**Network Security Management Policy And Procedure**

Doc: POL/0.1

Document Classification: Internal

July 2022

**Document Control**

| Document Name | Network Security Management Policy and Procedure |
| --- | --- |
| Document ID | POL/0.1 |
| Security Classification | Internal |

| **Authorization** | | |
| --- | --- | --- |
| Document Owner | Reviewed by | Authorized by |
|  |  |  |

| **Amendment Log** | | | |
| --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Section** | **Brief description of the change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

1.0 Introduction 4

2.0 Scope 4

3.0 Policy 4

3.1 Network Management Controls 4

3.1.1 Network Design 4

3.1.2 Network Services 4

3.1.3 Network Connectivity 4

3.1.4 Network Component Security 5

3.1.5 Installing Network Operating Systems (NOS) 5

3.1.6 Network Operating System Controls 5

3.1.7 Updating the Network Software 5

3.1.8 Network Security and Access Controls 6

3.1.9 Log Access 6

3.1.10 Terminal Timeout 6

3.1.11 Network Configuration Diagrams 6

3.1.12 Enforced Path 6

3.1.13 Node Authentication 6

3.1.14 Clock Synchronization 6

3.1.15 Network Devices 7

3.1.15.1 Firewalls 7

3.1.15.2 Other Network equipment’s 7

3.1.15.3 Modems /PDAs 7

3.1.15.4 Network Diagnostic Tools 7

3.1.16 Auditing, Logging and Monitoring 7

4.0 Procedure 7

4.1 Network Server Security 7

4.2 Network Access Control 7

4.3 Network Servers 8

4.4 Access to Third Party 8

4.5 Internet Service Management 8

4.6 Internet Service Logging and Monitoring 8

4.7 Identification of Network Equipment’s 9

4.8 Identification of Communications Lines 9

4.9 Network Diagram 9

4.10 Network Security Monitoring 9

4.11 Removable Media 9

4.12 Data Transmission 10

4.13 Network Assessment 10

4.14 Maintenance Contracts 10

4.15 Data Backup and Restoration 10

4.16 Malicious Software 10

5.0 Reference Documents 10

# Introduction

Networks have logically and physically extended data, processing and communication facilities across the {Company}. Network security assumes importance to the {Company} when viewed in light of the following:

* Networks change frequently as new users and devices are added and newer data communication technology is introduced.
* Usage of various networking, communications and computing technologies to effectively meet the IT needs.
* Sensitive data is increasingly transmitted over networks.
* Proliferation of Internet access has increased vulnerability as employees use Internet for information and knowledge.

The term “network” used in this policy section refers to all the types of networks like Local Area (LAN), Wide Area (WAN). Wireless (Wi-Fi) Network, Internet (Multiprotocol Label Switching (MPLS), Lease Line)

# Scope

This policy applies to all employees, apprentice, contractors, consultants, vendors and temporary staff members etc. who have access to network resources. All are expected to be familiar and comply with this policy.

# Policy

Configuration of computing and network components shall be controlled and documented. Adequate physical and logical security such as segregation of networks / network segments depending on the sensitivity of information and department requirements shall be implemented.

Clock synchronization shall be done on the network for integrity and non-repudiation of communication.

## Network Management Controls

## Network Design

* Networks shall be designed in conformance with sound security practices.
* The development, test and operational facilities, shall be separated to reduce the risk of unauthorized access of changes.
* The networks shall be segregated by implementing the most appropriate controls, which include, but are not limited to:
  + Running on separate computers, domains, and networks to ensure the protection of data passing over networks.
  + Individual / Different usernames and passwords to ensure that changes cannot be made accidentally or intentionally from one environment to another.
  + Segregation of duties of network administrators i.e. who have authorized access to the environments and who test operational systems to be achieved whenever appropriate.
* Network designs and architecture shall be documented and maintained, to include configuration settings for network hardware and software details.
* All hosts shall be security hardened to an appropriate level.

## Network Services

* Network Services shall be reviewed and those services that are not required shall be disabled.

## Network Connectivity

* Access to local system control utilities (e.g. Batch Files, Unix Scripts etc.) shall be controlled. Access to these utilities shall be limited to authorized personnel only.
* External parties shall not be allowed to connect to the internal network. If this is required then approval from Department Head and Head – IT shall be required. The access will be provided for the defined time frame only. For example: If any visitor wants to connect to our network then Head – IT’s approval is taken.
* For non-public information, all equipment that provides access to the network shall positively identify the user through a login sequence for providing access.
* Remote Access Software shall be used over the internal network only by authorized personnel.
* When access is no longer required, the requesting department within the {Company} or external connecting {Company} must notify the IT Team.
* The data card shall not be purchased as standard part of Desktop / Laptops.
* Automatic connections to external remote computer systems must not be allowed.
* Systems that do not authenticate to the {Company} network shall not gain access to the wireless network. This means that only computers / devices used and managed by the {Company} can use the network. The access to the wireless network shall be provided only after approvals from Department Head and Head – IT.

## Network Component Security

* All the network components should be identified and their use should be restricted.
* All network components shall be maintained in an inventory along with details. The Network Team shall identify all the network equipment’s by individual names and shall maintain a record of all network equipment’s in Asset Inventory along with its location and purpose of that equipment.
* All communication equipment like cables, network devices shall be secured from unauthorized physical access. The access control may be in the form of:
  + Access control systems like Keys, RFID access cards, Biometric scanners, Keypad locks, etc.
* Access to highly sensitive processing functions shall be secured by limiting the terminals from which these functions can be executed and physically and / or logically restricting these terminals.

## Installing Network Operating Systems (NOS)

* Network Operating System shall follow the Minimum Baseline Security Standard (MBSS), as mentioned below, but not limited to, are:
  + Proper configuration on the base operating system
  + Regular updating / patching of operating system and network accessing applications
  + Installation and maintenance of viable protective software
  + Proper over-sight of user accounts
  + Compliance with all applicable regulations regarding the data stored on, or transmitted through, the server
  + Data Protection
  + Regular Log Review
  + Proper care taken to physical security and access of the NOS

## Network Operating System Controls

* Each network user must have a unique user id and password. In case, common user id is used for some of the systems / servers where the customized instances / services are running, exception approval must be taken from Department Head and Head – IT.
* All user accounts must be associated with an applicable, informative full name and description.
* All the guest account shall be disabled.

## Updating the Network Software

* Network equipment must run an approved version of its operating software. Network Team shall provide and maintain a list of approved versions and patches. When a version is removed from the list, or a mandatory patch is added, the necessary updates will be applied as per the Patch Management Policy.
* Network equipment shall not be configured to load new operating software or configuration data automatically. Any such update shall be carried out manually by the Network Team.

## Network Security and Access Controls

* There should be proper authorization procedure for determining who is allowed to access which networks and networked services. Proper protection should be ensured for any such connectivity.
* All devices connecting to the network must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that the anti-virus software is up to date.
* Personally owned devices shall not be allowed to directly connect to the network. Personally owned devices shall only be connected to the network with approval from Department Head and Head – IT. Personally owned refers to devices that are not provided by the {Company} and directly connected means either by network cable or corporate Wi-Fi. However, a guest Wi-Fi facility can be used with appropriate approvals.
* External visitors may connect to the internet via a Guest Wi-Fi account with approval from Department Head and Head - IT. This will be via password that is changed regularly.

## Log Access

* Only authorized users must have access to utilities that reconfigure logging mechanisms.
* The log files must be protected from being accessed, modified or deleted by unauthorized users.

## Terminal Timeout

* Time out duration shall be specified for all terminals inactive for a set period of time.

## Network Configuration Diagrams

* Network configuration diagrams shall be considered as sensitive information. Network configuration diagrams shall only be made available to authorized individuals strictly on a need-to-know basis.
* Network configuration diagrams of existing network architecture having multiple levels (Level 1 – WAN; Level 2 – LANs; Level 3 – LAN Segments) with IP, WAN protocols and communication links (primary and standby) with details of bandwidths and data type for which the line is used for voice / data shall always be kept updated.
* Any change in the network configuration should be notified, to the officials responsible to maintain the Disaster Recovery Plan / Business Continuity Plans.
* All changes in access control must be accompanied by a valid business justification, and are subject to security review. All such changes should go through the ticketing tool. The requesting department is responsible for notifying the Network Team when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

## Enforced Path

* Users who have been given command line access to systems must, where feasible, be limited to the access or service needed. This may include controls such as restricted shells, application menu restrictions, or pre-programmed batch scripts.
* Menus and submenus options will be limited in the application systems in accordance with the business requirements.
* Direct access to system should not be allowed from the application system.

## Node Authentication

* Connections to any network computer systems shall be allowed only after authentication.

## Clock Synchronization

* System clocks must be synchronized regularly especially between the {Company}’s various processing platforms. This would allow for generating time based audit trails. Inaccurate audit logs hinder such investigations and damage the credibility of such evidence. The system engineers and network engineers in charge of the network must ensure that users cannot change this setting wherever appropriate.

## Network Devices

## Firewalls

* All internal network resources must be protected from the WAN / Internet, by one or more firewalls to protect services and systems from external untrusted network access.
* All services and systems hosting confidential data must be protected by a network firewall.
* All access through the firewalls accessing confidential information must be assessed on ‘Deny All – Allow Specific’ principle and ensure that firewall access must be enabled for applications and IP address combinations, wherever possible.
* Inbound internet traffic shall be limited to only system component and services within the respective security containers protected by firewall systems and to other authorized services and systems.
* For any change to be enabled in the firewalls, users must raise a ticket via the ticketing tool and the access will be enabled post approval from Department Head and Head – IT.

## Other Network equipment’s

Similar security procedures shall be established for other networking equipment’s. The Network Team is responsible for other network equipment’s security.

## Modems /PDAs

* Access to network using mobile devices (like PDA, Cell Phones GPRS device) is not allowed unless it is a mobile device authorized by the {Company}.

## Network Diagnostic Tools

* The use of network diagnostic tools shall be strictly controlled to prevent unauthorized users from obtaining sensitive information about the network.
* Diagnostic equipment and software shall be stored in a physically secure location when not in use. All workstations equipped with diagnostic software shall be secured (using password protection, etc.).
* Penetration testing tools may sometimes be deployed to assess the network’s robustness to internal and external attacks. It is essential that these tools must be run in a controlled environment, with written approval from Head – IT.

## Auditing, Logging and Monitoring

* Any problems with the network equipment’s leading to delay or stopping of any business processes should be escalated as an Incident and handled and escalated as per Incident Management Policy.
* Logging of activity on equipment is limited and restricted, and this logging will only be used to troubleshoot technology problems and to capture data to provide proof of illegal outside (external to Ice Warp) activity. Capturing of data from internally identifiable computers will only be done after approval from HR / Legal.

# Procedure

## Network Server Security

Access to network services and servers must be controlled to ensure that connected users or computer services do not compromise the security of any other networked services.

## Network Access Control

* Access to network and network resources must be on need to know basis and authorizations must be obtained from appropriate authorities before providing access.
* Networks must be logically or physically divided based on the criticality of the information stored in the networks. If the network is logically separated, appropriate perimeter security devices must be put in place. If the network is physically separated, controls must be in place to protect physical access to the network points at all ends.
* To maintain the privacy of the company information, company networks must not be used for personal and / or private information unrelated to business activities.

## Network Servers

* A server should be dedicated to a single network service, wherever possible. This will simplify configuration, thereby reducing the risk of configuration errors. In some cases, however, it may be appropriate to offer more than one service on a single host computer (e.g. DNS, ftp and http services).
* The network services that need to be provided on a server must be identified and documented. All unwanted network services must be disabled or removed.
* A documented backup and recovery plan for critical network equipment’s must be prepared, which should include the steps needed to maintain or restore the network services after various kinds of faults.
* In the absence of the Network Administrator, designated/authorized appropriately skilled persons from the IT Team must hold the responsibility of performing the related network and system administration activities.

## Access to Third Party

* Access to company network provided to external parties e.g. vendors / clients / consultants etc. must be given after careful analysis of need and after assessing risks involved in providing such access. A formal risk assessment must be conducted for each access.
* The following procedure shall be followed:
  + Department Head should be the initiators for access requirements for external parties as well as requirements of access to external parties.
  + Risk assessment shall be conducted by the Network Team to identify any risks involved in providing access to third parties. The risks identified shall be documented and specific controls required to mitigate the identified risks should be put in place in the {Company} and at the third party if required.
  + Restrictions on remote access will be included in the NDA signed between both the parties.
  + Every third-party access request will go through the ticketing tool. This request should contain what type of access is required; which application is going to be used, what data is going to be transmitted, encryption methodology required / used, etc. This shall be then approved by the Department Head interacting with the third party. Access shall be provided by the Network Team after approval from the Head – IT.
  + If the {Company} requires access to systems of other agencies, {Company} shall follow procedures and guidelines imposed by the external agencies. Internally, the Department Head and Head – IT should approve the access. Network Team shall maintain a record of these accesses and monitor them regularly.

## Internet Service Management

The Internet Security Policy shall be followed for providing the access to the employees.

## Internet Service Logging and Monitoring

* All sites accessed to Internet services must be logged.
* The Network Team must review the log files of firewall at least on a monthly basis.
* All security notification messages via electronic correspondence must originate from the IT Team. If any user receives such security notifications from external or any other source, he must report it only to the IT Team and not redistribute it.

## Identification of Network Equipment’s

The Network Team should identify all the network equipment’s by individual names and should maintain a record of all network equipment’s in a register (Asset Inventory) along with its location and purpose of that equipment.

## Identification of Communications Lines

Hardwired communication lines (e.g. network lines) must be catalogued and uniquely identifiable to the system being accessed to facilitate maintenance and security. All the lines along with its capacity should be documented and maintained by the Network team, as applicable.

## Network Diagram

* The Network team should be responsible for maintaining an updated network diagram. Periodic reviews must be conducted by the IT Network Manager to ensure that the diagram is updated to reflect the existing network architecture. Network diagrams should be updated as and when there are changes made to the network architecture.
* The Network Diagram should contain all network equipment’s along with their IP Addresses.
* The Network Diagram should contain all communication links (Primary and Stand-by) along with their bandwidths and data type for which the line is used for (voice / data)
* Adequate version control mechanisms and information classification controls should be in place for managing and updating the network diagram.

## Network Security Monitoring

Network Team is primarily responsible for monitoring the network. Systems should be monitored to ensure conformity to logical access policies and procedures. Logs from various network equipment’s should be monitored to detect unauthorized access to the network and maintain an audit trail. All the incidents on the network equipment’s for e.g. firewall must be logged for audit purpose.

Any problems with the network equipment’s leading to delay or stopping of any business processes must be logged into the ticketing tool.

## Removable Media

* All removable media such as USB drives, CD / DVD drives in network shall be disabled by default. USB hard drives / thumb drives / memory cards are generally not allowed and are blocked on the network. The same applies to I-pods, Zune and other music hardware that can be used as storage devices – these devices cannot be connected to the computer.
* USB drives, Floppy drives and CD-ROM drives shall be enabled for employees as per the ticketing tool process for a time bound access with approval from concerned Department – Head.
* Each access shall be given after careful analysis of need and after assessing risks involved in providing such access. A formal risk assessment must be conducted for each access.
* Before IT allows any USB device to access sensitive data on a computer, the USB device shall be reviewed by the IT personnel.
* The USB device that shall be used to copy data from one network to another has to be reviewed and scanned by the IT personnel and he / she has to verify that the USB device does not contain any virus / malware.
* Removable media should be labelled, handled and disposed as per Information Classification Policy.
* Exceptions – USB devices shall not be blocked on these computers:
  + Servers

## Data Transmission

* Any information from {Company} environment traveling over third-party networks or public networks must be encrypted, wherever required. Appropriate encryption algorithms must be used to maintain the integrity and confidentiality of the data.
* Appropriate technology shall be used for encryption after detailed evaluation.
* Access to encryption software must be given only on a need-to-know basis after authorization from appropriate personnel.
* Confidential information not being actively used, when stored or transported in computer readable storage media (such as magnetic tapes, floppy disks or CDs), must be secured through encryption or password.
* To prevent unauthorized disclosure of data when computers are sent out for repair or used by others within or outside the {Company} and data cannot be deleted; all data stored on hard disks must be encrypted or password protected, wherever feasible.

## Network Assessment

The machines on the network are Windows based and have been installed with all the latest patches and service pack, the vulnerability assessment on the network shall be performed by the IT Team.

## Maintenance Contracts

The IT Network Manager shall ensure that maintenance contracts are maintained and periodically reviewed for all network equipment’s.

## Data Backup and Restoration

The IT Network Manager is responsible for ensuring that backup copies of network configuration data are taken regularly.

## Malicious Software

Measures are in place to detect and protect the network from viruses, malware, ransomware and other cyber threats.

# Reference Documents

* ISMS Overview Policy
* ISO 27001:2013
* Statement of applicability for ISO27001:2013
* Logical Access Control Policy
* Physical and Environmental Security Policy
* Asset Register Template
* Change Management Policy
* Incident Management Policy
* Electronic Mail Security Policy
* Information Classification Procedure
* Internet Security Policy