CYBER SECURITY POLICY

Revised 2019

MISHRA DHATU NIGAM LIMITED
HYDERABAD

Revision History

Year	Version	Approval Authority	Date
2014	1.0	Board of Directors	06/12/2014
2019	2.0	Board of Directors	14/02/2019

Contents

Introduction

With the increasing use of Information Technology in business functions, organizations are increasingly dependent on Information infrastructure. Information on the networks can be accessed from anywhere in the world in real time. While this is good for the spread of information, it has also allowed for the proliferation of 'malicious information'. Hacker tools are now widely available on the internet. Some websites even provide tutorials on how to hack into a system, giving details of the vulnerabilities of the different kinds of systems. It does not take an expert programmer to break into a system. Anyone with malicious intentions can search the internet for programs to break into a system which is not properly secured.

It is hence vital for businesses with information infrastructure to ensure that their networks are secure. This is important to minimize the risk of intrusions both from insiders and outsiders. Although a network cannot be 100% safe, a secure network will keep everyone but the most determined hacker out of the network. A network with a good accounting and auditing system will ensure that all activities are logged thereby enabling malicious activity to be detected.

Before a network can be secured, a security policy has to be established. A Cyber security policy defines the organisation's expectations of proper computer and network use and the procedures to prevent and respond to security incidents. A Cyber security policy is the foundation of security because it outlines what assets are worth protecting and what actions or inactions threaten the assets.

Preamble

MIDHANI Cyber Security Policy 2014 is duly approved by the Board of Directors of MIDHANI in 2014. This policy is revised considering the guidelines mentioned in Cyber Security Policy Template 2018 given by Cyber Security Group, DDP.

All users of information, computing resources, systems and communication networks based on computers as well as personnel tasked to undertake the administration of information systems and such resources will be governed by this revised version.

All departments will adhere to the directions given in this policy. Any violation to any clause in this Policy will be dealt as misconduct.

Objective

The objective of this policy is to comply with the guidelines to maintain a proper level of cyber security, specifically in regards to connectivity to the Internet, commensurate with risk and threat assessment.

The main objectives of this Policy are to -

- Establish, implement, control, monitor, review and manage information infrastructure in a secured and resilient cyberspace
- Reduce vulnerability and build capabilities against cyber threats.
- Provide directions for incident response as well as crisis management in the event of a cyber-attack.
- To prevent unauthorized access, damage and interference to the information infrastructure.

Scope

This document essentially covers policy towards security of all information assets and procedures and is applicable to all employees of the company -full-time, part-time, or temporary; customers; contractors; vendors who may be connected through the network.

All efforts have been made to make this policy comprehensive. However, amendments may be incorporated in accordance with government orders / instructions / guidelines issued from time to time which are relevant in the environment and requirement pertaining to Cyber Security.

Cyber Organization

The organizational structure of the Cyber Security cell in MIDHANI is outlined below.

Chief Information Security Officer (CISO): CISO will be a senior level officer / Director of MIDHANI. He/She is responsible for formulating Cyber Security Policy and ensure its implementation and operational effectiveness of Cyber Security measures within MIDHANI. CISO will brief the Board on half-yearly basis about the Cyber Security progress and related issues pertaining to MIDHANI.

- **Cyber Security Officer (CSO)**: CSO performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. Contact details of the CSO should be made available in the intranet portal.

- **Incident Responder**: A member of team who prepares for and initiates rapid response to security threats and attacks such as viruses and denial-of-service attacks.

The overall responsibility for Cyber Security lies with the Head of the organisation of MIDHANI.

Role of HR

All aspects of cyber crime directly or indirectly are triggered by human resource. Appropriate Training and Checks will be provided to all employees for cyber security awareness and pro-active defense mechanism.

Role of HR: Measures related to verification, contracts of employment, nondisclosure agreements, contracts with third party, Do's and Don'ts, responsibility and commitments etc., will be enforced during various stages of engagement of employees. All violations to the cyber security policy will be logged and tracked, all offences to be categorized and dealt as per the IT Act 2010 and any amendments thereof.

Standards and Review

This Policy is based on established standards in Cyber security and follows the following documents:

(a) National Cyber Security Policy 2013
(b) National Information Security Policy And Guidelines (NISPG) ver 5.0
(c) IT Act 2010
(d) IT Security Guidelines given by Ministry of Electronics & Information Technology, GoI.
(e) IT Security Guidelines and Instructions issued by Ministry of Defence, GoI.
(f) National Cyber Security Crises Management Plan 2015
(g) ISO / IEC 27001 (ISMS)
(h) Cyber Security Framework 2018 issued by Cyber Security Group, DDP

Policy will be reviewed once in two years or on any change of threat perception or on occurrence of a major security incident.

Audits

This policy covers audit of all computer and communication devices owned or operated by MIDHANI. Security Audits may be conducted to protect entire Information system from the security threat inter alia the following:

- Unauthorized Access to confidential data
- Unauthorized access of the department computers
- Password disclosure compromise
- Virus infections
- Denial of service
- Open ports, which may be accessed by outsiders

Audits are to be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Monitor all security measures to ensure conformance with Cyber Security Policy of MIDHANI
- Investigate security incidents

To ensure compliance of this policy, MIDHANI will carry out audits as per the following periodicity. The internal and external audit report will be submitted to Cyber Security Group- DDP within one month of carrying out the audit.

- Internal audits to be carried out by Chief Cyber security officer every six months.
- External audit will be carried out once in two years by a CERT-In empanelled agency.

Policy statement

Use of the MIDHANI network and/or MIDHANI Information Technology (IT) Assets constitutes consent to this Cyber Security policy. Network users are responsible for following the security requirements set forth in this policy, and for immediately reporting suspected security violations to the MIDHANI Cyber Security Officer/IT department and/or Cyber Security Group, DDP.

Asset Management and Responsibility

Ownership of Assets:

All Information Technology (IT) Assets will be owned by the MIDHANI IT Department.

Inventory of Assets:

All IT assets will be clearly identified and inventory of the same will be maintained at all times by the IT Department. This will be updated yearly based on Annual Inventory Verification procedure to ensure its correctness.

Accountability of Assets:

All IT Assets will be clearly labeled as per defined Format. The IT department will be responsible for labeling and handling of all information assets like Servers, Network Components, Computers, Thin-clients, Laptops & other authorized Handheld devices, Removable secondary storage media, Printers, Scanners, Projectors, UPS, CDs/DVDs etc. It should be ensured that these are accounted for correctly and theft/loss is reported promptly to the Security Dept. of MIDHANI in order to avert any Cyber Security lapses.

Access Privileges of Assets:

Access control and Access rights will be defined for major important IT assets.
Access rights of Users of Asset will be removed upon transfer or relinquishing of appointment.

User Responsibility:

Additionally, the Users using any type of IT Assets is assigned the second-level ownership and is held responsible for proper, safe and secure handling and taking over of all IT assets in his/her possession as well as handing over to IT department of the IT asset including secure deletion of the information in it upon transfer or relinquishing of appointment. At the same time Users will ensure that unattended IT equipment in their area of control have appropriate physical and logical protection. No removable media will be left unattended on desks/work areas of users.

Classification of Information:

Information must be identified, classified, and labeled based on the sensitivity (i.e., the business impact if destroyed, damaged or disclosed) to MIDHANI. Users/ owners are responsible for classifying information they create and are responsible to ensure that the appropriate level of protection is consistently applied. Information may be classified according to the following scheme:

- Level 1 -- Confidential Information: This class represents important and/or highly sensitive material that is appropriate for only specific employees. Unauthorized disclosure, modification, or destruction of this information could cause serious damage to the company and our clients.
- Level 2 -- Institutional Information: This class represents information important to the company. Its destruction and/or modification could result in serious losses. This information must have controls to ensure its integrity and accuracy. Its use is therefore subject to certain restrictions.
- Level 3 -- Unrestricted Information: This class represents information that does not fall into one of the above classifications and is appropriate for all company personnel in addition to the general public. This information is not considered confidential, and its disclosure, modification and/or destruction does not need to be controlled.

Based on the classification, security classification of a digital document will be mentioned in a bold font on top and bottom of the page and will be applicable to all file formats including Power Point presentations, world files, pdf files, and text files, excel sheets, database reports etc.

For all such classified files/presentations, the designation, name and shop/department of the author along with date of creation will be mentioned on all the pages/slides. Numbering of the pages/ slides will be incorporated including the title page/slide.

Security classification must be given to all classified documents even at draft stage and once the document is finalized, all drafts must be deleted securely. Any draft or final official data whether restricted, confidential or secret will never be copied on personal laptop/CD/DVD or external HDD or any such media.

Where a User /Owner fails to give a classification, the information is assumed to be classified to Level 3, i.e. ‘Unrestricted’.

Isolation of Computers processing Classified Information

Computers and computer network used for creating, processing and storing classified information with security classification as CONFIDENTIAL and above will be stand alone, isolated and dedicated. These computers or computer networks will not be connected to (WAN/LAN) or any other network.
All such computers will be housed in a secured area with a stringent physical and/or logical access control mechanism in place.

Physical and Equipment Security

1. The operational site housing the critical information processing facilities / Data-Center(DC) of MIDHANI must be in location not prone to natural or man-made disasters, like Fire, Flood, Earthquakes, Lightening, Chemical contamination and Explosions and may have Surveillance system, access card controlled entry. Suitable floor structuring, lighting, power and air conditioning must be provided.

2. Physical protection against damage from fire, flood and lightning will be applied. The Site must have Fire detection and suppression system in Compliance with regulations imposed by the Fire dept of MIDHANI. Also it must have Water detectors installed under the raised floors and lightning protection system installed in the premises.

3. The DC sites will be equipped with adequate Firefighting systems and Automatic fire/smoke detection alarm to prevent fire hazards.

4. Stabilized Direct Power supply and Uninterrupted Power Supply units with Battery Backup as well as Power Generators as Standby arrangement must be used to provide protection from power fluctuations, power failures and other disruptions.

5. Adequate air conditioning preferably Precision ACs along with temperature and humidity monitoring sensors must be Installed for temperature and humidity control in DC.

6. There must be protective cabinets with Fire proofing and Secure locking at DC for Storage of Data Tapes, Software / Maintenance Media, System documents like Configuration files, License keys.

7. Responsibilities for physical security of the IT systems at the DC shall be defined and assigned to named individuals of IT department.

8. System documentation (such as configuration files) stored on computers will be protected against unauthorized access.

9. The DC ~~site~~ must be protected by a well-defined Security Perimeter implemented using state-of-art physical security system like Access-card / Bio-metric / Iris Controlled system.

10. Entry to the DC at all times shall be controlled, regulated and restricted to authorized personnel only.

11. In case the Data Centre uses the facilities of external service/facility provider for any operation, the service–provided shall sign non-disclosure agreements.

12. Maintenance of IT System at DC by an external agency should be carried out under proper supervision. Authorized IT personnel should invariably be present throughout such maintenance and it be ensured that no data file/program is copied and taken by the outside maintenance engineer.

13. All IT Equipment will be adequately and timely maintained / updated to ensure its continued availability and integrity. Before sending outside any computing device for repair or maintenance, all storage media like hard-disks, CD/DVD, etc will be removed and kept at secure location and the repair and maintenance will be carried out and tested using test drives available with the repair / maintenance agencies. Internal drives will be securely erased and formatted when relocated for fresh installation.

14. In case of replacement of faulty/damaged hard disk under warranty/AMC, the original hard disk will not be either returned to the repair agency, or if returned must be zero-filled to make the original information non-retrievable.

15. Devices containing information will be securely disposed off. Prior to disposal or reuse of equipment the information in it will be destroyed, securely deleted or overwritten to make the original information non-retrievable. Prior to disposal of the Device all the storage media in it must be destroyed as per existing instructions. Similarly all the secondary storage media if not intended for use, must be destroyed.

Network, Server and Database Security

Network Security:

The purpose of Network Security policy is to provide guidelines for configuration, maintenance and access to MIDHANI Network connections.

1. MIDHANI has centrally managed Networks for internal usage connecting all the personal computers and Servers. It is designed and configured in a layered approach with VLANs and Redundant arrangement of network components as well as communication links so as to deliver high performance and reliability whilst providing a high degree of access control and range of privilege restrictions.

2. Adequate bandwidth in the network will be built up to cater to the requirements of Data, Voice and Video-conferencing.

3. All LAN cabling will be structured using Optical Fiber Cable(OFC) and CAT 6 UTP to provide secure media as well as high bandwidth and it will be protected from unauthorized interception and damage. Any unused network sockets will be sealed off.

4. Physical check of cables to detect tampering will be carried out as part of the existing security checks at all levels.

5. Network will be adequately managed and controlled, in order to be protected from threats and to maintain security for the systems and applications.

6. All network devices procured by MIDHANI will incorporate IPv6 protocol suite for ease of migration to IPv6 in a phased manner.

7. Internal Network/LAN must be separate from the external Internet.

8. The internal network/LAN must have appropriate protection at the gateway using perimeter defenses such as - Firewall, IPS, DMZ and Antivirus to protect from external threat.

9. The rules for the firewall will be based on the explicit requirements of access to external public network for certain critical works. All firewalls activities will be logged and analyzed by the network administrator on periodic basis.

10. Intrusion Prevention Systems (IPS) will be in place to passively monitor traffic by examining the packets entering or exiting internal network/LAN.

11. Centralized Antivirus mechanisms will be in place in conjunction with the firewall to check all incoming traffic for any viruses or malicious code. In addition, antivirus client software will also be installed on individual servers and all host machines including PCs.

12. Use of a network management software package to monitor the LAN 24x7 for auditing and logging of activities in a network.

13. A qualified Network Administrator (NA) will manage the network. NA shall remain updated on the latest vulnerabilities notified by Cert-In.

14. Appropriate identification, authentication, and authorization will be used to control access by remote users if necessary, remote access to MIDHANI'S internal Network/LAN and resources will only be permitted provided the authorized users are authenticated.

15. Remote access as well as Remote management to network devices will be done through secure communication channels only.

16. Networked computers will preferably have only network printers/scanners which may be shared among a defined close user group based upon data usage.

17. Computers on the network will preferably have their CD/DVD writers removed and USB ports disabled/controlled. If required only one computer per department will be enabled with these devices which will be under direct charge of the Head of the department.

18. Transfer of data between networked computers will be done through the network/LAN only.

19. All Equipment including Servers, PCs and Printers, etc. on LAN will be identified using proper hostname to authenticate location & device connection.

20. File and printer sharing facility for sharing data on LAN will be used with access control and authentication mechanism.

21. For shared networks if any, the capability of users to connect to the network will be restricted in line with the access control process and requirements of the applications. The connection capability of users will be restricted through network gateways that filter traffic by means of pre-defined tables or rules.

22. Only secure Telnet (SSH) and FTP will be allowed on the network/LAN.

23. Blogs, forums and chat servers may be hosted on the network.

24. Voice over IP (VoIP) communication, if allowed, will be secured against eavesdropping, call misdirection, identity misrepresentation, data theft etc. through authentication and encryption of data.

Server Security:

The purpose of Server Security policy is to establish standards for the base configuration of internal servers that are owned and/or operated by MIDHANI. Effective implementation of this policy will minimize unauthorized access to MIDHANI proprietary information and technology.

General Configuration Guidelines-

1. MIDHANI will have separate servers configured to cater for each role i.e. Database, ERP application, Windows Thin-client services, Intranet, Internal Mails etc. All servers will be placed with appropriate protection using Perimeter defense comprising of Firewalls, IPS, DMZ and Antivirus.

2. Server operating system, firmware and server applications will be regularly updated to ensure continued availability and integrity. Protection against all types of Virus, Trojan, spy ware to be implemented on Servers. For this purpose, online Updation and Patching the servers will be permitted to access the internet on time-bound manner from behind the Perimeter defense.

3. MIDHANI shall designate a properly trained “System Administrator” and assign him the system security responsibilities.

4. The responsibility to create, modify, delete or archive information on the Server must rest only with the System Administrator (SA).

5. For Operating System, the configuration principle of ‘deny first, then allow’ be practiced so as to selectively turn on only those services/applications that are absolutely essential. All non-essential services, applications, protocols will be disabled and all unused accounts, default or sample files will be removed.

6. Physical and Logical Access Control to all servers will be ensured through two-factor authentication.

7. Access to operating systems will be controlled by a secure log-on procedure. Log on credentials will neither be transmitted nor stored in clear

8. All Servers and system software will be kept updated with the latest patches and signatures to ensure protection against known vulnerabilities at all times.

9. Direct access to the servers will be used rarely such as during maintenance or updation. Root/Administrator login will be allowed from the administrative console only.

10. The Servers should use different name with root/administrator privileges for Server Administration purpose for which login will be permitted over the network/LAN.

11. Passwords for the administrative purpose must be known only to designated officers.

12. Proper procedures will be established for updating the servers and applications.

13. Audit Trail/System-event Log files be enabled in all servers and checked regularly for any anomalies, unusual/doubtful/intrusion activity and documented.

14. Administrator activities must also be logged and analyzed/investigated periodically.

15. Restriction on connection times will be used to provide additional security. Inactive sessions will be made to shut down after a defined period of inactivity. Time-outs can be tuned to clear the session screen and also, close both application and network sessions after a defined period of inactivity.

16. No unlicensed/pirated software will be installed by users in systems.

17. Maintenance in the server system by an external agency should be carried out under proper supervision. SA should be present throughout such maintenance. It shall be ensured that no data file/program is copied and taken by the outside maintenance engineer.

18. Internal drives will be cleared of all data before sending it outside for repair / installation**.** In case of replacement of faulty/damaged hard disk that is under warranty/AMC, the original damaged hard disk will not be returned to the repair agency/AMC holder. If it has to be returned the hard disk must be zero-filled to make the original information non-retrievable.

Database Security:

The Database Security policy establishes security requirements for database servers that are critical to MIDHANI. This policy is intended to help protect centralized/ distributed computing environment from accidental or intentional damage. The policy is also intended to protect MIDHANI's connected assets from alteration or theft of data while preserving appropriate access and use. The following guidelines are applicable-

1. It must be ensured that all default passwords for the accounts are changed. If the default accounts are not in use, they need to be locked.

2. No default roles will be implemented. Roles of data base users will be defined and allocated by data base administrator.

3. Logs of all failed login attempts will be reviewed daily. Database account lock out should be configured after three failed login attempts.

4. Logical access to application software and information will be restricted to authorized users only

Information/Data Back-Up:

1. Back-up of business data/information and software will be taken and tested regularly in accordance with the Backup procedure of MIDHANI.

2. Off-site backup should be maintained for critical data.

Internet Security

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Acceptable use of the Internet for performing job functions includes:

- Communication between employees and non-employees for business purposes.
- IT technical support downloading software upgrades and patches.
- Review of possible vendor web sites for product information.
- Reference regulatory or technical information.
- Research & Development

The policy considers the following-

1. Internal Network/LAN must be separate from the external Internet and a strict Air-Gap between Internet and Network/LAN will be ensured at all times by MIDHANI.

2. Internet may be accessed either on a standalone PC or through a separate Network connecting all Computers which are meant to access Internet, using Leased line provided by service provider. This network will be purely utilized for provision of Internet connectivity and will be adequately protected using Firewall, Intrusion Prevention systems (IPS), Unified Threat Management Systems (UTM), Proxy server, Anti-virus etc. and permit centrally controlled Internet access.

3. Stand-alone computers with Class 3 Information data will only be used to access Internet.

4. A computer used for creating and storing official documents/information or a LAN networked computer will not be connected or used to access Internet either through Leased lines or Broadband or through any devices such as mobile, USB modems, Wi-Fi or wireless access points, etc.

5. No official or classified official work will be carried out on computers connected to Internet. Even if the content bears no classification, any work that can lead to security breaches or can jeopardize MIDHANI's functioning/National Interests should not be carried out on the computers connected to the Internet

6. Broadband or any other independent Internet connections may be provided to authorized officials only and on wired media only.

7. No Wireless connectivity for Internet be permitted inside MIDHANI without approval of Director and above.

8. Firewalls to be established at Network level and the rules for the firewall will be based on the explicit requirements of access to external Internet. All firewalls activities will be logged and analyzed by the network administrator on periodic basis.

9. IPS will be in place as second line of defense to passively monitor traffic by examining the packets entering or exiting and to check attacks originating from outside.

10. Centralized Antivirus mechanisms will be in place in conjunction with the firewall to check all incoming traffic for any viruses or malicious code.

11. Computer name of the Internet connected computer shall not reveal the appointment or MIDHANI's identity.

12. No removable media containing classified as 'Confidential' and 'Institutional' data to be used in Internet connected computer.

13. All downloaded data on Internet computer will be duly scanned with an updated version of Antivirus before use in order to avoid introduction of trojans, backdoors, key loggers or malware.

14. Removable media as well as any other storage device will not be exchanged between Internet and LAN connected / Official computers as well as Laptops.

15. In case of urgency for swapping of systems between Internet and LAN, it will not be allowed without sanitizing the systems e.g. secure deleting and formatting.

16. The Internet PCs to have latest Web-browser which are always kept updated and its own peripherals in terms of Printers, Scanners, UPS, CD/DVD drive which will not be shared with any other system especially LAN connected ones.

17. Use of Removable media on Internet Computer to be restricted to barest minimum with 'Auto Run' disabled.

18. Each authorized Internet user will be given a separate user account and password.

19. MIDHANI website to be audited for GIGW compliance by CERT-IN empanelled agency.

20. MIDHANI Website will be preferably hosted on NIC Web Server.

21. Web pages with company information must be correct in all respect and be published on the web-site only after proper approval.

22. Responsibility for updating and upkeep of MIDHANI Website shall be with Head of IT Department.

23. A secured Email System will only be implemented.

24. All official communications should be through official email IDs only. Permitted official will be provided with official Email-IDs hosted on NIC.

Security in Support Processes

Change Control Procedures
The implementation of changes will be controlled through formal change control procedures. Introduction of new systems and major changes to existing systems will be properly documented.

Technical Review of Applications after Operating System Changes
Application control and integrity procedures will be reviewed to ensure that they have not been compromise by the operating system changes.

Outsourced Software Development
Outsourced software development will be supervised and monitored by IT Dept.

Cloud Services
It is necessary for the MIDHANI to ensure that the security of the data is not compromised while hiring cloud services. Following addition measures will be adopted to ensure security over cloud services.

- The cloud services to be hired preferably from Government/PSU agencies.
- Ensure that cloud provider is using strong encryption methods.
- Data backup maybe managed by the MIDHANI itself.
- There must be barriers to keep critical information separate from other information and organizations.
- Cloud –Organization and Cloud-Cloud inter linkages must be secured.
- It will be ensured that the information data is accessible to authorized users only.
- Logs at Cloud service provider's end shall be maintained and stored in encrypted from. Access to logs must be limited to minimum persons.
- Security related issues/aspects will be covered under Service Level Agreements (SLA).
- As a rule, access to critical information should be minimum particularity from mobile endpoints. In cases, when it is required to access the information from mobile endpoints, their access points, devices or end points must be secured. This is equally applicable to cloud connectivity as well.
- There shall be adequate authentication mechanism to avoid any chances where an attacker can pose as a cloud subscriber.
- Threat/Risk management and mitigation strategy on cloud security should be part of IS Policy.
- There should be a breach reporting mechanism for any security related incident not only in the data that provider holds for subscriber but also the data it holds about the subscriber.
- Client side and server-side systems must be protected by timely updating, patching etc.
- Access to information, network services, operation systems, application and system should be controlled.

Embedded Software

While procuring hardware and software, Original Equipment Manufacturers (OEM)/Licensed Software suppliers will certify that the product being supplied is free from embedded malicious hardware and software.

User Level Controls

Personal Security:

i. Officials at all levels are responsible for strict observance of the cyber security policy and enforcement of the same.

ii. User ID with password protection will be used by all Users for any kind of access to system/information.

iii. All types of external secondary storage devices including external USB based hard disks, USB Pen Drive, CD/DVD, SD/Micro SD/MMC cards and PDAs/mobile phones with memory cards are not permitted inside MIDHANI by all employees unless otherwise approved by competent authority.

Desktop Computer/PCs:

i. All Computers in internal LAN will be given proper Host-name for identification.

ii. Operating system of user's computers will be configured with only essential services enabled. All non-essential services from cyber security point of view must be disabled on any given operating system.

iii. USB Ports, CD/DVD Drive, Writers, etc. will be disabled using appropriate software on all computers unless otherwise permitted.

iv. All classified information emailed, stored on removable media will be in encrypted form.

v. Internet connected Computers will not be used for drafting, storing classified documents.

vi. Prevention measures to protect against all types of malware like virus, spyware, trojan etc. will be implemented on all desktops.

vii. Use of pirated and unlicensed software shall be strictly prohibited. Only licensed software purchased by MIDHANI will be used on PCs.

viii. Automatic log-out for terminals and clear-screen/shut-down for desktops, based on time-out for inactive/not-in-use session, will be implemented.

ix. All devices and system software will be kept updated with the latest patches and signatures to ensure protection against known vulnerabilities at all times.

x. Prevention, detection and recovery measures to protect against all types of malicious codes like virus, spy ware etc will be implemented on all desktops

Mobile Computing Devices:

i. When using mobile computing devices for official purposes such as notebooks, laptops, and tablets, etc., special care will be taken to ensure that information is not compromised or lost due to theft.
ii. Appropriate standard operating procedures will be established at all levels based on this policy for accounting and protection of mobile computing devices from damage, theft and unauthorized access.
iii. Technologies like Wi-Fi, Blue tooth, GPRS, Wi-Max etc. will not be used. The responsibility of disabling these services, if available in any IT equipment, is of the user of the equipment.
iv. All official information stored on portable media will be in Encrypted form.
v. Secure erasing of files on mobile computing devices will be ensured before reuse.
vi. Official laptops containing classified/official data will be handled in accordance with this policy.
vii. No personal Laptop/tablet/Note books are permitted to be brought into office.
viii. Official laptop, to be used for presentation in other offices/stations will not contain any data of Level 1 classification.

User Access Control

i. Access to Systems, Applications and Information will be restricted to Authorized Users only.

ii. Users will ensure that unattended equipment has appropriate physical and logical protection.

iii. No removable storage media will be left unattended in office desks and work areas. All desktops will have clear screen policy when not in use.

iv. User Access control process will ensure Role Based access Control. Information systems that process classified data will have Mandatory Access Controls (MACs) in place

v. Adequate segregation of areas of responsibility, access rights and privileges will be implemented through a formal authorization process in order to restrict opportunities for intentional modification/misuse and to ensure that no single person can individually compromise the entire system/data. Principle of least privileges will be followed while using systems and services.

vi. Each User shall be provided a unique User Id with Password for all kind of login to any System/Computing device In addition, the dedicated Classified/Critical systems based upon the confidentiality of info/data being stored/handled, will have Two/Three factor authentication.

vii. There will be a formal User registration and de-registration procedure in place for granting and revoking Access to information systems and resources.

viii. Allocation of Passwords will be controlled through a formal password management process. User will follow password guidelines in the selection, use and protection of password.

ix. Access rights of Users who have been transferred, left the organization or superannuated shall be modified based on department head recommendations.

x. User access rights will be periodically reviewed by department heads and redundant users Ids/Accounts/responsibilities will be examined.

Monitoring

Integrity Management
The integrity of system hardware configuration info and critical software files will be maintained and monitored/tracked to ensure any unauthorized activity on the systems and networks.

Audit Logging
Audit logs recording user activities, exceptions, and information security events will be maintained to enable future investigations and access control monitoring.

Monitoring System Use
Procedures for monitoring use of information processing facilities will be established.

Protection of Log Information
The log information will be protected against tempering and unauthorized access.

Administrator Logs
Administrator activities will be logged.

Fault Logging
Faults will be logged, analyzed and appropriate action will be taken.

Clock Synchronization
For static networks the clocks of all devices and systems will be synchronized with an agreed accurate time source to ensure incident tracking and log analysis.

Password policy

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

Guidelines for Password Protection

1. Never write passwords down.
2. Never send a password through email.
3. Never tell anyone your password.
4. Never reveal your password over the telephone.
5. Never reveal or hint at your password on a form on the internet.
6. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
7. Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
8. Report any suspicion of your password being broken to IT.
9. Don't use common acronyms as part of your password.
10. Don't use common words or reverse spelling of words in part of your password.
11. Don't use names of people or places as part of your password.
12. Don't use part of your login name in your password.
13. Don't use parts of numbers easily remembered such as phone numbers, or street addresses.
14. Be careful about letting someone see you type your password.

The following password requirements will be set by the IT department:

1. Minimum Length - 8 characters recommended
2. Maximum Length - 14 characters
3. Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
    1. Lowercase
    2. Uppercase
    3. Numbers
    4. Special characters such as!@#$ %^&*(){} []
4. Passwords are case sensitive and the user name or login ID is not case sensitive.
5. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.
6. Maximum password age - 60 days
7. Minimum password age - 2 days
8. Account lockout threshold - 4 failed login attempts
9. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity.

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

Security Awareness

"Ignorant users" are widely recognized as the most serious threat to network security. If employees do not understand the power and proper use of the network, they can unintentionally compromise security (or be duped into it). In particular, employees must manage passwords properly and be aware of "social engineering" attacks.

Information Systems Acquisition and Development

An authorization process for new information processing facilities like procurement of hardware/software, establishment of LAN/WAN, development of software, automation etc. will take into account the existing cyber security policies/guidelines before authorizing the induction of such IT infrastructure to ensure that all relevant cyber security requirements are met.

To minimize the application level vulnerabilities, all application development will address the security issues at each stage of Software Development Life Cycle (SDLC).
Following issues will be addressed during software development

- Input Data Validation
- Output Data Validation
- Control of Internal Processing using Validation checks
- Protect Message Integrity and ensuring Authenticity.

Operational Control

Standard Operating Procedures
SOPs will be developed and documented to ensure adequate responsibilities and accountability for implementation and monitoring of cyber security measures wherever required.

Change Management
Operational systems and application software will be subject to strict change management control to ensure that all changes to equipment, software or operating procedures are duly analyzed, approved, supervised and carried out in a controlled manner to prevent inadvertent failures.

Segregation of Duties
Duties and Areas of responsibility will be segregated to reduce opportunities for unauthorized or internal modification or misuse of the assets.

Controls against Malicious Code
Prevention, detection and recovery measures to protect against all types of malicious codes like virus, spy ware etc will be implemented on all desktops, servers and at the gateways to the internal networks.

Patch and Signature Management
All devices and system software will be kept updated with the latest patches and signatures to ensure protection against known vulnerabilities at all times. The network administrator shall remain updated on the latest vulnerabilities notified by CERT-In.

Back-Up
Back-up of information and software will be taken and tested regularly in accordance with the backup procedure of the establishment and criticality of information.

Incident Response

An incident is an observable change to the normal behavior of a system, environment, process, workflow or person.

IT head or any senior staff from IT department by default is the Incident responder. The incident responder manages the response to a security incident, a Natural Disaster or other event requiring response from Emergency services.

Incident management process-

1. Users, vendor, customer, partner, device or sensor reports incident to IT.
2. IT may filter the incident as a false positive. Otherwise, IT creates a record that captures the incident, incident source, initial incident severity and incident priority.
3. Incident management team (IMT) gets additional incident data and performs preliminary analysis and determines criticality of the incident. At this level, it is either a Normal or an Escalation incident.
4. Normal incidents do not affect critical production systems and incidents that affect critical production systems must be escalated.
5. The incident is ready to resolve.
6. The IT team resolves the incident and submits for closure.
7. The user, vendor, customer or partner who had raised the incident receives the resolution.

User Education, Training and Cyber Security Awareness

User awareness and training being one of the major cyber security measure, adequate impetus will be given to cyber security training at all levels. Adequate funds for advanced/outsourced training, whenever required will be made available.

Acceptable Use Policy

This Acceptable Use Policy (AUP) is designed to protect MIDHANI, its employees, customers and other users from harm caused by the misuse of Information systems and data. Misuse includes both deliberate and inadvertent actions.

MIDHANI's systems are to support and enable the business. A small amount of personal use is allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs or injury being borne by MIDHANI.

MIDHANI trusts its employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's Information Systems.

MIDHANI will monitor the use of its Information system and the data on it at any time. This may include examination of the content stored within the email and data files of any user, and examination of the access history of any users.

MIDHANI reserves the right to regularly audit networks and systems to ensure compliance with this policy.

Users must take all necessary steps to prevent unauthorized access to confidential information. Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise, transfer to any system any information that is designated as confidential, or that they should reasonably regard as being confidential, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with Password policy.

Users who are supplied with computer equipment are responsible for the safety and care of that equipment, and the security of software and data stored it. Because information on portable devices, such as laptops, tablets and smart phones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only.

Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at least5 minutes of inactivity.

Users who have been identified for management of systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Network systems by whatever means and must report any actual or suspected malware infection immediately to IT department.

Business Continuity Plan/Contingency Plan

A business continuity process and Disaster recovery management process for IT systems should be in place to minimize the impact of any disaster on the organization.

Preventive mechanisms to be put in place to reduce the possibility of organizations experiencing a disaster or lessen the amount of damage if a disaster does hit. Recovery strategies by defining the recovery mechanism and strategies on how to rescue the organization to be implemented in terms of business process recovery, facility recovery, supply and technology recovery, user environment recovery and data recovery.

Risk Management

It is important to forecast uncertainty, map the threats and create counter measures to potential threats as it pertains to the use of technology within organization.

IT risk management framework must focus on:

1. Identify the threats
2. Map the severity and probability of each threat
3. Determine the impact of each threat
4. Implement control recommendations

Review & Audit:

Audit Preparation and Planning:

i. Internal Security audit will be audited in all departments once in six months. The CISO prepares the Annual Audit Plan in consultation with the other Shops / Department In-charges at the beginning of the year.

ii. The CISO prepares an Internal Audit Schedule and circulates to the auditors and sections to be audited at least one week before the scheduled internal audit. CISO identifies the names of the auditors who are to perform the audits and include their names in the internal audit schedule prepared as detailed above.

Auditors:

i. All internal Information Security auditors including the CISO are trained in the techniques of auditing and qualified by providing them an opportunity to attend an external or in-house training course on internal Information Security auditing.

ii. Information Security auditors from other Defence PSUs may be used if required. However, such auditors should have undergone training in security audit.

iii. CISO maintains a list of internal Information Security auditors eligible to perform internal Information Security audits.

iv. The CISO constitutes the audit team using qualified auditors from the list referred above.

v. The CISO prepare the check list and audit procedure for auditors to use in audit.

vi. Auditors are not allowed to audit their own work areas or those functional responsibilities under their charge in order to ensure independence of the internal Information Security audit.

Performing the Audit:

i. The planned and agreed audit schedule will be adhered to by all parties concerned.

ii. Auditors shall use checklist and respective ISMS procedures given while carrying out the audits. Audits are carried out by questioning the auditees, observing the performance of the system and examining the documentation and log records.

iii. The auditor analyses any apparent non-conformance or adverse condition to establish its validity as an audit finding the objective evidence. Any deviation from the approved procedures, guidelines and work instructions is considered as non-conformance. All these findings are noted on Auditor's Notes form (including Positive observations).

iv. All deviations or deficiencies are shown in non conformance reports. All non-conformance reports are signed by the concerned auditees and original NCR is given to auditee with a copy to CISO.

v. While reviewing the summary of the audit findings, CISO verifies the accuracy of reporting and clause numbers assigned to the non-conformance.

Audit Report:

i. At the end of the audit, CISO reviews and summarizes the audit findings and prepares a summary of Internal Information Security Audit report. CISO reports the audit findings to the management.

ii. CISO discusses the summary of Internal Information Security Audit report with members of Cyber security committee information for necessary corrective and preventive action.

GLOSSARY

Access
The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Access Control
The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Air Gap
To physically separate or isolate a system from other systems or networks.

Application Software
A software that is specific to the solution of an application problem. It is the software coded by or for an end user that performs a service or relates to the user's work.

Asset
A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Audit
A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analysis of activities to detect intrusions into or abuse of an information system. Inadequacies found by an audit are reported to appropriate authorities.

Audit Trail
A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Authentication
The process of verifying the identity or other attributes of an entity (user, process, or device).

Authorization
A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.

Backup
The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken

Compromise
A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.

Computer
Any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

Computer Network
Interconnection of one or more computers through:
(a) The use of satellite, microwave, terrestrial line or other communication media.
(b) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained

Confidentiality
A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

Critical Infrastructure
The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cyber Security
The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Data Centre
A data center is a facility composed of networked computers and storage that businesses or other organizations use to organize, process, store and disseminate large amounts of data.

Data Integrity
A condition in which data has not been altered or destroyed in an unauthorized manner.

Data Security
The practice of protecting data from accidental or malicious modification, destruction or disclosure.

Denial of Service
An attack that prevents or impairs the authorized use of information system resources or services.

Distributed Denial of Service
A denial of service technique that uses numerous systems to perform the attack simultaneously.

Encryption
The process of transforming plaintext into cipher text.

Event
An observable occurrence in an information system or network.

Exposure
The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

Failure
The inability of a system or component to perform its required functions within specified performance requirements.

Firewall
A capability to limit network traffic between networks and/or information systems.

Identity and Access Management
The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.

Incident
An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Incident Response
The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Intrusion
An unauthorized act of bypassing the security mechanisms of a network or information system.

Malware
Software that compromises the operation of a system by performing an unauthorized function or process.

Mitigation
The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

Network
A set of related, remotely connected devices and communications facilities including more than one co*mput*er system with the capability to transmit data among them through the communications facilities

Network Administrator
The person at a computer network installation who designs, controls, and manages the use of the computer network.

Password
Definition: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Phishing
Definition: A digital form of social engineering to deceive individuals into providing sensitive information.

Recovery
The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Response
The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Risk
The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.

Risk Assessment
The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Risk Management
The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Risk-based data management
A structured approach to managing risks to data and information by which an organization selects and applies appropriate security controls in compliance with policy and commensurate with the sensitivity and value of the data.

Rootkit
A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges, and conceal the activities conducted by the tools.

Spyware
Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

System Administrator
The person at a computer installation who designs, controls, and manages the use of computer system.

Threat
A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Unauthorized Access
Any access that violates the stated security policy.

Virus
A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability
A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Vulnerability Assessment and Management
Cyber security work where a person: Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.