Network Security

Table Of Contents

1.1 Policy Statement

In order to safeguard the Information Systems Network of Company , from various business and environmental threats, systems and procedures are developed and implemented by providing network security resources at a level that is appropriate for the nature of the data transmitted to protect all business data, related application systems and operating systems software from unauthorized or illegal access. In order to determine what level of security is appropriate, risk analysis must be performed on the data transmitted, every time the nature of the data changes significantly.

1.2 Scope

This chapter addresses Policies and Procedures related to the Network & Telecommunication security of Company's information resources. This policy and the associated procedures apply to the entire staff of company and any persons using the information systems resources of this Company. This includes contractors, consultants, third-party associates and any temporary employees and covers access to computing facilities, hardware, corporate data, applications software, systems software and telecommunication infrastructure.

1.3 Execution Responsibility

The Administrator-Network along with Administrator-Systems is responsible for implementing and executing the procedures mentioned in this chapter. The execution of the procedures will be monitored by Head-Infrastructure. CISO shall perform testing to ensure that the systems are compliant with the policies and procedures.

1.4 Detailed Procedures

1.4.1 Remote Access

1.4.1.1 Request for Remote Access Service

The service request related to remote access must be reviewed and approved by requester's department head and Head-Infrastructure

1.4.2.1 Use of Modem Bank

At all locations where remote access is required there must exist a modem bank. The modem bank must be attached to a dedicated communication's server. All incoming calls must be directed from these modem servers to the required destination.

1.4.2.2 Use of Secure Access devices

Remote access to systems that contain confidential/restricted information must be through the use of a secure access device. For example: Smart Cards, Tokens etc.

1.4.2.3 Dial-In Authentication

For non-public information, all equipment that provides dial-in capability to the network should positively identify the user through a login sequence before allowing access. This should be accomplished through the communications software itself or by a combination of routing the user directly to a specific application and or operating system and using its login routine.

1.4.2.4 Control of Dial-In Telephone Numbers

Telephone numbers for dial-in devices should not be distributed to anyone other than people who have demonstrated a business need to use them. The list of users with remote access should be maintained by the Head-Infrastructure. Remote user's access should be confined to the device installed at their end. Users should not be able to login from any other device.

1.4.2.5 Restrictions on Use of Remote Control Software

The Administrator-Network should impose adequate security controls for protecting the network before users are allowed to attach hardware and install remote control communications software (software that allows a remote user to dial into a PC attached to the network and issue commands from it as if it were attached to the network itself). The use of personal communications equipment (modems, ISDN cards, etc.) attached directly to personal computers with remote control software should be strictly controlled.

1.4.2.6 Disabling Default Network Equipment Passwords

All network equipment default passwords (e.g., routers, switches etc) should be changed during installation.

1.4.2.7 Remote Access for electronic mail

Remote access to electronic mail must be provided only through the use of an email client application.

1.4.3 Network Access

1.4.3.1 Control of Local System Control Utilities

Access to local system control utilities (e.g. Batch Files, Unix Scripts etc.) should be controlled. These utilities should be installed on local PCs and should be intended for use by the Systems Administrators to assist end-users resolve problems and access to these utilities should be limited to Systems Administrators.

1.4.3.2 System validation of User

Administrator-Systems should configure the host operating system to validate each user prior to allowing network access. Once verified, users should automatically be directed to applications for which they have been authorized.

1.4.3.3 Use of Networks limited to Business use only

The computing resources should be used for valid business reasons only. The protection of information contained on the company network is therefore the responsibility of Information Security Organization (ISO) and the activity and content of user information on the network is within the scope of review by the management. To maintain the privacy of the staff members, the network should not be used for personal and / or private information unrelated to job functions.

1.4.3.4 Restrictions on Network browsing

Each member a should avoid accessing areas on the company network for which they do not have a valid business need. While networks are intended to share information, it is each user's responsibility to exercise judgment over the information they access.

1.4.4 Firewall for Non-Public Data

- The entire company network should be isolated behind a firewall from public external networks. Also, any third party connection to company network for Intranet / Extranet connections (e.g., Customers and Suppliers) must be through a firewall only.
- All traffic from inside company to external networks, and vice-versa, should pass through a firewalled gateway that does not serve as a general-purpose host and therefore does not require features which weaken security (e.g., rlogin, telnet , finger etc.).
- Any connectivity to the external network should be authorized by the CTO

1.4.5 Access to third parties (Permanent)

1.4.5.1 Network Diagram

The Administrator-Network will be primarily responsible for maintaining an updated network diagram. Periodic reviews must be conducted by the Head-Infrastructure to ensure that the diagram is updated to reflect the existing network architecture.

1.4.5.2 Third Party agreements

Third party agreements must be entered for all permanent third party connections approved by the CTO. The agreement must include clauses that ensure that the third parties abide by Information Security Policy.

1.4.5.3 List of users

The Administrator-Network must maintain a list of users of third party having access to Company System. Privileges and activities of these users must be monitored closely.

1.4.5.4 Extended user authentication

Third parties being connected to company network on real time basis via a public network or any other external communication system must pass through extended authentication by use of a secure access device along with standard authentication procedure.

1.4.6 Third Party Connectivity (temporary)

1.4.6.1 Approval

Before allowing third party connectivity to the company network, the Head-Infrastructure, must obtain the approval from CTO.

1.4.6.2 Minimum rights to be granted

Temporary User ID and password must be granted with minimum rights that are required to perform the job by third parties.

1.4.6.3 Disabling of User ID

On completion of the maintenance activity or at the end of the day whichever is earlier, the temporary User ID must be disabled by the Administrator- Systems.

1.4.6.4 Close monitoring of activities

Logs of activities (e.g., resources accessed, system or application start, stop with user identity and time of action) carried out by maintenance personnel must be generated and closely monitored by the Administrator- Network.

1.4.7 Third Party Connectivity (for use of third party network resources)

Data traveling over the third party network resources must be encrypted using approved encryption techniques. Refer Chapter "Information Classification" for detailed procedures.

1.4.8 Network Operations and Monitoring

1.4.8.1 Use of Router Access Control Lists

The Administrator-Network should implement access control lists on routers to block all unauthorized traffic into the Company network.

1.4.8.2 Log-On Process

A system greeting screen allowing specific information about the organization, operating system, network configuration or any other internal matters must not be provided until a user has successfully provided with a valid user-ID and a valid password. Where systems software permits, every log-in banner must include a special notice, as a system-warning message. This notice must state:
"The system is to be used only by authorized users, and by continuing to use the system, the user represents that he/she is an authorized user. Legal and punitive action will be taken against all unauthorized users".

1.4.8.3 Authentication of Unattended File Transfer Processes

Software that performs unattended file transfer to or from other systems should authenticate the origin and destination file names as well as any user submitting the request unless the information being transferred is classified as Public.

1.4.8.4 Logging of Events on Restricted Information Systems

Security-related event logging should be done for all system platforms and all applications, which utilize sensitive information.

1.4.8.5 Overwriting Log Files

Log files should never be overwritten or deleted until they are backed up to off-line storage. Log files should be maintained as off-line storage till such time that the CISO and the Internal Auditor review them. In event that issues are identified in log file review, the log files should be archived and maintained till resolution of the issue. In case no issues are identified, log files may be deleted after clearance from the reviewing parties.

1.4.8.6 Activities to be logged

Log files should record at the least:

- Login failures
- Account lockouts
- All system or application administrator actions
- System or application start, stop, re-initialization (with user identity and time of action)

1.4.8.7 Frequency of Log File Review

Log files should be reviewed daily, or not less often than log file rotation or overwrite.

1.4.8.8 Access to Log-Files

Access to log files in both electronic and hard copy form should be limited as per "need-to-know" basis.

1.4.8.9 Network Security Monitoring

Monitoring of activity on the network environment should be performed by the Administrator-Network by employing network security tools in order to detect any abnormalities in network functioning in time, to take remedial action. For e.g.,

- Changes to Router configuration tables (such as address filtering of network traffic by the Router)
- Changes to Router configuration and access such as changes in password, should be set as alerts in network monitoring system
- Logging of Router availability loss for resolution of denial of service problems

1.4.9 Network Component Security

1.4.9.1 Identification and Restricted Use of Network Components

Administrator- Network should ensure that all network components are uniquely identifiable and restricted for their intended business function. This includes protection for all vulnerable points in the network.

1.4.9.2 Identification of communication lines

Hardwired communication lines (e.g., network lines, telephone lines, etc.) must be catalogued and be uniquely identifiable to the system being accessed to facilitate discovery of wiretaps.

1.4.9.3 Control of Physical Access to Network Equipment

All network and server equipment including LAN-servers, bridges, routers, switches, hubs, multiplexors etc., should be physically secured from unauthorized access by placing them in locked rooms or closets.

1.4.9.4 Location of Terminals for Performing Critical Functions

Where technically feasible, access to highly sensitive processing functions should be secured by limiting the terminals from which these functions should be executed and physically and / or logically restricting these terminals. These terminals should be secured by physical (e.g., keyboard locks) and / or logical (access control software) means when unattended.

1.4.10 Router security

1.4.10.1 Router Installation Standards

Following points represent the physical installation criteria designed to support the integrity of router operations:

- Ensure appropriate power supply delivery to unit, including recommended voltage, transient, current and interrupt considerations
- Ensure that environmental controls (temperature, humidity constants, emergency lighting, access leeway, etc.) are in accordance with manufacturer's recommendations.
- Verify the following while installing the routers,
    - Clean start-up
    - Validation of self-diagnostics
    - Avoidance of trouble indicators and
    - Positive indicators for the router installation

1.4.10.2 Router Initial Configuration

The initialization of the routers is only required on (1) initial installation, or (2) in the event of sudden and dramatic power loss and/ or failure of configuration data held in Flash memory.

Along with the installation guidelines given by the vendors, following configuration procedures should be considered:

- Number of ports configured on the router should not exceed either:
    - Physically installed ports or
    - Ports required to be used for different services.
- Firmware configuration must be limited to the flash memory specified for initial configuration.

1.4.10.3 Router Maintenance

The preventive maintenance controls and procedures for the routers include:

- Regular housekeeping upkeep, including a dust-free environment, removal of debris from immediate area etc. and the regular checks for integrity of cable installations, including attachment of cable ends, coiling of excess cable lengths, orderly cable runs, and cleanliness of connections
- Assurance of uninterruptible power supply (UPS), including maintenance of battery installations, cleanliness of power cord junctions and contacts, cleanliness and integrity of grounding straps and conduits, checks of case ground integrity, etc.
- Physical installation integrity, including tightness of rack mounting bolts and screws, slide hardware, and ancillary connections.

1.4.10.4 Router Administration

Authentication, identification and account management: The following procedures should be implemented:

- All login devices on the router should utilize password authentication before allowing the access. All login passwords should be encrypted.
- Multiple privilege levels should be defined to segregate administration duties as follows.
    - Every Network Administrator should only be allowed to access the level that has been approved by the Head-Infrastructure. Access rights should be governed by "least privilege" and "need to know" principles.

- The router access rights and privilege document should be prepared detailing the profile of each administrator and access rights for viewing of the router configuration and changing the router configuration.

- The router should be configured to log-off idle user sessions after a defined in-activity time-out limit so as to save the router resources and protect a back-door entry.
- The "secret password" utility/ feature should be used to protect the access to privileged and advanced commands on router. The secret password uses an improved encryption algorithm over the normal password.
- The router configuration tables should ensure that the first rule in Access Control List denies the traffic coming into internal network, which has an internal source IP address. This is to prevent an attack by the intruder who can spoof or trick the router to think that the packet is coming from an authorized network, sub-network or host computer.
- IP source routing must be disabled on the router, else 'source route' packets would bypass the filtering rules defined in ACL on the router.
- The router should deny all services except the minimum required for functioning of company

Access Control:

- Access rights procedures and password controls should be implemented for providing access and privileges for creating, modifying, maintaining and reviewing the router access control list (ACL). The router tables and ACL should be accessed from specific hosts on the network and access should be allowed only to Administrator-Network.
- Simple Network Management Protocol (SNMP) access, normally used to query the router for operational information as well as updating the router configuration, should be secured with an access control list.
- The access control list on the router should be mapped with security policies and procedures and filtering rules defined in firewall system.
- Suitable warning banners and messages should be displayed upon any attempted access to the router and router tables, specifically marking them as "Private" and declaring such access as "Illegal" or "Unauthorized".
- Access to router connecting to the Internet should be controlled by an ACL. The packet filtering rules should be enabled on this router to block "127.0.0.1" (loop-back address), to minimize the threat of "IP spoofing" as Denial of Service (DoS) attacks utilize loopback address to get into the network.

Router Integrity and availability:

- Current versions of router configuration files should be stored on a secure place (server) and reviewed periodically.
- The services and ports enabled at the router should be mapped with the ACL and the rules therein.
- The router should run the current version number (major and minor) of the operating system to ensure that vendor security patches and upgrades are applied in a timely manner.

- If supported by the router, the TCP Intercept feature must be enabled to prevent the TCP SYN-Flood denial of service attacks so that the open connections are intercepted well in time and SYN-flooding is prevented.

Auditing, logging and monitoring the routers

- The accounting and auditing feature should be enabled with appropriate parameters and levels for generating audit logs and monitoring the user activity on router. Following router logs should be monitored:
    - Any attempt to access or use the service specifically denied by the router
    - Outside data packet with the IP address of the computer inside the LAN
    - Send / receive the data from IP address not list
- The audit trails should be logged from a router to a secure host computer (syslog server) within the network to enable real-time monitoring.

Router Documentation:

- To administer a router in a secure and consistent fashion, rules should be documented about acceptable traffic. This policy should, in turn, define, for each router, the types of traffic that will be allowed (rest of the traffic will have to be denied). The router documentation should detail the following particulars:
    - Rule
    - Direction (in/ out)
    - Source address
    - Destination address
    - Protocol
    - Source Port & Destination port
    - Acknowledgement sent (Yes/ No)
    - Action (permit/ deny)
- Configuration changes to the router should follow standard change control procedures and documentation.