using controls, such as:

- Reconciliation of input/output control totals, for example, batch input totals or balances match batch output totals or balances
- Validation of output data values, for example, correct range and type
- Plausibility checks using business logic, consistency and correlation techniques to check whether the output is reasonable
- Completeness checks, for example, input records processed with no errors and hold file empty
- Backup-restore, checkpoint, and rollback processes to reverse invalid program runs gracefully, accurately, completely and reliably
- Recording relevant information (including validation pass/fail) in application logs, audit trails, and so on
- Input validation checks on downstream systems (see below)

Applications in a sequential process must generate and provide sufficient control information to downstream systems to enable them to verify the completeness and accuracy of their data inputs. Downstream input validation errors may trigger investigation of the upstream systems as well as the data interfaces and associated processes.

11.3 Cryptographic Controls

11.3.1 Policy on Use of Cryptographic Controls

Cryptography must be used to protect information with high confidentiality and/or integrity requirements, or to provide strong non-repudiation, where other controls are deemed inadequate.

Where necessary, functional and technical requirements for cryptography should form part of security design specifications and the controls should be developed, tested, implemented, configured, operated and maintained throughout the system development life cycle.

Asymmetric cryptosystems used by MDINetworX must conform with the overall structure and controls for MDINetworX's Public Key Infrastructure (PKI), in particular the controls necessary to generate key pairs, bind public keys unambiguously to authenticated individual people, systems or organizations, and to protect private keys against unauthorized disclosure.

Symmetric cryptosystems must comply with the specific requirements identified by risk analysis. Current published cryptographic standards should be used where possible.

Cryptosystems, parameters and security requirements must be re-evaluated periodically by IAOs and the ESO. Changes may be necessary from time to time to maintain security; therefore, systems should be designed with this possibility in mind (for example, using crypto libraries and modular architecture). MDI NetworX uses AES 256 as its encryption algorithms.

Legacy systems with outmoded cryptosystems should be upgraded or retired from service depending on the risk of compromise, or compensating controls may be necessary. It is especially important that systems are upgraded promptly if there is a significant possibility that valuable historical data might be retained and subsequently compromised by a third party.

Where included in system security designs as the result of risk assessments, digital signatures should be used to protect the authenticity and integrity of important electronic data, such as:

- Financial transactions involving funds or money transfers, payments, receipts, and so on
- Contracts and agreements between MDINetworX and third parties
- Authentication of users, programs and systems
- E-mails and electronic messages containing other important information

Depending on the degree of protection/level of trust required by the business, digital signatures must be cryptographically verified using public keys intended for signing and published on valid digital certificates issued by:

- MDINetworX (as part of the MDINetworX PKI)
- Other Certificate Authorities trusted by MDINetworX (for example, VeriSign)
- Other third parties (for example, PGP certificates)

Legal advice should be followed where relevant regarding laws and regulations impacting the import or export of encryption systems or encrypted data, and to ensure that digital signatures are binding.

MDI shall establish VPN tunnel (Host – Host based) to have a secured transaction of data between MDI and it's client. However, the final decision to implement the VPN tunnel would be taken by the client. If client doesn't agree to have a VPN tunnel established then MDI would not implement the same. MDI has a VPN tunnel established between MDI US and India offices for secured exchange of information.

For transmitting data files MDI shall ensure that one of the encryption method is followed:

- Encrypting the files using PGP key
- Data Transfer on SFTP

For full-disk encryption, logical access is independent of O/S access.

Documentation (and regular approval by CISO) of exception for not enabling encryption for systems storing covered information/PII/PHI other critical information, if any.

Decryption keys are not tied to user accounts.

Key Management

According to the security requirements identified by risk analysis, the confidentiality of private keys and shared secret keys, and the integrity of all cryptographic keys, must be strictly maintained using the following controls:

- Encryption and other logical access controls (for example, the use of tamper- resistant smartcards to protect public and private keys stored in digital certificates)
- Physical access controls, such as limited and controlled key distribution and storage (for example, Cryptographic Hardware Security Modules certified compliant with FIPS 140-1 Level 3)
- Key archive/escrow and recovery systems (see below)

Key generation must use the best available randomization techniques to prevent keys being guessed (except by brute force attacks which are limited by using long keys, cumulative delays, and so on, that restricts the rate of guessing).

Keys must be changed as often as is necessary to minimize the possibility of an attacker compiling a significant volume of data encrypted with a single key. Keys should have defined periods of validity. Details for specific systems must be defined in system security designs.

Systems must be designed to facilitate the archive/escrow and controlled recovery of cryptographic keys from secure storage (key vaults) where necessary, for example if keys are lost, compromised or damaged, or for use in contingency situations. Given the level of risk, key vaults must incorporate strong physical, logical and procedural controls to prevent unauthorized access to, use of, modification of or damage to the stored keys.

Systems must be designed to permit compromised keys to be withdrawn rapidly from service, for example by publishing an authenticated Certificate Revocation List.

In case, if any key is being compromised by any employee of MDI NetworX, then a police complaint shall be lodge post changing the key on the individual responsible.

In addition, only the directors shall have the rights/access to the secret authentication like the OTP's.

11.4 Security of System Files

11.4.1 Control of Operational Software

Implementation of software on production systems must be controlled to minimize the risk of corruption of operational systems. Only designated IT personnel, operating under the authority of the IAOs of the corresponding systems, are permitted to update production program libraries. All such updates must be authorized and logged (see 12.4.3 Access Control to Program Source Code).

Access to all source and executable code (including compilers and third-party modules) in production must be controlled. Changes to such code must be strictly controlled through the Change Control Process (see 9.1.2 Change Management).

Executable code must not be moved to, or created within, production until evidence of successful testing and production acceptance has been obtained and approved by the IAOs and IT operations. The corresponding program source libraries must be updated beforehand except in the case of authorized emergency interventions when updates may occur soon afterwards.

Previous versions of software programs must be retained under configuration management as a contingency measure including at least the most recent prior version and, where justified, by the risk or requirement for other business, regulatory or legal reasons, a certain number of previous versions or all versions within a defined period.

Vendor supplied software used in production must be properly maintained; especially in respect of security patches (see 12.6 Technical Vulnerability Management). This implies using versions currently supported by the supplier and covered by suitable maintenance/support agreements. New versions or patches must be applied where this reduces net risks to MDINetworX, comparing the current situation with the projection once the updates have been applied. As part of this risk assessment, updates should normally be tested unless the delay is judged by the IAO (on advice from the ESO and Risk Management) to be more risky than the chance of failure.

Physical or logical access to production systems must only be given to suppliers for support purposes when necessary, and with management approval. Suppliers must comply with this policy manual. Suppliers' activities while logged on to the system must be controlled, monitored, and logged to provide reliable evidence for management reviews or audits.

Whereas internal application functions control logical access to application data items by application users and administrators (for example, applying access rules defined in User Roles (see 10.1 Business Requirement for Access Control) and encryption to protect sensitive data items (see 11.3 Cryptographic Controls), operating system controls must prevent unauthorized direct access to application program and data files (including application utilities/tools, application configuration/parameter files, application startup/shutdown scripts and application log files) by other users.

Application program and data files should generally be owned on the system by dedicated user IDs that are configured to block interactive use.

MDI shall ensure that all the applications and operating systems are tested for usability, security, and impact prior to production. The tests shall include tests on usability, security, and effects on other systems, and are carried out on separate systems.

Direct read-only access to application programs and data files is authorized for routine systems management activities, such as backups, performance and capacity monitoring, and security monitoring. Other direct access is only permitted when authorized through the change control procedures (see 11.5.1 Change Control Procedures).

11.4.2 Protection of System Test Data

Test data must be secured according to its classification.

The use of production data for development or testing should be avoided wherever possible. If there is no alternative, production data must be desensitized by, for example, removing or obfuscating any sensitive information, including EPHI. MDINetworX Secret or EPHI classified production data must not be used for development or testing.

The following rules must be applied to protect production data when used for development or testing purposes:

- Essentially the same access controls which apply to production systems must also apply to other systems using copies or subsets of production data.

- Each time, copying of production data for use in development or testing must be specifically authorized by the IAO and logged by IT operations.
- Production data must be securely erased from other systems and media as soon as practicable after the work is completed.

11.4.3 Access Control to Program Source Code

Program source code and associated information (such as designs, specifications, program listings, test plans and reports) should be maintained under change control procedures (see 11.4.1 Control of Operational Software) in separate libraries for development, test and production environments, controlled by designated librarians.

Access to program source libraries should be restricted to authorized people undertaking legitimate business activities. Maintenance and copying of program source libraries should take place under the standard IT change control procedures (see 11.4.1 Control of Operational Software).

Physical and logical access to program source code and associated items is strictly controlled in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Programs under development, testing or maintenance should not be cataloged into production program source libraries. Only code that has completed Production Acceptance Testing and been approved for production use may be cataloged into production libraries.

Updates to code held in program source libraries and the issue or compilation of code from libraries should be performed directly by, or under the authority of, the designated librarian and must be logged.

Old versions of source programs should be archived, with a clear indication of the dates and times when they were operational, together with all supporting software, job control, data definitions and procedures (see 11.4.1 Control of Operational Software).

Third party-owned source code should be held in escrow if MDINetworX is critically reliant on the ability to maintain/update the code, particularly if there is any doubt about the vendor's resilience or capabilities.

11.5 Security in Development and Support Activities

11.5.1 Change Control Procedures

Significant changes to production environments should be explicitly approved by the IAOs whose systems will or may be impacted, and by IT operations. MDI shall ensure that it has standard SDLC process in place.

As far as possible, changes must be controlled to ensure that technical, physical, and procedural security controls relating to the existing production systems, data and the supporting infrastructure are not compromised. Change control procedures should therefore ensure that:

- Proposed changes are risk-assessed by competent persons (such as Information Security, Risk Management, Development, Testing and/or IT operations staff) to characterize potential adverse impacts on the production systems, data and infrastructure, plus the associated information security controls

- Changes are proven effective by Production Acceptance Testing (see 11.1.1 Security Requirements Analysis and Specification)
- Change implementations are carefully planned in order to minimize business disruption and risk, for example with suitable contingency (fallback) arrangements
- Developers and IT support staff are given access only to those parts of the production environment that are strictly necessary for their work, and for the minimum period
- System, operations and user documentation is updated on the completion of each change and redundant documentation is archived or securely disposed of
- Versions are controlled using version management, documentation and libraries (see 11.4.1 Control of Operational Software)

Where absolutely essential (for example, urgent patches necessary to address severe security vulnerabilities), emergency changes may be made to production systems without completing in advance the conventional change control process outlined above, provided nevertheless that sensible control measures are taken within the practical constraints, for example:

- The relevant IAOs and IT operations specifically pre-authorize such emergency changes on each occasion
- At least two workers are involved in implementing the changes
- Details of the changes are carefully recorded as they are made and the records are reviewed by relevant managers as soon as possible afterwards.
- Documentation is updated as soon as practicable after the event and to the same standard as for conventional changes.

Where suitable technical vulnerability scanners, installation verification routines and integrity checkers are available for a given system, they should be run after the implementation of application changes to verify that additional known vulnerabilities have not been introduced, installations have not been damaged and system integrity remains intact.

Managers responsible for application systems are also responsible for the strict control (security) of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

Access to program source code and associated items is strictly controlled in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

MDI shall ensure that the program source codes are stored in a central location, specifically in program source libraries. MDI to follow the below for all its applications:

- program source libraries are not held in operational systems
- the program source code and the program source libraries are managed according to established procedures
- access to program source libraries is strictly limited to SIT/IT who are required to perform their job functions
- the updating of program source libraries and associated items, and the issuing of program sources to programmers is only performed after appropriate authorization has been received from Sr. Management and Compliance Team

- program listings are held in a secure environment
- an audit log is maintained of all accesses to program source libraries
- maintenance and copying of program source libraries is subject to strict change control procedures.

11.5.2 Technical Review of Applications after Operating System Changes

Prior to the implementation of significant operating system changes (such as software upgrades or patches), application systems must be tested to ensure that the risks of adverse impacts on application security and production capabilities are minimal.

Operating system changes must be implemented through the established change control procedures, including the post-installation verification (see 11.5.1 Change Control Procedures).

11.5.3 Restrictions on Changes to Software Packages

Wherever possible, vendor-supplied software packages should be used without significant modifications.

Where it is deemed essential to modify a vendor-supplied software package, the following rules must be respected:

- The consent of the relevant IAO and vendor must be obtained in advance.
- The associated risks and potential impacts must be assessed, especially if MDINetworX will become responsible for the future maintenance of the software as a result of the change.
- Changes must be applied to clearly-identified copies of the software.
- All changes must be fully tested and controlled (see 11.5.1 Change Control Procedures).
- All changes must be fully documented so that they can be re-applied if necessary following future software upgrades by the vendor.
- The continued effectiveness of built-in application and system security controls must be verified on completion.

11.5.4 Information Leakage

Software must be purchased from trusted sources. This is vital in the case of applications and the associated operating system programs and IT infrastructure supporting critical business processes.

Where the risk of security compromise is assessed as significant, source code should be formally audited for threats, such as backdoors, covert channels and Trojan horse functions as part of Production Acceptance Testing. If this is not possible, formal independent certification of the software (for example, against Common Criteria) is acceptable.

Wherever possible, source code should be obtained and compiled under controlled conditions in-house for production use rather than simply using supplied executable programs. Again, this is vital in the case of applications and the associated operating system programs and IT infrastructure supporting critical business processes.

Access to both source code and executable programs must be controlled for all production software (see 10.5 Operating System Access Control and 11.4.1 Control of Operational Software).

Other controls include intrusion detection/prevention systems and firewalls configured to identify and block unauthorized communications.

11.5.5 Outsourced Software Development

MDI does not outsource any Software Development. In case, if MDI outsources development activities to its vendor then contracts for outsourced software development should specify:

- Requirements for the quality of code, the accuracy of work performed, and the extent of pre- and post-delivery testing
- Compliance with this Information Security Policy Manual, standards, guidelines, and so on, including aspects, such as risk analysis, documented security specifications, quality assurance, change control, installation verification processes, licensing, escrow and intellectual property rights
- MDINetworX's right to audit the development and testing processes
- Liabilities and liquidated damages

11.6 Technical Vulnerability Management

11.6.1 Control of Technical Vulnerabilities

MDI shall ensure plans for security testing activities are developed, implemented, maintained, and reviewed for consistency with the risk management strategy and response priorities.

Timely information about technical vulnerabilities of information systems being used should be obtained, MDINetworX's exposure to such vulnerabilities evaluated and appropriate measures taken to accept or address the associated risks. MDINetworX's compares the results from previous vulnerability scans in order to verify that vulnerabilities have been remediated in a timely manner

Specific information needed to support technical vulnerability management should be recorded in the information asset inventory (see 6.1.1 Inventory of Assets) including software vendors, versions, state of deployment (for example, what software is installed on what systems) and IAOs for significant software assets.

MDI shall identify and document all assets including information assets that contains ePHI, PII whether it is stored in an encrypted or unencrypted format. The asset inventory shall include the network address, machine name or the host name, purpose of the system, asset owner and the department the asset is allocated to. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organizations network.

The asset inventories include all information necessary to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and a business value. The inventory does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned. Records of property assigned to employees is reviewed and updated annually. The record is be used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department.

MDI shall ensure that the above inventory of assets shall not be duplicated. The ISO shall have the final copy of the asset inventory. The ISO shall share the asset inventory once in six months with the administrative and the IT teams for verifying if any changes in the assets have occurred and the corresponding team would reply to the email with the changes. ISO will again maintain the final copy of the asset inventory.

While conducting vulnerability and penetration tests, ensure risks related confidentiality, integrity, and system availability are not compromised.

MDI shall get the vulnerability tests performed by its IT team at least annually for all the below:

- Switches
- ADC/DC
- Firewall
- SFTP
- Application servers (Golem/PMS)

Further, MDI shall ensure that all critical and high vulnerabilities shall be resolved if there is no risk allocated with such resolution.

MDI shall ensure that it:

- determines the causes of the vulnerabilities
- evaluates the need for actions to ensure that vulnerabilities do not recur –*MDI implements vulnerabilities that are critical in nature.*
- determines and implements appropriate corrective action - *This can be achieved by implementing the suggestion points in the vulnerability report.*
- reviews the corrective action taken – *This can be verified by checking that the same vulnerabilities are not repeated*.

Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities:

- IT operations, in conjunction with Information Security, are responsible for vulnerability monitoring, risk assessment, patching, asset tracking, and coordination.
- The ESO is responsible for maintaining adequate information sources for technical vulnerabilities including IT vendors and various trusted third parties, such as Qualys and CERT.
- Potentially relevant technical vulnerabilities should be risk assessed to determine whether changes are needed (such as patching systems or applying other compensating controls/workarounds, such as disabling ports/services, applying additional monitoring, or making procedural changes), and if so, to establish the timescales and responsibilities.
- Depending on the risk and hence urgency, normal change management, emergency change or information security incident response procedures should be followed (see 11.5.1 Change Control Procedures and 12.2 Management of Information Security Incidents and Improvements). Such decisions should be reviewed if risks change (for example, exploits begin circulating, further information on the vulnerability is released or new

information comes to light on the potential impacts), implying that the risks need to be monitored until the situation is resolved. High risk systems should be prioritized if possible.

- The risks associated with installing patches should be assessed against the risks arising from the vulnerabilities, and appropriate testing undertaken accordingly.

Activities and risk management decisions in response to technical vulnerabilities should be recorded for possible management review and post-event learning.

The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency. Also, training on the same for any new IT personnel shall be provided in case if the IT personnel is not much aware of the vulnerabilities.

MDI shall ensure plans for security testing, training, and monitoring activities are developed, implemented, maintained, and reviewed for consistency with the risk management strategy and response priorities. The vulnerability tests shall be performed at least once every 6 months. The security trainings shall be included in the ISMS & HIPAA trainings and shall be provided once in each year. The Compliance team shall continuously review the vulnerability report and will highlight the same to the Compliance Lead if any systems are reported in the vulnerability report.

The Compliance Manager reviews testing, training and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

MDI shall ensure that it maintains a documented list of authorized users of information assets.

11.6.2 Website Vulnerabilities and Threats

- SQL Injections: MDI shall use at least one of the following process in order to avoid SQL Injections
    - Use of Prepared Statements (with Parameterized Queries)
    - Use of Stored Procedures
    - Allow-list Input Validation
    - Escaping All User Supplied Input
    - Enforcing Least Privilege
- Cross-site Scripting : MDI shall ensure to follow the below guidelines in order to avoid XSS
    - Never Insert Untrusted Data Except in Allowed Locations
    - HTML Encode Before Inserting Untrusted Data into HTML Element Content
    - Attribute Encode Before Inserting Untrusted Data into HTML Common Attributes
    - JavaScript Encode Before Inserting Untrusted Data into JavaScript Data Values
    - CSS Encode and Strictly Validate Before Inserting Untrusted Data into HTML Style Property Values
    - URL Encode Before Inserting Untrusted Data into HTML URL Parameter Values
    - Sanitize HTML Markup with a Library Designed for the Job
    - Avoid JavaScript URLs
    - Prevent DOM-based XSS
    - Use HTTP Only cookie flag
    - Implement Content Security Policy

  - Use an Auto-Escaping Template System
  - Properly use modern JS frameworks
  - X-XSS-Protection Header
- Credential Brute Force Attacks : MDI shall ensure to follow the below process in order to avoid Brute Force attacks
  - Limit failed login attempts
  - Make the root user inaccessible via SSH by editing the sshd_config file
  - Don't use a default port, edit the port line in your sshd_configfile
  - Use Captcha
  - Limit logins to a specified IP address or range
  - Two factor authentication
  - Unique login URLs
  - Monitor server logs
- Website Malware Infections & Attacks : MDI shall ensure to follow the below
  - Install anti-virus and anti-spyware software
  - Use secure authentication methods
  - Use administrator accounts only when absolutely necessary
  - Keep software updated
  - Control access to systems
  - Adhere to the least-privilege model
  - Limit application privileges
  - Implement email security and spam protection
  - Monitor for suspicious activity
  - Educate your users
- DoS/DDoS Attacks : MDI shall ensure to follow the below
  - Buy More Bandwidth
  - Build Redundancy into Your Infrastructure
  - Configure Your Network Hardware Against DDoS Attacks
  - Deploy Anti-DDoS Hardware and Software Modules
  - Deploy A DDoS Protection Appliance
  - Protect Your DNS Servers

11.7 Configuration Management

11.7.1 Baseline Configuration

The access to Configuration Management is restricted to IT Team. MDI must develop, document and maintain a current baseline configuration of the information system. The organization must review and update any baseline configuration changes within the information system.

As part of its baseline MDI's operating systems shall have in place supporting technical controls as provided below:

- Sophos Antivirus

- Sophos DLP
- The access to MDI's network shall only be granted through MDI's Firewalls
- Port filtering using group policies
- Audit logging as stated in "IT015-Security Audit, Logging & Monitoring Policy"

Along with maintaining a baseline configuration, the organization shall:

- Retain previous five versions of the baseline configuration for a rollback if necessary.
- Maintain a baseline configuration for development and test environments that is separate from the operational baseline configuration.
- Vendor supplied software used in operational systems must be maintained at a level supported by the supplier, and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application. The organization maintains information systems according to a current baseline configuration and configure system security parameters to prevent misuse.

11.7.2 Configuration Change Control

Updating of the operational software, applications, and program libraries are being performed by authorized IT administrators and operational systems should only hold approved programs or executable code (i.e. no development code or compilers).

If MDI is required to perform changes to mobile device operating systems, patch levels, and/or applications then the formal change management process shall be followed. For formal change management process refer to section 9.1.2 Change Management of the same document.

MDI must determine the types of changes required to the information system that are configuration controlled. There must be systematic proposal, justification, implementation, test/evaluation, review and disposition of changes to the system, including upgrades and modifications.

The changes shall be proposed by IT personnel along with justification, implementation, test/evaluation plans. The Sr. Management shall review the entire change request and only upon approval from the Sr. Management, the IT team shall continue with the change process.

If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the MDI IT Team must show evidence of a formal migration plan which shall be approved by Sr. Management to replace the system or system components.

MDI shall use centralized tool as the configuration control system to keep control of all implemented software as well as the system documentation. Previous versions of application software are retained as a contingency measure. Old versions of software are retained in the centralized tool along with all required information and parameters, procedures, configuration details, and supporting software for as long as they are required and would be shredded only upon the Directors approval. MDI compares the results from previous vulnerability scans in order to verify that vulnerabilities have been remediated in a timely manner Refer Annexure 1 of "GRC006- Retention Policy".

The SIT Managers who are responsible for application systems DocGem (PMS) and Golem are also responsible for the security of the project or support environment and they shall ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment. Further, project and support environments are strictly controlled. All application changes shall only be performed post receiving approval from Sr. Management.

Any decision to upgrade to a new release takes into account the business requirements for the change, and the security and privacy impacts of the release. The organization shall:

- Verify changes to the system take into account the security related issues
- Tests, validate and document changes to the information system before implementing changes on the operational system
    - Testing should not interfere with the information system operations
    - The individual/group conducting the testing must be aware of the all information security policies and procedures, and the specific health, safety and environmental risks associated with a particular facility and/or process.
    - Once the testing is passed on the testing environment system, the change would be initially implemented on few systems from the operations. In case, if there are no deviations/issues highlighted, then the same is being implemented on all the production systems.
    - Tests must be scheduled during planned system outages time
- Retain and review the documentation of every approved configuration-controlled change to the system
- Notify the Sr. Management and the Information Security Officer prior to conducting a change to the information system.
- An audit log is maintained of all updates to operational program libraries.
- Document the rollback strategy in the change ticket before changes are implemented
- In case, if the upgradation/change does not satisfy the requirements or is creating error or bugs, then the change shall be immediately revoked / rolled back to the previous version so that there is no harm in the system.

All the changes shall be managed strictly and consistently and by following the change management process as defined in “SIT004- Change Management Policy”. Further, formal management responsibilities and procedures are in place to ensure satisfactory control of all changes to equipment, software or procedures, including:

- the identification and recording of significant changes;
- the planning and testing of changes;
- the assessment of the potential impacts, including security impacts, of such changes;
- the formal approval for proposed changes; and
- the communication of change details to all relevant persons

The above said change process shall be applicable to all the assets used by MDI as documented below but are not limited only to these assets:

- Desktops

- Servers
- Laptops
- Mobile Phone
- Switches
- Wi-Fi Routers
- Routers
- Firewall

11.7.3 Access Restrictions for Change

The organization must define, document, approve and enforce physical access restrictions associated with any changes to the information system. The organization shall:

- Only allow qualified and authorized IT personnel to obtain access to information system components for purposes of initiating changes, upgrades, or modification.
- Record any access during a configuration change must be implemented to monitor any unauthorized change to the information system. Once the information system change has been executed, audits must be performed to verify that no unauthorized changes have occurred.
- Not allow the installation of unlicensed or unauthorized software.

11.7.4 Configuration Settings

The organization must establish and document configuration settings for information technology products within the information system that are most restrictive and consistent with operational requirements. Any deviation from standard configuration settings must be identified, documented, and approved before implementation into the production environment. The organization shall:

- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
- Incorporate detection of security related configuration changes for tracking, monitoring, correcting and archival purposes.

11.7.5 Least Functionality

The organization must provide only essential capabilities and specifically prohibit or restrict the use of certain functions, ports, protocols and/or services. All functions and services provided by the organization must be carefully reviewed to determine if necessary for the production environment. All unnecessary functions, ports, protocols and/or services must be eliminated.

11.7.6 Configuration Review

The organization shall perform annual checks on the technical security configuration of the systems using Desktop Central. The IT personnel shall extract the log report and shall share the same with the compliance lead. Compliance lead shall review and revert back in case if there are any deviations. If any non-compliance is found as a result of a technical security configuration compliance review, the organization:

i. determines the causes of the non-compliance;

ii. evaluates the need for actions to ensure that non-compliance do not recur;
iii. determines and implements appropriate corrective action; and
iv. reviews the corrective action taken.

11.8 System and information integrity

The following standards apply to, and represent, the security controls established to meet an acceptable level of protection for MDI's information systems. They serve as the base set of procedural requirements that are implemented to provide system and information integrity.

(a) Flaw Remediation
(b) Malicious code protection
(c) Information System monitoring
(d) Security Alerts, Advisories and Directives
(e) Security function verification
(f) Software, firmware and Information integrity
(g) Spam protection
(h) Information input validation
(i) Error handling
(j) Information handling and retention
(k) Memory protection

All the above-said points are already covered in various sections of the policy and thus have not been detailed in this section.

MDI shall ensure that it has:

(xi) Developed and documented systems and information integrity policy and procedures
(xii) disseminated the system and information integrity policy and procedures to appropriate areas within the organization
(xiii) reviewed and updated defined system and information integrity requirements at least once in each year.

12. Information Security Incident Management

12.1 Reporting Information Security Events and Weaknesses

12.1.1 Reporting Information Security Events

The Privacy and Security Officers must work with HR, Workplace Services, and managers to implement and maintain procedures for reporting and responding to incidents related to facility, network, system, or data security. All the requirements specified in this policy meets the guidelines as stipulated by HIPAA omnibus and HITECH act. Further, the requirements of HITECH is covered during the annual HIPAA trainings.

Further, as per the HITECH breach notification process:

HHS issued regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached.

These “breach notification” regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The regulations, developed by OCR, require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

“This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care. These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information,” said Robinsue Frohboese, Acting Director and Principal Deputy Director of OCR.

The regulations were developed after considering public comment received in response to an April 2009 request for information and after close consultation with the Federal Trade Commission (FTC), which has issued companion breach notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA.

To determine when information is “unsecured” and notification is required by the HHS and FTC rules, HHS is also issuing in the same document as the regulations an update to its guidance specifying encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information.

Further as per HIPAA Omnibus:

The Department of Health and Human Services (HHS) released the HIPAA Omnibus rule on January 17, 2013 designed to give patients additional rights to their health information and increase penalties to organizations that fail to protect Personal Health Information (PHI). The rule goes into effect on March 26, 2013 and it includes some changes to data breach response requirements.

HIPAA required covered entities to conduct a risk assessment when a data breach occurs. The risk assessment would determine whether the breach impacted an individual enough to require notification. If the risk assessment determined that the risk was low then the covered entity did not need to notify the individuals nor the Office of Civil Rights (OCR). According to HITECH Answers, the HIPAA Omnibus rule now requires that covered entities retain documentation on the risk assessment performed that could be provided to the OCR if their decision not to notify is called into question, in other words, a burden of proof. If the OCR finds that the covered entity did not meet the burden of proof, it may find the covered entity to be negligent and fine them accordingly or require them to perform corrective action. The rule also adds new requirements for determining the harm to the individual.

Also of interest to HIPAA data breaches is the revised language that broadens the definition of business associates to include more downstream providers who touch PHI. This increases the number of companies that will need to adhere to the HIPAA requirements. These companies will need to become compliant before the rule takes effect but many may not even be aware that they will soon be subject to HIPAA.

Employees can make complaints and/or changes concerning the information security policies and procedures or the organization's compliance with the policies and procedures by emailing the details to CIMT@MDINetworX.com. The employees shall report any incident that they observe without fear of repercussion.

MDI has a point of contact established for the reporting of information security events – Dhanashri Oza (ISO). It is ensured that Dhanashri Oza is known throughout the organization, is always available and is able to provide adequate and timely response. Further, MDI assigns Dhanashri Oza as responsible for sharing information and coordinating responses and has the authority to direct actions required in all phases of the incident response process.

The Compliance team shall provide security incidents knowledge to all the new hires during their HIPAA trainings.

All associates, contractors, and third-party users must be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures should include the following:

- Suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed
- Information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event
- The correct behavior to be undertaken in case of an information security event, that is:
    - Noting all important details (for example, type of non-compliance or breach, occurring malfunction, messages on the screen, strange behavior) immediately
    - Not carrying out any own action, but immediately reporting to the point of contact
- Reference to an established formal disciplinary process for dealing with associates, contractors or third-party users who commit security breaches

This policy refers to the specific procedures and programs to address incidents and also refer to a forensic program. Procedures are developed to provide for the definition and assessment of information security incidents (e.g., an event/incident classification scale to decide whether an event classifies as an incident), roles and responsibilities, incident handling, reporting and communication processes.

The organization formally assigns job titles and duties for handling computer and network security incidents to personnel with designation Assistant Manager and above from IT department and ISO will support the incident handling process by acting in key decision-making roles.

Incident management includes feedback to individuals or organizations reporting an incident, tools to support incident management activities, references to possible sanctions, plain language communications to stakeholders (e.g., law enforcement and third-party organizations or individuals affected by a breach). MDI doesn't have a automated workflow for handling incidents and are relying on emails. Any complaint received on cimt@mdinetworx.com will be treated on priority.

Further, to verify whether an event reported to the CIMT is an actual incident. MDI shall collect necessary evidences as soon as possible after the receipt of the email.

Information security events and incidents can be as provided below:

Incident Categories	Impact
Impermissible disclosure of EPHI	Extreme High
Loss of service, equipment or facilities	Medium
System malfunctions or overloads	Medium
Human errors	Low
Non-compliances with policies or guidelines	Low
Breaches of physical security arrangements	High
Uncontrolled system changes	Medium
Malfunctions of software or hardware	Medium
Access violations	High

The above list will be updated as and when the ISO becomes aware of new incident category.

To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (see 12.2.3 Collection of Evidence).

Process to Report a Phishing Attack

In our commitment to maintaining a secure information environment, it is essential that every employee is vigilant and prepared to respond to potential phishing attempts. The following process outlines the steps to report a phishing attack:

1. Initial Identification of Phishing Attempt:

When you receive an email that appears suspicious or potentially a phishing attempt, be attentive to common indicators, including:

- An unknown sender or an unusual sender address.
- Unexpected or unsolicited attachments or links.
- Content that evokes urgency, fear, or curiosity.
- Poor grammar or unusual language.
- If any of these signs are present, exercise caution.

2. Do Not Interact:

- Under no circumstances should you interact with a suspicious email. Do not open attachments, click on links, or reply to the message.

3. Isolate the Email:

- If you suspect an email to be a phishing attempt, promptly isolate it from your regular email folder. Move it to the spam or quarantine folder if available. This step is crucial to prevent accidental interaction with the email.

4. Reporting Methods:

- There are two primary methods for reporting a phishing attack:

a. Email Reporting:

Compose a new email addressed to your organization's dedicated phishing reporting address (e.g., "itteam@mdinetworx.com").In the email, provide the following information:

The sender's email address.

The subject line of the suspicious email.

Any details about attachments or links within the email.

You can attach the suspicious email as an attachment if it's safe to do so.

b. Incident Ticket Submission:

Visit your organization's incident management system or helpdesk portal.

Create a new incident ticket, selecting "Phishing Attack" as the incident type or category.

Provide detailed information about the incident, including the sender's email, subject, and any attached files or links.

12.1.2 Reporting Security Weaknesses

Workers should note and report any observed or suspected security weaknesses in, or threats to, IT systems or services to their managers and/or to the Service Desk as soon as practicable.

Workers must not themselves attempt to “explore”, “evaluate”, “confirm” or “prove” suspected weaknesses which might result in the following:

- Lead to serious security breaches
- Interfere with forensic analysis
- Be interpreted as a deliberate misuse of the system and result in disciplinary or legal action.

Similarly, workers must not attempt to repair or deal with software malfunctions unless explicitly instructed to do so by the Service Desk. Competent IT professionals explicitly authorized by management to evaluate and deal with security issues, software malfunctions, and so on, will normally be mobilized by the Service Desk.

12.1.3 Reporting Insider Threat

Employees should note and report any observed or suspected insider threats in, or threats to the organization to their manager and/or to the Information Security Officer as soon as practicable.

Few of the examples of the insider threats are:

(f) Frequent access of workspace outside of normal working hours. Either the HR or the compliance lead can observe this during reviewing the physical access. However, if any employee notices such behavior in other employees, they shall immediately highlight the same.
(g) Requests for clearance or higher-level access without need. This can be observed by any of the managers while approving the access requests that they receive.
(h) Irresponsible social media habits. No employee is authorized to post anything regarding the organization or any other employee on any of the social media. If any employee observes this, they are requested to highlight this to the ISO on priority.
(i) Behaviours that demonstrate sudden affluence without obvious cause, such as large pay raise, inheritance, etc.
(j) Maintaining access to sensitive data after termination notice
(k) Use of unauthorized external storage devices
(l) Visible disgruntlement toward employer or co-workers
(m) Chronic violation of organization policies
(n) Decline in work performance

MDI has implemented an insider threat program, which includes security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. If any insider threat incident has been received, the ISO will coordinate this with the HR and the corresponding reporting manager on whom the incident has been registered and come to a conclusion post verifying the actual incident and the corresponding evidences.

12.2 Management of Information Security Incidents and Improvements

12.2.1 Responsibilities and Procedures

Incident management responsibilities and procedures must ensure a quick, effective and orderly response to all types of information security incidents including the following:

- Availability failures – for example, loss of IT services resulting from information system/network failures or denial of service attacks
- Integrity failures – for example, system or network dysfunction caused by viruses and worms; misuse of systems
- Confidentiality failures – for example, unauthorized disclosure of or access to sensitive information

Incidents may happen at any time of day or night; therefore, response processes must provide round-the-clock coverage through shift operations and/or on-call responses.

Extending contingency and disaster recovery plans that are designed to recover IT systems or services as quickly as possible (see 13 Business Continuity Management), incident response procedures should cover the following:

- Analysis of reported security events and weaknesses (see 12.1 Reporting Information Security Events and Weaknesses) and monitoring of systems, alerts and vulnerabilities (see 9.10.2 Monitoring System Use) in order to identify and prioritize security events that appear to indicate actual incidents or near-misses
- Containment (for example, disconnecting affected systems from the network pending further analysis)
- Analysis and identification of the causes of incidents (“What happened exactly? Who and which IT assets were involved? Which controls were missing or failed? What damage was caused to the business?”)
- Planning and implementation of remedies to prevent recurrence, if necessary (“What should we do to prevent this from happening again?”)
- Communication with those affected by or involved in the recovery from incidents, including management and where appropriate external authorities (see 12.1.1 Reporting Information Security Events)
- Applying the learning from incidents to achieve continuous improvement in our ability to manage information security risks (see 12.2.2 Learning from Information Security Incidents)

Log files, audit trails and similar forensic evidence must be collected and secured carefully, as appropriate, for the following purposes:

- Internal problem analysis
- Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, for example, under computer misuse or data protection legislation

It is particularly important that computer evidence which may potentially be required for subsequent legal action is collected and stored securely in accordance with the applicable rules of evidence (see 12.2.3 Collection of Evidence).

Action to recover from security incidents and correct system failures must be carefully controlled, ensuring that:

- Only authorized workers are allowed privileged access to live systems and data for the purposes of diagnosing and resolving security incidents
- Emergency actions taken are fully documented, reported to management and reviewed in an orderly manner
- The integrity of business data, systems and security controls are reconfirmed as soon as possible so that normal use may resume

Balancing the desire to restore service against the need to (a) evaluate the causes of an incident, (b) resolve any control failures and (c) gather evidence of a breach, is a matter of judgment by the relevant IAO, on advice from the ESO, Risk, Legal, and other functions.

MD I shall ensure that this Information Security Policy Manual is :

- formally documented
- protected – by keeping it in the location where only the compliance team and Sr. Management has access
- controlled – by maintaining version numbers along with the changes that are being made on the document
- retained according to federal, state and organizational requirements.

The Information Security Policy Manual also incorporates a Plan, Do, Check, ACT (PDCA) cycle for continuous improvement in this document, particularly as information is obtained that could improve the Information Security Program, or indicates any shortcomings of the Information Security Program.

MDI shall ensure that reports and communications are made without unreasonable delay and no later than 30 days after the discovery of the incident, unless otherwise stated by law enforcement in writing or orally. If the statement is made in writing, the notification is delayed for the time specified by the official. Incident reports include a description of the event, the date of the breach and date of discovery, a description of the types of information involved, recommended steps for individuals or organizations affected by the incident, the steps the organization has or will take to address the incident or breach, and organizational point of contact information.

Roles and Responsibilities:

ISO (Information Security Officer):

- ISO shall ensure to collect all the evidences that will ensure that the event highlighted is an actual incident.
- If the incident is actual, ISO shall immediately notify the Sr. Management about his/her observations
- ISO shall block all the accesses of the user responsible for the incident until the investigation or the incident process is complete
- Proper documentation shall be maintained for each activity carried by the ISO
- ISO shall provide proper feedback to the individuals reporting the event/incident
- ISO shall determine the RCA and bring an effective precautionary measure to avoid such scenarios in future
- ISO shall recommend the further course of action to the Sr. Management.

Sr. Management :

- Sr. Management shall review the evidences collected by the ISO and shall guide him/her to the right direction
- Sr. Management shall ensure that ISO has been provided with freedom to grab the evidences and receives complete co-operation from other departments
- Sr. Management shall ensure that strict disciplinary action would be taken against the users who doesn't co-operate with this investigations
- Sr. Management shall review the actions proposed by ISO and approve/provide feedback on the same.

- Once the event is proved to be an incident, it should be communicated to all the managers of the organization
- If the incident affects any of the client/vendor then the same shall be communicated to them within 24 hours once it is decided that the event is an actual incident

12.2.2 Learning from Information Security Incidents

Security incidents should be analyzed to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, and possibly changes to this Information Security Policy Manual (see 4.1.2 Review of the Information Security Policies).

Taking confidentiality into account (for example, having removed details of the individuals involved or other sensitive information), information security incidents may be used for security awareness purposes (see 7.2.2 Information Security Awareness, Education, and Training).

12.2.3 Collection of Evidence

Suitable evidence must be collected, retained, analyzed, and presented following documented procedures in compliance with the applicable rules for evidence covering admissibility (whether or not the evidence can be used in court) and weight (the quality and completeness) of evidence. We must for example maintain the chain of custody.

MDI shall ensure that it maintains a list of employees involved in security incident investigations and the resulting outcome.

To adhere to regulatory requirements and ensure the availability of historical incident data, incident logs will be retained for a period of three years. This retention period facilitates compliance, analysis, and auditing activities, ensuring the preservation of valuable information for the continuous improvement of our information security management system

12.2.4 Testing of Incident Response procedures

MDI shall ensure that it performs test for its incident response procedures at least once in each year. The organization creates a dummy scenario and creates workaround with what action would have been taken if any such incident is being observed.

12.3 Incident Management Process

- The Compliance team shall provide security incidents knowledge to all the new hires during their HIPAA trainings.
- Currently the security/information incidents are categorized as below:
  - **a. HIPAA Breach**
    Any incident that is non-compliant as per HIPAA privacy rule is considered as HIPAA Breach.
    Example: Writing PHI data on a notepad/paper.
  - **b. Physical Security Breach**
    Associate/vendor entering operations floor without an ID card/temporary/visitor badge are few of the examples of Physical Security Breach
  - **c. Unauthorized Network Access**
    Associate having access to network folder that is not required to perform his duties is one of the example of unauthorized network access
  - **d. Loss/Theft of Confidential Documents**
    Employee file being misplaced is one of the example of Loss/Theft of Confidential Documents
  - **e. Other (system failure or loss of service, malicious code, denial of service, errors, unauthorized disclosures of covered information, system misuse, unauthorized wireless access points, and identity theft)**

- If any employee notices any incident either belonging to him/her or with any other employee, he/she shall notify the CIMT (Corporate Incident Management Team) through sending an email to CIMT@MDInetworx.com
- It is the responsibility of the employee to report any incident that they notice on the same day of the incident or at least within 24 hours of the incident being observed.
- Compliance Lead will immediately enter the details of the incidence from the email in the Helpdesk tool.
- Once a ticket is raised, it is initially assigned to the Compliance Lead. It is the responsibility of the compliance lead to respond to the incident within 24 hours. He shall identify whether the incident raised by the associate has actually occurred. If the incident has not occurred, the Compliance Manager shall reject the ticket. If the incident has occurred, the Compliance Manager shall review the priority (and change the priority if required) of the incident and change the status of the ticket from "Open" to "In Process".
- Actions shall be taken based on the priority of the incident.
- If the priority of the ticket is "High", then action to be taken immediately and the incident shall be resolved on/before 1 hour.
- If the priority of the ticket is "Medium", then the incident shall be resolved on/before 1 day.
- If the priority of the ticket is "Low", then the incident shall be resolved on/before 1 week.
- **Priority Matrix**: -

  For High priority incidents, the ticket status shall be changed from "Open" to "In process" within 15 minutes, if not then the employee shall immediately refer escalation matrix provided in this document to escalate it to the next level.

  For Medium priority incidents, the ticket status shall be changed from "Open" to "In process" within 4 hours, if not then the employee shall immediately refer escalation matrix provided in this document to escalate it to the next level.

  For Low priority incidents, the ticket status shall be changed from "Open" to "In process" within a day, if not then the employee shall immediately refer escalation matrix provided in this document to escalate it to the next level.
- Once the incident is closed, the CIMT shall conduct a final meeting and update the "Security Incident Intake Form" available with the Compliance Manager.
- For each incident raised the Root Cause shall be determined and shall be emailed to all the CIMT members along with the Corrective and/or Preventive actions.

- On a weekly basis, the compliance team verifies if any incidents have occurred and prepares a consolidated report and shares the same with the Sr. Management. If any incident(s) has occurred then the corresponding status shall be highlighted. In addition to the incidents occurred, the compliance lead shall review all the historical incidents along with its corrective action plan to verify that the corrective action is working as per the requirement.
- MDI shall maintain a list of employees involved in security incidents with the resulting outcome from the security incident investigations.
- If there is any incident observed, the incident response program shall also include, analysis and identification of the cause of the incident, containment, increased monitoring of system use, planning and implementation of corrective action to prevent recurrence.
- MDI shall follow the below phases for the entire process:
    - The user shall raise the incident on the MDI Ticketing Tool
    - Compliance Lead to verify the incident. In case, if the compliance lead is not reachable, anyone from the CIMT team shall verify the incident.
    - CIMT meeting to be scheduled and discussion on the action plan
    - Taking appropriate action including disciplinary action
    - Updating the incident intake form and closing the incident ticket
- The Information Security Officer (ISO) is the person responsible for coordinating incident responses and has the authority to direct actions required in all phases of the incident response process if the action is limited to employees/assets inside the organization. However, the authority to direct actions to external agencies (including government authorities) is only available with the Directors of the organization.
- MDI shall ensure that none of the workforce members would interfere with federal or state or government investigations or disciplinary proceedings through willful misrepresentation or omission of facts or by the use of threats or harassment against any person. In case, any of the employee is observed interfering with the investigations or disciplinary proceedings then strict action would be taken against the employee including termination.
- The information gained from the evaluation of information security incidents shall be used to identify recurring or high-impact incidents. The incident response and recovery strategy shall be updated in the "Incident Report Consolidated" report. In case of recurring incidents, the recovery strategy shall be revisited and improved recovery strategy shall be considered so as to reduce the recurrence.
- If the reported incident is observed to be actual incident then the corresponding stakeholders shall be reported. This reporting also includes notifying internal and external stakeholders, the appropriate Community Emergency Response Team and law enforcement agencies in accordance with all legal or regulatory requirements for involving that organization in computer incidents.
- Employees and other workforce members, including third-parties, are able to freely report security weaknesses (real and perceived) without fear of repercussion.
- MDI's incident responses are formally managed and include, but not limited to, the following elements:
    (i) collecting evidence as soon as possible after the occurrence
    (ii) conducting information security forensic analysis, as required
    (iii) escalation, as required
    (iv) ensuring that all involved response activities are properly logged for later analysis
    (v) communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know
    (vi) dealing with information security weakness(es) found to cause or contribute to the incident
    (vii) once the incident has been successfully addressed, formally closing and recording it.

Escalation Matrix:

Level	Name	Role	Response Time	Email ID	Mobile #
Level 1	Prasad Pawar	Manager – IT	24 hours	prasadpa@mdinetworx.com	+91 9552588517
Level 2	Abhijit Pardeshi	Director - Information Technology	6 hours (post escalated to level 1)	abhijitp@mdinetworx.com	+91 9011036942
Level 3	Dhanashri Oza	Information Security Officer	2 hours (post escalated to level 2)	dhanashrio@mdinetworx.com	+91 7391094900

MDI adheres to the HIPAA Omnibus HITECH requirements for responding to a data breach (of covered information) and reporting the breach to affected individuals, media and federal agencies.

Below are the Phases of Incidence Response:

- Incident Reporting
- Allocation of reported Incident
- Allocating the priority for the incident
- Based on the priority of the incident, actions will be taken accordingly
- Collection of Evidence
- Learning from the Incident
- Improvement in the system

A program of business processes and technical measures are established to triage security-related events and handle different types of information security incidents including:

- System failure or loss of service
- Malicious code
- Denial of service
- Errors
- Unauthorized disclosure of covered information
- System misuse
- Unauthorized wireless access point
- Identity Theft

In addition to normal contingency plans, the program also covers, analysis and identification of the cause of the incident, containment, increased monitoring of system use, planning and implementation of corrective action to prevent recurrence.

13. Business Continuity Management

13.1 Information Security Aspects of Business Continuity Management

13.1.1 Including Information Security in the Business Continuity Management Process

A business continuity management process is necessary to reduce the disruption to MDINetworX and MDINetworX hosted clients' information systems caused by disasters and security failures to an acceptable level through a combination of preventative and recovery controls.

MDINetworX maintains physical controls to limit access to MDINetworX facilities to authorized personnel during a disaster recovery event. The Information Security Officer coordinates facility security policy and procedures with the disaster recovery coordinator and the local security coordinator at each designated facility.

The Directors shall have the ownership to run the BCP and have complete authority to change the plan at any time.

Managers and members of the MDINetworX workforce must follow MDINetworX's Security Policies and Procedures at each location regarding access during a disaster recovery process to maintain facility integrity.

Business continuity must be managed consistently throughout MDINetworX, addressing the business dependence on critical business processes by ensuring availability of the supporting IT systems. This implies that business continuity management must extend to all parts of the organization (see 5.1.1 Management Commitment to Information Security).

All the employees shall be trained on the Business continuity plan annually and a copy of the plan shall be provided to employees whose designations are Information Security Officer, Sr. Managers, Managers, Assistant Managers, Deputy Managers, Sr. Solution Architect, Assistant General Manager, Group Leaders, Sr. Project Managers, Associate Directors, System Administrator, Database Administrator and Sr. Management so that the same can be referred in case of any emergency.

All managers and the SPOCs who are required to carry out the BCP plan shall be trained separately on their roles within 90 days of assigning the role in the BCP.

Business continuity management processes should address the following:

- Identify the necessary capacity for information processing, telecommunications, and environmental support is available during contingency operations, e.g., during an information system disruption, compromise or failure
- Identify essential missions and business functions and associated contingency requirements
- Provide recovery objectives, restoration priorities, and metrics

- Address contingency roles, responsibilities, and assign individuals with contact information
- Identify and prioritize critical business processes through a structured plan- organizational Business Impact Analysis (BIA) process involving senior managers, IAOs, Risk Management, and the ESO.
- Identify information assets associated with or necessary for critical business processes (see 6.1.1 Inventory of Assets)
- Identify events that can cause interruptions to MDI's Business processes.
- Based on the Risk Assessment Performed, determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period.
- Based on the results of the risk assessment, a risk treatment plan is prepared and adopted. Further, the business continuity strategy is developed to identify the overall approach to business continuity. Once this strategy has been created, endorsement is provided by Sr. Management
- Clarify the risks of system failures on critical business processes in terms of their likelihood, impact-time profiles, and so on, in order to derive and document availability requirements (see 13.1.2 Business Continuity and Risk Assessment)
- Result in the specification, design, development, testing, and maintenance of suitable control measures for resilience (dual-live configurations, redundant systems and communications with automatic or manual failover, spare capacity, 'over-engineering' of systems, real-time system monitoring and urgent response processes, and so on) in normal operation despite minor incidents, such as hardware failures, and for off-site Disaster Recovery (DR) following whole-of- site disasters and similar serious incidents
- Integrate and align IT resilience and DR arrangements with business continuity plans in accordance with the business continuity strategy (see 13.1.3 Developing and Implementing Continuity Plans Including Information Security)
- Ensure the continuity plans are maintained (meaning updated to reflect changes in the IT and business environments) and recertified regularly against the availability requirements through suitable tests and exercises (see 13.1.5 Testing, Maintaining and Re-Assessing Business Continuity Plans)

13.1.2 Business Continuity and Risk Assessment

Whereas many information security incidents may be predicted based on past experience, some are too rare or inherently unpredictable to enable specific planning. Therefore, conventional scenario-based business continuity planning must be combined with contingency planning techniques to cater for unanticipated eventualities.

BIAs should consider all MDINetworX's business processes, involving the relevant senior business managers and IAOs as well as risk and security experts. BIAs should identify, quantify, and prioritize risks against criteria and objectives relevant to MDINetworX including critical resources, impacts of disruptions, allowable outage times (Recovery Time Objectives), Recovery Point Objectives and recovery priorities.

MDI shall ensure that when new requirements are identified, any existing emergency procedures (e.g. evacuation plans or fallback arrangements) are amended as appropriate.

Depending on the results of the BIAs and Risk Assessments Performed, business continuity strategies and plans should be developed and endorsed by management to define MDINetworX's approach to business continuity.

MDI shall ensure that the recovery and restoration of business operations and establish an availability of information in a time-frame as specified in "Establish Recovery Priorities" in the BCP plan.

13.1.3 Developing and Implementing Continuity Plans Including Information Security

Plans should be developed and implemented to maintain and/or restore operations within required timescales following interruption to, or failure of, critical business processes.

The business continuity planning process should incorporate:

- Identification by business managers and IAOs of maximum acceptable losses of information and services through the BIA process (see 13.1.2 Business Continuity and Risk Assessment)
- Identification and agreement of responsibilities and business continuity procedures
- Implementation of systems and procedures for maintaining/recovering/restoring business operations, information systems and data within required timescales
- Reviews of internal and external business dependencies plus the associated Service Level Agreements and contracts
- Operational procedures to follow pending completion of recovery and restoration of service
- Education of workers in the business continuity, crisis management and recovery procedures, for example through disaster recovery exercises
- Change control/maintenance and periodic testing/exercising of the plans
- Recovery and restoration of business operations and establish an availability of information in a time-frame specified by the organization
- Documentation of agreed procedures and processes
- Testing and updating of at least a section of the plans
- Particular attention is given to the assessment of internal and external business dependencies and the contracts in place

Ownerships:

- For any emergency procedures including but not limited to BCP plan and resumption plans, the compliance manager holds the ownership
- For manual fallback of IT processes, IT manager holds the ownership
- For manual fallback of software processes, SIT Head/Incharge holds the ownership
- For all other fallback processes Compliance manager holds the ownership.

Further, the ownership for any task is allocated only if he/she is the owner for the respective process.

The planning process should focus on business objectives and priorities, for example, restoring client-facing systems within a reasonable period after an unplanned outage. The procedures for obtaining necessary electronic covered information during an emergency is defined. The only covered information that would be required to be restored is the Golem DB which is frequently backed up in the NAS device. If required, the backup will be downloaded and restored within the same day. The services and resources facilitating this should be identified, including IT and non- IT resources as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. Following an interruption to business operations, full information system restoration without deterioration of the security measures originally planned and implemented can be achieved.

Business continuity plans address organizational vulnerabilities and therefore contain sensitive information that must be appropriately classified and protected against unauthorized access, damage or loss.

Business continuity plans should be stored both on- and off-site in order to enable awareness/training and to escape coincident damage affecting the main and recovery locations. Other materials necessary to execute the continuity plans should also be stored on- and off-site as appropriate.

If alternative temporary locations are to be used for disaster recovery, they should be capable of being secured to a level equivalent to the main sites. Sufficient environmental security shall be in place in the offsite location.

Crisis management plans and activities may be different from business continuity management depending on the scale of the event. Most incidents should be accommodated by normal management procedures and resilience measures, whereas serious incidents will require special crisis handling and disasters will further require the invocation of disaster recovery plans. Plans must take account of the fact that health and safety of personnel takes precedence over other activities.

MDI shall ensure that Operations and QA shall be given priority during the Business Continuity activity so that the service deliverables are met. Below physical / logical assets are required to accomplish the Business Continuity plan:

- Backups at Offsite Location (For India: Koregaon Park, Pune; For US: Linthicum, MD) to restore the DB and the application
- 30 Laptops (For India Only)
- 30 keyboards (For India Only)
- 30 mouse (For India Only)
- Data Cables (For India Only)
- 1 Server (For India Only)
- Wireless Access Point

MDI shall ensure that it would automatically switch to the alternative internet service provider if the first ISP fails.

13.1.4 Business Continuity Planning Framework

All business continuity and disaster recovery plans must address information security requirements and satisfy agreed business priorities. The ISO therefore has an important coordination role to ensure that plans are internally and externally consistent.

Each business continuity plan should describe the general approach to ensuring information and systems availability, escalation processes and conditions, as well as the individuals responsible for executing each component of the plan.

When new requirements are identified, emergency procedures, evacuation plans, fallback arrangements, and so on, should be amended accordingly. Changes to business continuity plans and procedures must be proactively managed to ensure that they remain up-to-date and effective (see 13.1.5 Testing, Maintaining and Re- Assessing Business Continuity Plans).

Continuity plans, emergency procedures, manual fallback, and resumption plans for each business department are information assets owned by the respective heads of department. Systems resilience, DR and fallback arrangements for IT and communications facilities belong to the respective IT service providers. For continuity plan and emergency procedures the compliance manager would have the ownership. For manual fallback of IT activities IT manager would have the ownership and for software development, the SIT head would have the ownership. For resumption plans respective process owners would be responsible.

The business continuity planning framework should address the identified information security requirements by:

- Describing the conditions for activating the plans and the processes to be followed (for example, how to assess the situation, who is to be involved)
- Describing emergency actions and crisis management responses to be taken following an incident which jeopardizes business operations or health and safety of personnel
- Fallback procedures describing the actions to be taken to move essential business activities or support services to alternative temporary locations and to restore business processes to operation within the required timescales through disaster recovery arrangements
- Temporary operational procedures to follow pending completion of recovery and restoration (for example, suitable default messages explaining the situation on client contact/voice response systems)
- Resumption procedures describing the actions necessary to resume normal business operations
- Maintenance schedules specifying how and when plans are to be exercised/tested, and processes for reviewing and maintaining plans
- Awareness, education and training activities designed to create understanding and promote effectiveness of the business continuity and disaster recovery processes
- Roles and responsibilities describing who will execute each component of the plan and nominating alternatives as required
- Critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures

13.1.5 Testing, Maintaining and Re-Assessing Business Continuity Plans

Business continuity plans should be tested annually and updated regularly to ensure that they are up to date and effective. This requires effective change management, version control and periodic review processes.

Continuity plans must be reviewed, and if necessary, updated by their owners and/or by the Business Continuity Manager, ESO, or auditors periodically according to the level of risk and business criticality. Continuity plans relating to critical business processes must be reviewed and revalidated by management at least twice a year. Other plans must be reviewed and revalidated by management every year. Change management and version control processes must ensure that updated plans are distributed and re-tested appropriately.

Changes that are likely to require plan updates include:

- Acquisition of new IT equipment or systems upgrades
- New workers including associates, contractors and business partners
- Changes to addresses or telephone numbers

- Changes to business strategies or processes, including dependencies
- Changes of location, facilities or resources
- Legislative or regulatory changes
- Other changes that affect operational, financial or information security risks

Depending on the level of assurance needed by management and the maturity of the plans themselves, techniques to prove that continuity plans will operate correctly if actually employed include:

- Table-top walk-through, discussing the theoretical operation of continuity arrangements
- Technical resilience and DR testing (ensuring information systems either continue operating despite minor interruptions or can be restored effectively following a disaster)
- Recovering systems and checking operations in isolation at DR locations without affecting live operations (parallel testing)
- Exercises simulating particular disaster scenarios (useful for making people more familiar with their post-incident/crisis management roles)
- Testing third party facilities and services against the contracted commitments, in conjunction with the third parties
- Full-scale rehearsals confirming that the organization, personnel, equipment, facilities and processes are fully prepared for any eventuality
- Continuity test results should be recorded and suitable actions taken to improve and revalidate the plans, where necessary.

In addition to the BCP drill, MDI shall also perform Business Impact Analysis annually also consideration shall be given to the outputs of the BCP drills during the BIA.

14. Compliance

14.1 Scope

The scope of this compliance plan applies to all departments except for finance department.

Below are the department for which this compliance plan shall be applicable:

(a) Operations
(b) Quality
(c) IT
(d) SIT
(e) HR
(f) Administration
(g) Sr. Management
(h) Compliance

14.2 Compliance with Legal Requirements

14.2.1 Identification of Applicable Legislation

IAOs must seek advice on applicable legal, regulatory, and contractual obligations from Legal and Compliance Departments. Relevant statutory, regulatory, and contractual obligations must be explicitly defined and documented for each information system. The specific controls and individual responsibilities to meet these requirements must be similarly defined and documented in the system documentation (meaning functional and technical specifications; security designs; installation, configuration, usage and maintenance procedures, and so on). Copies of such documentation must be retained securely for compliance assessment.

In relation to its use of IT, general obligations on MDINetworX include:

- Intellectual property rights applied through copyright, trademarks, patents, registered designs, and so on (see 14.1.2 Intellectual Property Rights)
- Laws and regulations regarding the safeguarding of organizational records, maintenance of data integrity and availability, and so on, especially in relation to the accuracy and timeliness of financial reporting, for example, annual reports and taxes (see 14.1.3 Protection of Organizational Records)
- Data protection and privacy laws protecting the rights of individuals (see 14.1.4 Data Protection and Privacy of Personal Information)
- Laws regarding various forms of computer misuse, fraud, telemarketing/spam, and so on, (see 14.1.5 Prevention of Misuse of Information Processing Facilities)
- Laws relating to the use and export of strong encryption
- Anti-money laundering and other regulations relating to fraud, and so on
- Confidentiality/non-disclosure agreements and various contractual terms (for example, the enforceability of digital signatures)

- Laws and regulations regarding monitoring of the actions of associates and third parties (for example, explicit notification of subjects that monitoring is taking place; rules constraining the use of gathered information for other purposes; limited ability to use information for law enforcement purposes, such as fraud prevention)

14.2.2 Intellectual Property Rights

Management must implement procedures to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights and trademarks.

Management must ensure that MDINetworX associates comply with legislative, regulatory and contractual requirements restricting the copying, use or dissemination of proprietary material. In particular, only information that is developed by and belongs to MDINetworX, licensed or provided by the developer/owner to MDINetworX, or is legally placed without restriction in the public domain, may be used. Management reviews and/or audits should be undertaken in order to confirm compliance with these requirements.

Management must protect MDINetworX's intellectual property rights by imposing similar legal obligations on third parties where applicable, supplementing the mutual trust arising from effective business relationships (for example, third party use of computer programs developed by MDINetworX should be protected through suitable license agreements). The extent of any compliance checking activities undertaken by MDINetworX should reflect management's assessment of the risks, costs and benefits of such checks.

Software Copyright

Commercial software and "shareware" products are usually supplied under license agreements that limit legal use and/or copying.

Commercial software products must be acquired through normal procurement processes, ensuring that management authorize the purchase and evidence of suitable usage and other rights is obtained and retained by MDINetworX. Information asset registers must be maintained to record software licenses (see 6.1.1 Inventory of Assets).

Procedural and/or technical controls should be implemented to ensure compliance with specific license terms, for example, to prevent the maximum permitted number of concurrent users being exceeded.

Management must check periodically that only authorized software and licensed products are installed, using automated software audit tools and/or manual methods.

Trademarks

MDINetworX must avoid infringing third party rights in relation to trademarks, for example by checking proposed MDINetworX trademarks against the official registers and by explicitly acknowledging trademarks belonging to third parties if used in marketing materials, user guides, and so on.

Management should decide whether and where to register trademarks belonging to MDINetworX in order to gain legal protection in the relevant jurisdictions.

Associates must seek advice from Compliance Department if considering licensing or using patented technology belonging to a third party, or if intending to patent an invention on behalf of MDINetworX.

14.2.3 Protection of Organizational Records

Important MDINetworX records, as determined by management through the information classification process (see 6.2 Information Classification), must be protected from loss, destruction, and falsification to the extent necessary to minimize risks to MDINetworX, for example through the use of digital signatures (see 11.3 Cryptographic Controls). Records may be categorized into record types, for example, accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of storage media, for example, paper, microfiche, magnetic, optical.

Some records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples include records that may be required as evidence that MDINetworX operates within statutory or regulatory rules, or to ensure adequate defense against potential civil or criminal action, or to confirm the financial status of an organization with respect to shareholders, partners and auditors. The time period and data content for information retention may be set by national laws or regulations.

Any cryptographic keys associated with encrypted archives or digital signatures (see 11.3.1 Policy on Use of Cryptographic Controls) must themselves be securely archived and made available to authorized persons when needed.

In order to reduce the risk that media used for long-term archival of records may degrade in storage, archive media must be handled carefully and stored in stable environmental conditions according to the media manufacturers' recommendations.

The ability to restore archived data must be tested periodically to ensure the media remain readable. Archived data must be transferred to replacement media as soon as practicable if the bit error rate trend or physical condition indicate the onset of unacceptable media degradation, or if the storage technologies or data formats are becoming obsolete.

Data storage systems must be chosen such that required data can be retrieved in a manner acceptable to the courts, for example, all records required can be retrieved in an acceptable timeframe and format, using cyclic redundancy checks, control totals, and so on, to ensure data integrity and digital signatures for authenticity and non- repudiation (see 11.3.1 Policy on Use of Cryptographic Controls).

The system and processes of storage and handling must ensure clear identification of records and of their statutory or regulatory retention period, and destruction of records after the defined retention period if they are no longer needed by MDINetworX.

To meet these obligations, the following steps must be taken within MDINetworX:

- Guidelines must be issued on the retention, storage, handling and disposal of records and information.

- A retention schedule must be drawn up identifying essential record types and the period of time for which they must be retained.
- An inventory of sources of key information must be maintained (see 6.1.1 Inventory of Assets).
- Suitable physical, technical and procedural security controls must be implemented to protect essential records and information from loss, destruction and falsification, and to prevent unauthorized access.

The Legal department must be consulted if MDINetworX intends to enter into confidentiality or similar non-disclosure agreements or contracts with third parties in order to ensure that the agreements satisfy MDINetworX's requirements in a legally binding manner.

14.2.4 Data Protection and Privacy of Personal Information

Compliance with data protection legislation requires appropriate management controls. The Privacy Officer must provide guidance to IAOs, users, and service providers on their individual responsibilities and the specific procedures that must be followed.

Individuals must be properly informed of their rights if personal data are being collected. Practical examples of this include the following:

- The opportunity to opt-in but default opt-out of marketing communications when supplying contact details for another purpose
- Notification if personal data are to be transmitted to a country where data privacy regulations are less strict
- Users should be notified when telephone conversations, video pictures, or e- mails are being recorded or monitored, for example, by labels fixed to the telephones and/or the playing of recorded audio messages.

Personal data may be disclosed or used in connection with law enforcement activities, fraud prevention, and similar situations, even if this does not fall within the registered purposes. Personal data must not be disclosed to third parties outside the registered purposes unless covered by a valid court order. The Legal department must always be consulted first if a third party demands access to personal data, and should be consulted if personal data are to be used internally for non-registered purposes.

MDI ensures that the public has access to information about the organization's security and privacy activities and is able to communicate with its senior security official and senior privacy official at cimt@mdinetworx.com. This information is publicly available on the MDI's online website.

14.2.5 Prevention of Misuse of Information Processing Facilities

Worker access to MDINetworX's IT facilities and systems is provided for authorized business purposes. Use of these facilities for non-business or other unauthorized purposes is regarded as improper. If such activity is identified by monitoring or other means, the worker's manager should be informed and may result in disciplinary action.

Monitoring usage of IT systems by workers may require them to be advised of such monitoring without their explicit agreement. Advice must be obtained from the Legal department before implementing monitoring procedures and/or technology.

As it may be a criminal offence to use a computer for unauthorized purposes, all MDINetworX and third-party users must be given written authorization to use MDINetworX systems, a copy of which must be signed by the user and securely retained by MDINetworX. Generic obligations to comply with information security policies, and so on, must for example be embedded within employment contracts (see 7.1.3 Terms and Conditions of Employment) and third-party service contracts, while specific obligations may be included on the forms regarding user access to sensitive business systems. Users must be explicitly informed that no access or use of IT systems is permitted unless specifically authorized.

MDINetworX must implement suitable controls to ensure compliance with applicable information security legislation, including where applicable the following:

- Antivirus controls (see 9.4.1 Controls against Malicious Code) and access controls (see 10 Access Control) must be implemented on all applicable platforms, application systems and networks.
- The storage or use of virus-writing, 'root kits' and similar hacking tools on MDINetworX equipment is forbidden unless explicitly pre-authorized in writing by management for legitimate business purposes.
- Intrusion detection systems, security event logging, reviews, and audits of security controls, real-time alarms, and incident response procedures must be used to identify and respond as soon as possible to attacks in progress, whether externally or internally originated.
- At log-on, a standard warning message should be presented to users to the effect that the system being accessed is private and that unauthorized access is not permitted (Legal Department should help specify the precise wording). Users should actively acknowledge the message to continue with the log-on process, especially in the case of systems giving access to highly sensitive information including personal data.

14.3 Compliance with Security Policies and Standards and Technical Compliance

14.3.1 Compliance with Security Policies and Standards

Managers must ensure that all information security procedures within their area of responsibility are carried out correctly.

IAOs must sponsor regular reviews of the compliance of their application systems with this Information Security Policy Manual and the HIPAA Security Evaluation Rule, plus other security requirements.

All areas within the organization must be reviewed, including:

- Information systems (platforms, networks and applications)
- Information systems serviced providers (IT and third parties)
- Information security processes and responsibilities

In addition to these routine reviews, Internal/External Auditors may review compliance against MDINetworX information security policies, standard, guidelines and other good practice from time to time according to their own risk-based audit schedule. Similarly, MDINetworX management may commission ad hoc information security reviews by competent internal or third-party assessors at any time, for example to address the root causes of security incidents (see also 14.3.1 Information System Audit Controls).

Exceptions to this policy manual that have been explicitly approved by the ESO must be reviewed at least annually (see 1.4 Policy Exceptions).

14.3.2 Technical Compliance Checking

Information systems and networks must be regularly checked by Information Security for compliance with relevant technical security standards, security designs, and so on, to ensure the adequacy and effectiveness of the associated hardware and software controls.

Independent specialists (such as qualified IT auditors or third-party experts) must carry out technical auditing under the authority and supervision of MDINetworX management, supported as necessary by technical staff and others. As with the policy reviews noted above, this should involve a combination of routine and ad hoc reviews. Such reviews must be designed, performed and controlled in such a way as to minimize adverse impacts on production services, while generating valid and useful information on actual or potential security vulnerabilities (see also 14.3.1 Information System Audit Controls).

14.4 Information Systems Audit Considerations

14.4.1 Information System Audit Controls

IT systems, processes, and controls must be regularly audited by independent auditors in accordance with defined audit standards and procedures. In addition to the independent audits, MDI shall also conduct internal audits on its information security management once in each year.

IT audit assignments must be scheduled using a risk-based planning process. The scope of IT audits must be defined by audit managers and agreed with IAOs and/or other managers as applicable.

Audits involving checks on production systems and networks must be carefully planned in conjunction with management to minimize the risk of disruption.

Reasonable IT resources for performing audits and reviews (such as access to systems, data, technical staff, procedures, and so on, and any special processing or reports) must be identified by the auditors, agreed and made available by management.

Wherever possible, auditors must be limited to read-only access to the production networks, systems and data being audited unless otherwise justified and approved by management.

Auditor access to production systems and networks must be monitored and securely logged in the same way as any other user.

If necessary, audit utilities, test scripts, and so on, must be verified and uploaded on behalf of the auditors by system administrators. Requirements for special or additional processing must be agreed with management where it may impact production services.

Any information copied for further examination must be erased when the audit is completed, unless it is to be retained as audit evidence (in which case it must be at least as well protected as the original information).

In addition to audits, non-audit reviews or assessments of IT systems, processes or controls may be commissioned at any time by IAOs or managers for a variety of purposes. Management must control and monitor the execution of such reviews according to their purpose. The scope, process and reporting of such reviews must be as determined by management. Such reviews must not be called audits unless they are performed by independent and competent auditors following defined audit processes (see above).

MDI shall ensure that it gets assessed by Third-Party annually for the below certificates/Reports:-

- ISO 27001
- SOC2 Type2
- HiTrust

14.5 Contact Details of the Senior Privacy Official

Below are the contact details of the Senior Privacy Officer / Data Privacy Officer / Information Security Officer:

Name: Dhanashri Oza
Mobile: +91 7391094900
Email: dhanashrio@mdinetworx.com

Anyone with query/concern on any of our compliance policies and/or need to highlight any incident and/or for answering your security questionnaire can contact the above-mentioned personnel.

15. Information Security Workforce Development and Improvement program

MDI's Information security workforce development and improvement program include:

(i) defining the knowledge and skill levels needed to perform information security duties and tasks
(ii) developing role-based training programs for individuals assigned information security roles and responsibilities
(iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions.

MDI's Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

15.1 Knowledge and skill levels needed

MDI shall ensure that the ISO shall be at least graduated in Computer Science with a minimum of 2 years experience in US Healthcare domain (Any Role) and Compliance (Any Role).

15.2 Role based training

The ISO shall provide the role-based training to all the required resources who is assigned the role in Incident Management, BCP and Information security within the first 30 days of their joining and at least once in each year thereafter.

Objective:

- It ensures that relevant training is delivered for the specific roles
- It helps the employees who have been assigned specific duties to gain a deeper knowledge through relevant information
- Employees feel that the training is specially developed for their role which boosts their confidence

Scope:

The initial role-based training during the time of joining is provided to resources who have been assigned specific roles in either Incident Management, BCP and/or Information security. Further, the annual role-based training is extended to all the employees with designation of Assistant Manager and above to ensure that everyone is aware about who is responsible for what all activities.

Roles and Responsibility:

It will be the responsibility of the Information Security Officer to have the Role based training conducted and ensure that everyone participates. The Information Security Officer shall arrange for the training on a specific date/time during which everyone who is required to be participated are available. Further, if any employee(s) misses the training then the same shall be separately conducted and explained to the user.

Coordination:

The information security officer shall coordinate with all the departments to make this training a success.

Compliance:

The ISO is authorized to limit network access of individuals who do not co-operate with this training. If any grace period is required, it has to be approved by the Sr. Management. However, the grace period shall not exceed 30 days of the actual scheduled date.

Communicating threat information:

The ISO shall ensure that he shall discuss all the threats identified during internal audits/Risk assessment process and take inputs/suggestions on remediating the same from all the stakeholders during the Role based trainings.

Legal responsibilities and business controls:

The ISO shall assign all the legal responsibilities to the right candidate in order to be compliant with the legal clauses. Further, relevant controls shall be identified and plans to implement the same shall be documented.

15.3 Communicating security policies during induction training

MDI's HR team shall ensure that they communicate and brief all the employees who joins the Organization about MDI's security policies. Below are the security policies that needs to be communicated:

- ADMIN001-Access Control Policy
- ADMIN002-Visitors Policy
- ADMIN003 - Return of Assets Policy
- ADMIN004-Disposal of Media Policy
- ADMIN005 - Emergency Evacuation Policy
- ADMIN007 - Asset Management Policy
- BCP_India / BCP_US
- HR010-Onboarding Policy
- HR011-Policy - Sexual Harassment
- HR015-Separation Policy
- HR019 - Anti Slavery Policy
- IT001-Workstation Allocation Policy
- IT002-IT User Access Management Policy
- IT004-Backup Policy
- IT009-Email & Messaging Policy
- IT010- Computer Usage Policy
- IT013-Account Lockout Policy
- IT015-Security Audit, Logging & Monitoring Policy
- Information Security Manual
- GRC004-HIPAA Compliance Policy
- GRC005-Mobile and Removable Media Device Usage policy
- GRC006- Retention Policy
- GRC007-Risk Management Policy
- GRC008 - Privacy Policy
- GRC011 - Standards of Conduct
- GRC013-Data Destruction Policy
- GRC014 - Work from Home Policy
- GRC017 - Whistleblower and Non-Retaliation Policy
- GRC018 - Disaster Recovery Plan

16. Appendix A

CIMT Matrix	
Functional Role	**Name**
Enterprise Security Officer (ESO)	Alpana Sharma
Operations Help Desk	Ashok Bhalerao
	Dhanashri Oza
Server Support Services	Sourabh Bhat
Network Support Services	Sourabh Bhat

For detailed roles of the CIMT Team members refer (5.1.3 Allocation of Information Security Responsibilities)

17. Revision History

Version No	Effective Date of the Change	Author	Description of Changes/Revision	Approved By
1.0	01-Nov-2016	Amar Uttarkar	Initial Issue/Draft	Amit Virwal
2.0	09-Jun-2017	Amar Uttarkar	Entire Manual has been altered to satisfy ISO 27001 Requirements	Amit Virwal
3.0	01-Jul-2018	Amar Uttarkar	Procedure if the cryptographic key is compromised has been added in section 11.3.2; Access to secret authentication added in section 11.3.2; Wireless Password Construction has been included in section 10.3.4;	Amit Virwal
4.0	05-Dec-2018	Amar Uttarkar	Sr. Management Commitment towards information security further briefed under section 5.1.1; Role of ESO removed and the roles were assigned to ISO; Retention for the review of independent audit is defined for 3 years; Section 5.2.1 updated to include Security Requirements while dealing with Third Parties; Section 5.2.3 updated to include the due diligence for vendors who may have access to MDI's Information Systems; Section 6.1.3 updated to include the exclusion to restrict the blocking of copy/paste; Section 7.2.1 to include signing the acceptable use policy; Section 8 to include the purpose & scope for the physical and environmental security; Inserted section 8.2.5 Wireless Security; Section 9.5.1; Information Backup procedure was explained in detail; Section 9.10.1 has been detailed to include all the fields that needs be present in the audit logs; The bulleted points 5 - 8 were added in section 10.2.3; Section 11.6.1 briefed to include asset inventory; Added Section 11.7 Configuration Management; Priority for BCP to Operations & QA is defined in Section 13.1.3; Password/Account Reset procedure using AD Self Service Tool in Section 10.2.3;	Amit Virwal
5.0	21-Oct-2019	Amar Uttarkar	Addition of Sr. Management roles in 5.1.3; Authorities have been documented in 4.4; Addition regarding AD Self Service tool in 6.2.3;	Amit Virwal
5.0	22-Dec-2020	Amar Uttarkar	Annual Review; No changes performed	Amit Virwal
5.0	01-Dec-2021	Amar Uttarkar	Annual Review; No Changes	Amit Virwal
6.0	01-Jul-2022	Amar Uttarkar	Added a new statement in the section 8.2.5 “ MDI shall ensure to change the default SNMP community strings on all its wireless devices.” ; Added a new statement in the section 11.2.1 “ MDI shall ensure that all its application that includes DocGem and Golem shall undergo automated application vulnerability testing with an emphasis on input validation controls by a qualified party on an annual basis.” ;	Amit Virwal

6.1	01-Dec-2022	Amar Uttarkar	Process of creating the domain ID using AD Manager is added in section " 10.2.1 User Registration" ; Change of Anti-Virus from TrendMicro to Sophos in multiple section of the document; Change in escalation matrix and CIMT matrix. Policy updated as per HiTrust requirement;	Alpana Sharma
7.0	07-Dec-2023	Dhanashri Oza	Added section in 6.2.3 Disposal/Destruction"- Paper Disposal process ,Added Section on Phishing Awareness, under 9.4.1 Controls against Malicious Code added Methods and Tools for Phishing Attack Prevention and Detection, under 12.1.1 Reporting Information Security Events added reporting phishing attacks, under 12.2.3 Collection of Evidence added retention period of 3 years.	Alpana Sharma
7.0	10-Jul-2024	Dhanashri Oza	Annual Review; No Changes	Alpana Sharma