POWERING TAMILNADU'S PROGRESS...

IT Security Policy

Version 2.0

TAMIL NADU ELECTRICITY BOARD LIMTED
TANGEDCO & TANTRANSCO

144, ANNA SALAI,
CHENNAI- 600 002, TAMIL NADU, INDIA

Document drafted by

SETS

Society for Electronic Transactions and Security

MGR KNOWLEDGE CITY, CIT CAMPUS,
TARAMANI, CHENNAI - 600113.

PREPARED BY:

Shri. Krishnan Muthu Kumaran, Security Analyst

UNDER THE GUIDANCE OF:

Shri. Karthikeyan Shanmugam, Senior Security Analyst

1 Document Versioning

S.No.	Title	Version
1.	IT Security policy for Tamil Nadu Electricity Board	2.0

Table of Contents

1 Document Versioning 3

2 Executive Summary 7

3 Introduction 8

3.1 Scope 8

3.2 What is Information Security Policy? 8

3.2.1 How Information security policy is approached? 8

3.3 Information Security Policy Framework 9

4 Roles & Responsibilities 10

5 Enforcement & Violation Handling 10

6 Management Policies 11

6.1 Security Policy Program Management 11

6.2 Security Assessment and Authorization 12

6.3 Risk Assessment 12

6.4 System and Service Acquisition 13

7 Operational Policies 14

7.1 Awareness and Training 14

7.2 Configuration and Change Management 14

7.3 Contingency Planning 15

7.5 Collection, Retention, and Classification of Electronic Data 16

7.6 System and Data Security Maintenance 17

7.7 Media Protection 18

7.8 User Security 18

7.8.1 Third Party Access 19

7.9 Privileged Administrative Access 19

7.10 Physical and Environmental Protection 19

7.11 Software Licensing and Usage 20

7.12 Supply Chain Protection 20

7.13 System and Information Integrity (Vulnerability Management) 20

7.14 System Development 21

8 Technical Policies 21

8.1 Audit and Accountability 21

8.2 Backup and contingency 21

8.3 Encryption 22

8.4 Firewall 22
8.5 Identification, Authentication, and Access Control 23
8.5.1 Access Control 23
8.5.2 Account Administration 24
8.5.3 Identification and Authentication 24
8.6 Passwords and Passphrases 25
8.7 Screen Saver Usage 25
8.8 Security Breach Mitigation 26
8.9 Infrastructure Protection 27
8.10 Intrusion Detection and Prevention Systems (IDPS) 28
8.11 Virus Detection 28
8.12 Wireless Communications 29

9 Acceptable Use 30
9.1 General Principle 30
9.2 Organization Ownership 31
9.3 User Privacy 31
9.4 Confidential Information 32
9.5 Incidental Personal Use 33
9.6 Prohibited Use 33
9.7 Information System Security 34
9.7.1 Electronic Messaging Systems 35
9.7.2 Internet and Intranet 36
9.7.3 Remote Access 36
9.8 Violations 36

10 Acceptable Encryption Policy 37

11 Risk Assessment Policy 39

12 Clean Desk Policy 40

13 Digital Signature Acceptance Policy 42

14 Disaster Recovery Policy 44

15 Email Policy 47

16 End User Encryption Key Protection Policy 49

17 Password Protection Policy 53

18 Security Response Plan Policy 57

19 Remote Access Policy 60

20 Router and Switch Security Policy 62

21 Wireless Communication Policy 66

22 Web Application Security Policy 68

23 Information Logging policy 72

24 Server Security Policy 76

25 Software Installation Policy 79

26 Technology Equipment Disposal Policy 81

27 Change Management and Control Policy 84

28 Software Development Policy 89

29 Acceptable Use Policy 92

30 Procedure Memorandum for E-mail Management 98

31 Procedural Memorandum for Information Logging 109

32 Procedural Memorandum for Firewall 110

33 Procedural Memorandum for IDS/IPS 113

34 Procedural Memorandum for Securing the Web Server 115

35 Procedural Memorandum for Sever Operating System 124

36 Procedural Memorandum for Workstation Operating System Security 134

37 Conclusion 156

38 Reference 157

39 Appendix A: Glossary and Acronyms 145

40 Appendix B: Incident Reporting Procedures 163

2 Executive Summary

The objective of the TNEB Information Security Policy is to define and describe the responsibilities and required best practices for all members of the organization with respect to information security and the protection of organization information.

The policy comprehensively applies to all individuals in the organization and all forms of information resources. It describes, based on an individual's role, the responsibilities of members of the organization to prevent unauthorized access to physical and electronic information, consistent with regulation and organization policies.

The policy also outlines the responsibilities of those who are responsible for implementing, enforcing and abiding by this policy. The Procedures for the Protection of organizations Information, incorporated by reference, describe the specific procedures required to comply with the policy.

3 Introduction

3.1 Scope

This policy covers all the use of Information Technology and all the by which accessed. This policy applies to all staff and employees and visitors of the TNEB. This policy applies to all use of IT on TNEB premises even if the organization doesn’t own the equipment.

This policy applies to all IT provided by TNEB wherever it takes place. If the equipment or information is provided by the organization this policy applies wherever in the world the activity takes place.

3.2 What is Information Security Policy?

Information Security Policy is a document that states how an organization plans to protect the organization's physical security and information technology (IT) assets. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change.

A organization's security policy may include an acceptable use policy, a description of how the organization plans to educate its employees about protecting the organization's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

3.2.1 How Information security policy is approached?

Management’s biggest challenge lies not in the writing of specific policies and standards but in the orderly development and implementation of policies and standards. An organization can increase the odds that its information security policies and standards will actually influence security by adhering to the following seven “requirements.”

- Step 1: Identifying the organizational issue that impact information security policy
- Step 2: Identifying the various classes of policy users This policy covers ALL the use of Information Technology and ALL the ways by which Electronic Information is accessed
- Step 3: Organizing information security policies into categories
- Step 4: Reviewing the draft policies with management, users and legal counsel
- Step 5: Train all various classes of policy users on information security policies
- Step 6: Enforce the information security policies
- Step 7: Reviewing and modify policies atleast annually

3.3 Information Security Policy Framework

TNEB is a power generation and distribution company owned by Government of Tamil Nadu. TNEB was formed on 1st July 1957 as the Madras State Electricity Board according to the Electricity Supply Act of 1948 as a successor to the erstwhile Electricity Department of the Government of Madras under the authority of the Department of Power. It was responsible for electricity generation, distribution and transmission, and it regulated the electricity supply in the state. Later it was renamed Tamil Nadu Electricity Board.

In October 2008, the Government of Tamil Nadu decided to divide TNEB into two subsidiaries. On 1 November 2010, TNEB Limited became a holding company with two subsidiaries, Tamil Nadu Generation and Distribution Corporation Limited (TANGEDCO), responsible for power generation, and Tamil Nadu Transmission Corporation Limited (TANTRANSCO), responsible for power transmission.

Tamil Nadu Electricity Board (TNEB) has the ability to create and access a wide range of physical and information technology (IT) Assets. The overall aim of the policy is to ensure that: -

- The required level of confidentiality is always maintained
- The integrity of information is always protected
- The information is always available to authorized users.

4 Roles & Responsibilities

Chief Engineer of Information Technology will be appointing a CISO. The CISO will be responsible for developing, implementing, and administering information security program, reporting all organization information systems security incidents, risks, and vulnerabilities to the Head of the management and CERT-In.

The designation of the CISO is intended to establish clear accountability for the development and implementation of policy for information systems security management activities, provide for the coordination and assessment of the organization information security program, and ensure greater visibility and transparency of such activities within users.

The CISO maintains authority to elevate the organization security posture to appropriate levels in response to security threats. The CISO has jurisdiction over security related events, functions, vulnerabilities and threats and may execute system from the organization networks, Internet/Intranet sites, servers, or workstations.

The CISO has authorization in the implementation of automated physical security systems that may integrate with Department of IT identity management and credentialing systems (with the Facilities Management Department, Human Resources, or other). When a unified credentialing system that also gives user access to information systems is adopted and implemented, then the CISO becomes the managing entity and authority for issuance of the credentials.

5 Enforcement & Violation Handling

Violations of this security policy shall be reported to the appropriate management and the CISO. Management will be conducting regular audits and actively monitor for violations of this policy. Violations may be defined as an act or event that exposes the organization or agency to actual or potential damage through the compromise of information systems security, the disclosure of sensitive or confidential information, the unauthorized use of organization data or resources, and the use of information systems for personal gain, unethical, harmful, or illicit purposes. Other events defined as violations may include, but are not limited to, the theft, loss, unauthorized use or misuse, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denial of service of organization information or information systems.

Organization personnel regulations require that employees abide by applicable laws, regulations, and standards of conduct. Intentional violations, regardless of the number of violations, may result in disciplinary action up to and including termination. Organization maintains the right to refer information security incidents to external authorities and to seek legal action against personnel that misuse organization information systems in a manner that violates law and applicable policy.

6 Management Policies

6.1 Security Policy Program Management

TNEB has been authorized a CISO position with the mission and resources to coordinate, develop, implement and enforce information security policy program. The CISO shall develop formal information security policies and procedures that address purpose, scope, roles and responsibilities, management commitment, coordination among agencies and departments and operational and technical controls to ensure compliance consistent with applicable directives, policies, regulations, standards, and guidance.

The security policy and procedures shall define minimum acceptable parameters for the implementation and use of information technology, communications systems and data (sometimes referred to as 'IT assets' and 'content') authorized boundaries- technical and behavioral provide an overview of security requirements for information systems, describe security controls in place for mitigating risk and achieving compliance, and be formally approved by authorized or delegated officials.

The Security Policy, procedures and related guidelines shall be periodically reviewed for effectiveness of security controls, roles and responsibilities and it shall be updated for its holding company's. TNEB Limited became a holding company with two subsidiaries, Tamil Nadu Generation and Distribution Corporation Limited (TANGEDCO) and Tamil Nadu Transmission Corporation Limited (TANTRANSCO).

Developed information system security policies, procedures, and other guidance shall be Published centrally to organization intranet readily available to all users.

6.2 Security Assessment and Authorization

The CISO will be developing formal and documented security assessment and authorization procedures and strategies that address purpose, scope, roles and responsibilities, management commitment, coordination among agencies and departments, and operational and technical controls to ensure compliance consistent with policy, and applicable directives, operational policies, regulations, standards, and guidance.

CISO will be reviewing assessment, policies, procedures, and strategies annually by determing the effectiveness of existing security controls and team roles and responsibilities. TNEB leadership will be determining personnel authorized to determine the acceptable levels of risk to operations and information assets to guide the implementation of appropriate security controls. Organization leadership will be formally authorized connections from information systems to external information systems through interconnection security agreements such as Service Level Agreements, Firewall Rules Requests, Exceptions to Policy etc. Requests will be including details of specific to each connection including the system or data source being connect to the interface characteristics, security requirements, and type of information transmitted. Interconnections will be monitored to verify enforcement of security use policy, controls and requirements.

The organization Security program shall include a configuration management process, determinations of impact of changes to information systems and operations, monitoring, ongoing security control assessments, and reporting the security state of information systems.

Refer to the considerations outlined in Web Application Security policy and Change management and control policy.

6.3 Risk Assessment

The CISO will be developing a risk assessment program that addresses the purpose, scope, roles and responsibilities, management commitment, technical controls and procedures, and adequate coordination with agencies to ensure adequate security controls consistent with applicable directives, policies, regulations, standards, and guidance.

The CISO shall be initiating and/or conduct initial risk assessments for new information systems to determine the likelihood and magnitude of harm in the event of unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information processed, stored, or transmitted. Risk analyses and assessments of information and systems shall include determination of values associated with critical infrastructure and other information system assets, the associated vulnerabilities and threats to the information and systems, the probability and impact of potential threats, and cost benefit comparisons of impacts and associated countermeasures.

Refer to the considerations outlined in Risk Assessment policy.

6.4 System and Service Acquisition

TNEB systems and service acquisition process shall be referring the IT Security Policy as per the requirement. TNEB will be acquiring IT products, solutions and services shall include a determination of information security requirements and should include clear delineation and understanding of roles and responsibilities of the vendor/contractor/solution provider and the agency staff, reference to the TNEB regulation. Organization will be ensuring adequate security controls are included in the solution, Implementation process of the solution and maintenance/support services consistent with applicable local laws and policies.

Software services vendors and manufacturers will be demonstrating that acquired products, components, applications, and services employ the necessary security compliance standards, quality control processes, and validation techniques, and provide necessary documentation related to the use, configuration, installation, operation, and use and maintenance of security features and functions of an acquired product, component, or service. Services provider/implementers must adhere to implementing the standards in the solution required by Policy, or if not available, work with the organization for a mitigating resolution or Waiver if necessary. Providers of external information system services (hosted, WEB-based, or ‘Clouds’) are comply with organization information security requirements and employing appropriate security controls in accordance with applicable directives, policies, regulations, standards, and guidance. Contracts will be defining TNEB oversight, internal and external user roles and responsibilities, and processes to monitor security control compliance by external service providers.

The application of information system security engineering principles in the design, development, implementation, modification, and operation of TNEB information systems integrated throughout the entire system development lifecycle (SDLC). The systems development lifecycle shall include the development of effective security policy, architecture, and controls as a foundation, define physical and logical boundaries, and incorporate security throughout the entire system lifecycle.

Refer to the considerations outlined in Software Development policy.

7 Operational Policies

7.1 Awareness and Training

Information security awareness and training program will be incorporated as part of the TNEB training and education programs for employees and others to educate the user community in the issues related to vulnerabilities and cyber-security breach risks associated with information technology, and the importance and methods of protecting organization information and information systems. Security awareness will be continually emphasized, reinforced, updated, and validated.

New users of TNEB information systems should attend or participate in an approved Information Technology and Information Security Awareness orientation training class within 90 days of being granted access to any TNEB information systems. Users shall receive security awareness training and sign an acknowledgement indicating they have read TNEB information security policies. Records or certifications indicating the completion of security awareness training shall be retained for TNEB users. The information security policies, procedures, and other guidance are centrally managed and readily available to all users, administrators, and other stakeholders.

7.2 Configuration and Change Management

IT systems are been designed, configured, hardened, and maintained according to organization System Hardening Standards to adequately safeguard information to the extent possible or feasible. Baseline configurations and configuration deviations of TNEB information systems, network devices, and communications infrastructure shall be documented, reviewed, and updated. General requirements include, but are not limited to, installing operating systems from approved sources and media, applying vendor patches, removing or disabling unnecessary software and services, enabling audit logging and other security protections, and changing the passwords and usernames of default accounts.

System Administrators shall analyze hardware and software for flaws, weaknesses, incompatibility, and other security or functionality impacts and vulnerabilities in a test environment prior to an implementation into the production environment. Security functions shall be reviewed and verified after changes to systems have been implemented to ensure the functions and features are implemented correctly, operating as intended, and producing the desired result.

Changes to TNEB information systems shall be implemented after a security impact analysis to be conducted to include a risk assessment and determination if additional security controls need to be implemented. Mandatory configuration settings within the information system will be maintained using Configuration baseline standards and security configuration checklists that reflect the approved operational requirements. Exceptions from the mandatory configuration settings for systems, components, and services will be formally requested, documented, and approved by the organization. Information system configurations shall provide only the necessary capabilities by restricting the use of unnecessary functions, ports, protocols, and services.

Inventory and Asset tracking systems implemented and information System Assets are been identified numbers affixed in obvious locations as possible. For making modifications, additions, and/or the removal of network Management devices and configurations. If required, approval must be obtained through the TNEB Configuration and Change Management Procedures. Modifications and additions to network infrastructure shall be governed by a change management process. Configurations for systems, software, hardware, infrastructure, and peripherals shall be formalized, documented, and periodically reviewed.

Refer to the considerations outlined in Change management and control policy.

7.3 Contingency Planning

IT infrastructure and critical information systems should have a viable Continuity of Operations Plan (COOP) and a Disaster Recovery Plan to continue an ability to function in the event of an IT emergency or interruption, and, to respond to and enable the restoration of vital operations and resources in a reasonable time. Organization will identify information systems processing and data storage plans which include alternative site(s) for essential systems that permit the restoration of information systems in the event of an interruption, failure, or compromise to the TNEB primary processing site. A prioritization of critical system restoration for various situations should be included.

TNEB will be maintaining contingency plans for information systems used for essential missions and business functions. Contingency plans shall include the identification of critical infrastructure systems and functions, provide restoration priorities and expected timeframes, address staff roles and responsibilities in the event of a disaster, consider alternatives to maintaining essential mission and business functions during an interruption, compromise, or failure and address the eventual information system restoration without deterioration of the security measures originally defined.

TNEB will be designing network and telecommunications that minimizes wholesale network disruptions, and establish alternate back-up services to resume information system operations for essential mission and business functions when the primary network/telecommunications capabilities are unavailable. Management shall determine the necessity and acceptable risk for their systems and ensure the necessary allocation of personnel and resources for the development and maintenance of a COOP for critical information systems supporting of essential business functions.

Refer to the considerations outlined in Disaster Recovery Policy.

7.5 Collection, Retention, and Classification of Electronic Data

Organization information systems contain electronic/digital data and information – “data”. Any data within any TNEB information or communications systems is the property of TNEB. Employees, contractors, partners, and any people that have access and use TNEB information systems and data must comply with the retention of records requirements and must categorize records appropriately to ensure the appropriate disposition of specified records at the end of the applicable scheduled retention period. Information stored electronically or on paper shall be evaluated for criticality and sensitivity. The criticality of data shall identify the degree to which the organization depends on the data for continued operations or even survival. Physical marking, labeling, or other notation is required to identify all documents, email, media, or reproductions of confidential information. Information not specifically labeled will be treated as Internal Use information. Collections of information from various sources with multiple classifications shall be classified at the highest sensitivity level of the information included.

Authorized personnel shall ensure that publicly accessible information does not contain non-public information such as information protected by law. Authorized personnel shall review all content proposed to be published to a publicly-accessible information system prior to release. Sensitive or Confidential information may not be removed on media from TNEB premises unless the information owner has approved in advance. Media may include, but is not limited to, external hard drives, flash drives, floppy disks, CDs, DVDs, magnetic tape cartridges, and paper documents. Data owners shall ensure that security measures are implemented prior to the transmission of Confidential or Sensitive information to destination systems and that destination systems are adequately secured according to the adequate protection requirements.

Refer to the considerations outlined in Clean Desk Policy, Procedural memorandum for information logging and E-Mail Management.

7.6 System and Data Security Maintenance

The confidentiality, integrity, and availability of TNEB information are sustained through information system maintenance policies and procedures for systems installed on-site, at remote sites, or through remote third-party processes.

Maintenance procedures should be documented. Maintenance records should be kept and include the date and time of maintenance, name of individual performing maintenance, a description of maintenance performed, and a list of any equipment removed or replaced. A log of any persons requiring escort that are not pre-authorized/budged is required if access is needed in a secure facility. System functionality, security controls, and approved baselines must be tested and validated after maintenance or repair. Maintenance agreements through TNEB contracts shall include reference to the TNEB IT Security policy. When spare parts equipment maintenance is required, system owners must explicitly approve the removal of any devices or formats from TNEB information systems requiring maintenance. Hard drives, storage media and other devices shall be sanitized prior to removal from facilities and prior to the release to vendors or maintenance personnel for maintenance to prevent unauthorized disclosure of data and minimize impacts to the confidentiality, integrity and availability of TNEB information systems and data.

Maintenance personnel, to include manufacturers, contractors, vendors, and other personnel, shall hold formal access authorization from designated TNEB personnel to conduct maintenance on TNEB information systems, components, and software. Personnel authorized to escort maintenance personnel shall have the necessary technical competence to supervise information systems maintenance.

7.7 Media Protection

Information systems, diagnostic tools and applications, and data storage devices must be approved for use to access TNEB systems and information. Information systems and devices may not be connected to the TNEB network infrastructure unless accredited and approved. Personally-owned devices such as music players, PDAs, memory devices, USB drives or similar, smart phones, tablets, and cameras are prohibited from being connected to resources unless authorized through a formal approval process. TNEB information stored on decommissioned hardware and storage media shall be irretrievably destroyed, in a manner to permanently and irreversibly delete data to prevent access by unauthorized individuals. Storage media may include, but is not limited to, hard drives, storage systems, removable disks, floppy disks, CDs, flash drives, and other forms of removable media and storage devices. Sanitization requirements will be determined by the system profile of the device to be decommissioned and the sensitivity level of the information processed or stored. Storage media and devices shall be sanitized prior to the release to vendors or maintenance personnel for maintenance to prevent unauthorized disclosure of data.

7.8 User Security

Access to TNEB information and systems shall only be granted to authorized users who include all employees – merit or non-merit, technical support or end-users, authorized contractors, and volunteers with a valid access need to perform official duties. TNEB employees and contractors that are authorized perform privileged user functions, such as developing, implementing and/or administering information systems, shall sign and acknowledge the requirements of acceptable use and privileged use. TNEB employees and contractors sign agreements defining the acceptable use of information systems and information protection requirements to assist in deterring the unauthorized disclosure of TNEB Confidential, Sensitive, and Internal Use information and mitigating risk to TNEB information systems.

Refer to the considerations outlined in Acceptable use policy.

7.8.1 Third Party Access

Third parties shall only use TNEB information and systems for the purpose of the business agreement and any other TNEB information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others. Unless allowed in the contract, a third party may not give access to or distribute TNEB systems, information and data to another third party without permission. Compliance with contracts and third-party agreements shall be monitored.

Third party vendor accounts and maintenance equipment on the TNEB network that connects to the Internet, telephone lines, or leased lines shall be disabled when not in use for authorized maintenance or support. Software and hardware used by third parties providing services to TNEB shall be properly inventoried and licensed. Contractors found to be in violation of TNEB policies will have their systems access revoked, devices confiscated, and may also be removed from the TNEB engagement.

7.9 Privileged Administrative Access

Inactive privileged system accounts or privileged user accounts shall be reviewed and disabled according to TNEB policy. Administrative users shall not misuse their administrative privileges, and specifically not use their privileges to circumvent security policy.

7.10 Physical and Environmental Protection

Facilities that host critical information system should be a secure environment with access restricted to authorized personnel. Access to information systems facilities may be further restricted by the CISO upon actual or potential security threats, events, or circumstances. Signage for restricted access areas and locations shall be practical and clear but the importance of the location shall be minimally discernible.

Access to information systems facilities shall be granted only to TNEB employees and contractors whose job responsibilities require access to that facility through controlling mechanisms. Visitors shall be escorted in restricted areas of information system facilities. Individuals granted unescorted access to an information systems facility shall sign any required facility access agreements.

Physical access to information system infrastructure, distribution and transmission lines within facilities shall be controlled to assist as a preventive measure to accidental damage, disruption, and physical tampering. Emergency power shutoff capabilities shall be protected from unauthorized or unrestrained activation.

7.11 Software Licensing and Usage

Commercial software that has not been acquired through official TNEB procurement process or channels is prohibited and cannot be installed on any TNEB system to include websites. Copyrighted software for which TNEB does not have specific approval to use shall not be installed or stored on TNEB information systems. Systems administrators will remove any software determined to be unlicensed or unapproved. Users should not download software products or unauthorized open source from the Internet without approval from the system administrator, unless it is required to view/receive/read documents and information from that source that includes a step to allow the download. TNEB employees and contractors shall abide by all software and product license agreements and not illegally copy or distribute software. TNEB authorized to remove any unlicensed or unapproved software from any TNEB information system. TNEB may initiate an investigation when illegal or unauthorized software is found on systems.

7.12 Supply Chain Protection

IT Security policies and standards shall be applied for information systems, components, and products whereby they do not violate license agreements and warranties. TNEB may conduct review of contractual agreements that involve IT products/services supply chain process for integrity and vulnerability assessment that may compromise its use. All firms, vendors, contractors, consultants either supplying IT or communications products to TNEB or supplying staff resources (contractors/consultants) are required to adhere to TNEB IT Security Policies.

7.13 System and Information Integrity (Vulnerability Management)

IT Systems and data must be protected from unauthorized use, hacking, malicious activity that may interrupt services, compromise data. TNEB shall identify, report, and correct system flaws, vulnerabilities, or incidents in compliance with local laws, policies, directives, and guidance. The process for identification, reporting, and remediation of vulnerabilities and flaws shall be timely as per CERT-IN guidelines. Delegated personnel shall receive information system security alerts, advisories, and directives from vendors, approved vulnerability advisory councils, and other organizations on a reoccurring basis. Security alerts, advisories, and directives shall be disseminated to personnel responsible for administering information systems and a timeframe shall be determined for implementation within the approved Configuration and Change Management process. Integrity verification applications and tools shall be employed to inspect information for tampering, errors, and omissions. Operational policies and technical implementations shall be utilized to monitor the integrity of TNEB system and applications.

7.14 System Development

TNEB systems shall be developed and maintained in accordance with the Systems Development Life Cycle, utilizing the Systems Development Life Cycle Standards (SDLCS) or similar. Systems shall maintain access control features to restrict access in accordance with the concept of least privilege. Application-program-based access paths other than the formal user access paths shall be deleted or disabled before software is moved into production. To ensure proper segregation of duties, owner responsibilities shall not be delegated to the custodian.

Refer to the considerations outlined in Software Development Policy.

8 Technical Policies

8.1 Audit and Accountability

System administrators and data owners shall review event logs on a periodic basis to detect unauthorized access attempts, unauthorized system changes, performance anomalies, and other events. TNEB information systems and network devices shall maintain centralized time synchronization with an approved time source server to ensure the generation of consistent time stamps across auditable event data. Access to auditable security related event data shall be limited to authorized personnel and protected through methods such as encryption and system backup to ensure the confidentiality, integrity, and availability of auditable events.

Refer to the considerations outlined in Server Security, Procedural memorandum for information logging and Server operating system.

8.2 Backup and contingency

Part of IT Security management includes having appropriate processes for backing-up data, assuring the integrity of systems functionality, and maintaining operations. The data back-up process must use secure transport to ensure the integrity of the data. Backups of TNEB

Confidential and Sensitive information that is stored shall be encrypted. TNEB shall maintain appropriate backup, contingency and continuity of business plans for recovery of systems in the event of a disaster based on risk assessments and business requirements. Backup and recovery processes shall be documented, tested, and periodically reviewed.

8.3 Encryption

Encryption usage requirements shall consider the type and classification level of information, laws that govern protection requirements, storage location or media type, transmission medium and internal requirements for the timely and continued availability of information. Organisation shall establish standards and procedures that address when encryption, digital signatures, and digital certificates shall be used in accordance with local laws and policies and guidance. Organisation shall use open-standard based encryption algorithms to share encrypted data internally and externally for data that requires encryption to support interoperability needs.

Confidential or Sensitive data shall be encrypted during transmission using encryption measures strong enough to minimize the risk of the unauthorized disclosure if intercepted or misrouted. Secure transmission methods shall be used to distribute decryption capabilities to the recipients of encrypted data. Options may include a public key infrastructure or a separate communication that includes a verification of the identity of the recipient. Organisation implementations of storage or transmission encryption shall include an encryption key management plan to protect the confidentiality, integrity, and availability of information. Encryption key management plans shall ensure that data can be decrypted in the event of loss or unavailability of cryptographic keys. Encryption key management plans shall address the handling of keys suspected or confirmed to be compromised. The plan shall address what actions will need to be taken in the event of a compromise, to include impacts to any system software and hardware, existing cryptographic keys, and existing encrypted data.

Refer to the considerations outlined in Acceptable Encryption Policy, Digital Signature Policy and End User Encryption Key Protection Policy.

8.4 Firewall

In order to protect and manage access between the networks and the Internet, Firewalls and other access control devices are a critical component. Firewalls control access to internal and external IT resources. Access control devices, such as firewalls, which filter network traffic, shall segment the internal network infrastructure to support access policies.

Firewalls shall be configured to deny all traffic by default and permit only those services approved by the organization. Access to internal information systems from any external network shall be limited only to services and protocols necessary for mission critical operations of information system resources. Ports and protocols that have inherent vulnerabilities and are unnecessary for business system functionality shall be denied implicitly at firewalls. E-commerce servers including payment servers, database servers, and Web servers shall be protected by firewalls in a demilitarized zone (DMZ). Firewall change requests shall be documented through established change management procedures and approved only when a clear business requirement or impact has been determined and a risk analysis has been performed by the organisation.

TNEB firewalls shall be physically and logically protected to ensure only authorized personnel have access. Firewall administrators shall maintain and use individual accounts and passwords to authenticate to the firewall in accordance with access management and password policies. Firewall configurations should be archived as part of configuration management and disaster recovery requirements.

Refer to the considerations outlined in Procedural memorandum for Firewall and Web server.

8.5 Identification, Authentication, and Access Control

8.5.1 Access Control

Data and system owners shall implement operational procedures and technical controls to ensure access to TNEB information and systems is based upon the principle of least privilege and an authorized need to know and access. The principle of least privilege, providing only the access necessary to perform assigned duties, shall be implemented to ensure the confidentiality, integrity, and availability of TNEB information systems and data.

Authorization to create a user ID and password must be received from a designated approval authority. Requests for user, administrative, and system access must be approved according to formal access request procedures. Remote access to TNEB information resources shall be capable only through approved and encrypted remote access implementations to ensure the confidentiality and integrity of remote access sessions. TNEB shall monitor for unauthorized remote access and violations of usage restrictions. TNEB may confine wireless communications to organization-controlled boundaries and monitor for unauthorized wireless connections.

TNEB shall scan for unauthorized wireless access points and take appropriate action if an unauthorized connection is discovered. TNEB shall disable internal wireless networking capabilities embedded within information systems or components when not intended for use in mission or business functions.

8.5.2 Account Administration

Provisioning of credentials (usernames/passwords) that grant access to organization networks shall be maintained exclusively. Requests for information system accounts shall maintain a formal and valid access authorization based on approved intended system usage within personnel mission and business functions. Information system accounts shall be categorized based upon the access type and level of privilege required. Types of accounts may include user, system, application, guest, group, and temporary accounts.

Users shall be assigned a unique account and user ID. Credentials shall not be shared or written down. Accounts inactive for 60 days shall be disabled. Accounts for individuals on extended leave for more than 60 days shall be disabled unless specifically approved through the formal exception to policy process. TNEB shall maintain a formal process to modify user accounts to accommodate events such as name changes, accounting changes, and permission changes. TNEB information systems shall enforce account lockouts when a determined threshold of consecutive invalid login attempts by a user is exceeded. In this instance, accounts shall not be unlocked until released by an administrator.

Account management events, to include the creation, modification, and disablement of accounts, shall be audited and notifications sent to appropriate personnel. TNEB shall audit relevant account management events for abnormal time-of-day activity, duration, excessive privilege, and other a typical usage by information system accounts.

8.5.3 Identification and Authentication

TNEB information systems shall enforce complexity requirements for all user, administrative, and system account passwords. Complexity requirements shall ensure a minimum of 6 characters, to include uppercase letters, lowercase letters, numbers, and special characters when technically feasible for the system. Passwords shall be treated as confidential information and be encrypted in storage and transmission. Password minimum and maximum lifetime restrictions shall be enforced and password reuse prohibited or minimized. Access to all TNEB information systems, including but not limited to, databases, operating systems, applications, and file systems, shall require authentication with valid credentials.

User and System IDs, including administrator, system or service accounts, and network device IDs, shall have a private authenticator assigned. Default passwords shall be constructed in accordance with this password policy and changed immediately upon first logon. In the event the integrity of a password has been compromised, or suspected of compromise, the password shall be changed immediately.

8.6 Passwords and Passphrases

TNEB information systems enforce complexity requirements for all user, administrative, and system account passwords. Users shall ensure to use a minimum of 6 characters when creating passwords, to include uppercase letters, lowercase letters, numbers, and special characters when technically feasible for the system. TNEB information system users shall properly protect passwords from unauthorized disclosure or modification. Passwords shall not be shared with anyone internal or external.

Users are required to maintain password secrecy. Passwords shall not be written down or stored in an unapproved retrieval system without proper security controls. Users shall not reveal their passwords in either electronic or verbal communications. Passwords for all general user and administrative accounts shall be changed every 90 days and password reuse minimized according to system specifications. System and service accounts shall comply with the same requirements unless specifically approved through the formal exception process.

Refer to the considerations outlined in Password Protection Policy.

8.7 Screen Saver Usage

Screen savers are required to protect systems from unauthorized access and must be applied. Department of IT may force screen savers through system policy on TNEB information systems. User authentication shall be required to unlock the screen saver. Screen saver timeout thresholds shall be enabled and set in accordance with the TNEB standard image for workstations. Screen saver settings may not be modified without written authorization.

Screen saver images or desktop images will be removed if discovered to contain offensive or malicious content as defined in policies regarding inappropriate content, or if determined to introduce unnecessary threats or vulnerabilities that could degrade the performance of the enterprise information infrastructure or system.

8.8 Security Breach Mitigation

TNEB shall carefully assess the probability of unauthorized alteration, disclosure, or loss of information for which they are accountable and responsible. Organisation should perform security risk assessments for agencies business processes and operations. Security assessments shall be performed only by approved Department of IT personnel, contractors, and vendors. Department of IT shall use automated system tools that provide real-time notification of detected misuse, vulnerability exploitation, and unauthorized intrusion. Security baselines shall be developed and tools will report deviations and exceptions to policy. Department of IT shall deploy, maintain, and monitor security devices that will inspect Internet traffic and usage, email traffic and content, LAN traffic, protocols, and device inventory, and operating system security parameters and controls.

System and security event logs from various sources shall be collected and monitored for indications of misuse, intrusion, vulnerabilities, and misconfigurations. Log sources may include intrusion detection and prevention systems, firewalls, domain controllers, access control devices, vulnerability assessment utilities, file and member servers, applications, backup systems, printers, fax machines, workstations, mobile communication devices, and other services and systems.

Authorized security personnel are authorized to perform security assessment or penetration tests against systems and infrastructure and management approval to include password strength determinations, scanning for unauthorized and non-compliant devices and infrastructure, inappropriate sharing of devices, vulnerability determinations, and other assessment activities.

Organisation shall be granted physical and logical access to all facilities and systems required to respond to security issues and events, appropriately conduct assessments, perform and support investigations, and other security related functions.

Security violations, concerns, suspected and confirmed instances of successful or attempted intrusions shall be immediately reported, who will investigate. System anomalies in system performance are normally indicative of system compromise and must be reported to the Department of IT Service Desk.

Refer to the considerations outlined in Procedural memorandum for workstation operating system.

8.9 Infrastructure Protection

Department of IT shall be responsible for all aspects of the TNEB network infrastructure and will manage and administer all future developments, implementations, and enhancements to this infrastructure. Modifications, additions, and the removal of network management devices and configurations shall not be made without the approval of Department of IT and shall be governed by Configuration and Change Management processes and procedures. Department of IT will establish operational and technical methods of protecting against unauthorized connections to the enterprise IT environment. Network device addresses, services, and approved ports and protocols are allocated, registered, and managed centrally by Department of IT. Non-sanctioned or non-standard protocols shall be approved by Department of IT and the Information Security Office.

TNEB internal network addresses shall remain private and protected using Network Address Translation. Systems requiring access to external networks shall have private addresses translated to a legal registered public address prior to transmission. Interconnections of network infrastructure with external third party networks shall be approved by agency management, submitted through the Change Management process. This includes connections to external telephone networks. Routers, switches, hubs, taps, wireless access points, or any other network infrastructure devices shall not be installed on the TNEB network without approval from Department of IT. Network infrastructure or information systems that provide services shall not be extended or re-transmitted without Department IT approval. Information systems shall prevent access to system management functionality from general users through access control mechanisms. Information systems shall protect against or limit the effects of Denial of Service (DoS) attacks by implementing technical controls and managing excess capacity, bandwidth, utilizing protection mechanisms against IP spoofing, implementing access filters, and establishing connection limits. TNEB shall employ information systems to monitor and control communications at key system boundaries and connect to external networks or systems through managed interfaces in accordance with enterprise security architecture.

Internet traffic shall be routed through DMZs and associated technical equipment/solution which provide content inspection and analysis and allow for access policy management based upon organization security policy and acceptable use requirements.

Refer to the considerations outlined in Router and Swtich Security and Appendix B: Incident reporting procedure.

8.10 Intrusion Detection and Prevention Systems (IDPS)

TNEB shall utilize multiple types of IDPS technologies to achieve comprehensive and accurate detection and prevention of malicious events. IDPS signature releases and software shall be kept current as to add new IDPS functionality, new detection capabilities, or refine existing detection capabilities.

IDPS administrators shall maintain and use individual accounts and passwords to authenticate to the devices in accordance with access management and password policies. TNEB IDPS shall be planned and deployed based on regulatory requirements and infrastructure networks and shall maximize the analysis of traffic transmitted and received. Alert and notification functions for indications of intrusive activity from IDPS devices shall be enabled and monitored by information security personnel daily. Suspected and confirmed instances of intrusions shall be immediately reported.

Refer to the considerations outlined in Software Installation and Procedural Memorandum for IDS/IPS.

8.11 Virus Detection

Department of IT shall implement and maintain a centralized anti-virus solution that provides automated protection for publicly-accessible systems, perimeter devices, and internal server and client endpoints of the organization infrastructure. Standalone and networked workstations and servers shall use the Department of IT-approved virus protection software and configurations. Anti-virus software shall maintain centralized event logging for coordinated response and analysis. Web and email gateway anti-virus software shall be installed and configured for real-time active monitoring at the perimeter according to Department of IT-approved configuration standards. Email file attachments shall be scanned in real-time to inspect for viruses or other malicious code. Virus protection shall be installed on TNEB file servers and configured to identify and clean viruses that infect files shares. Internet traffic shall be scanned in real-time to ensure that transmissions and downloads do not contain viruses or other malicious code.

Virus protection software on information systems shall not be disabled, bypassed, or altered in any manner. Virus pattern and scan engine updates shall be current and updated. New virus patterns and anti-virus engine updates shall be centrally acquired by DIT and distributed to information systems after release by the anti-virus software vendor. The automatic update frequency of the virus protection software shall not be altered to reduce the frequency of updates. Viruses which are automatically cleaned by the virus protection software shall constitute a security incident and be reported.

Refer to the considerations outlined in Software Installation Policy.

8.12 Wireless Communications

Wireless communications devices shall be subject to regulations, rules, guidelines, and policies regarding the appropriate transmission and use of information and conduct. Wireless communications devices may include, but are not limited to, access points, laptop, tablets, PDAs, phones, digital assistants, pagers, wireless cards, and other information systems that can utilize wireless services or provide wireless capabilities.

Wireless access points and wireless communications devices shall be registered with a central wireless device database managed by Department of IT and shall be approved by Department of IT prior to deployment. Unauthorized devices shall be removed from service by Department of IT. Wireless devices shall be Department of IT-approved vendor products and maintain approved security configurations.

Department of IT shall maintain a list of wireless standards to include approved wireless technologies, configuration standards, and best practice procedures for secure installations. Access points and wireless devices approved for use shall be configured to meet the security controls standards established by Department of IT prior to deployment. Wireless infrastructure design shall support a hardware address that can be registered and tracked for authorized use. For example, MAC-based authentication shall be employed by allowing only registered MAC addresses access to the access point.

Wireless systems shall support and employ strong user access control which authorizes the device or user against an external database approved by the Information Security Office. Users shall either be routed outside the TNEB firewalls or authenticate to a TNEB network segment based on the concept of least privilege once authenticated. Information systems whether wired or wireless shall use an approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic when connected to wireless networks. Wireless implementations shall maintain point-to-point hardware encryption of not less than 128-bit encryption. The transmission of data wirelessly between clients, mobile devices, and other systems shall utilize Department of IT-approved encryption methods. Wireless network default service set identifiers (SSIDs) shall be changed from their default vendor settings to unique names. SSIDs shall be non-trivial and difficult to guess and shall be a minimum of 10characters in length. Wireless LANs shall be segregated from traditional wired LANs through the use of firewalls, VLANs, or DMZs. Wireless access points are subject to periodic penetration testing and auditing by authorized personnel. Access points shall be physically located in a secure and/or monitored area to prevent unauthorized access and physical tampering. Access points shall be located appropriately within the intended broadcast area of service. Devices shall not be placed near windows or against the outside walls of buildings. Access points shall be secured using an administrative password in accordance with the Password Policy. Administrators shall ensure all vendor default usernames and passwords are removed from the device. Administration of the device through the wireless network is prohibited.

TNEB has the right to confine public wireless communications within its facilities and monitor for unauthorized use. Federal law enforcement authorities have the right to access and monitor use and content from public wireless access points.

Refer to the considerations outlined in Wireless Communication Plan Policy.

9 Acceptable Use

9.1 General Principle

TNEB information systems are intended for performing organization business. Users of information systems are expected to abide by this Policy, as well as any other applicable local, laws and regulations, and policies and procedures, regardless of whether a particular information system is located internally or remotely, as in a cloud or similar type of off-site data storage, or whether data is transmitted, stored or received on mobile or fixed devices.

Examples of applicable information systems and resources may include, but is not limited to:

- Desktop PCs and Workstations
- Servers and network communications equipment
- Mobile devices such as laptops and tablets
- Issued cell phones, smart phones, and other voice and data devices
- Desktop telephones, projectors, and teleconferencing equipment
- Accessible enterprise resources such as email, instant messaging, internet, and other productivity software
- Remote access technologies that enable secure communications between personal devices for instances of telework or other purposes
- Other enterprise technologies acquired and approved for enabling electronic access to resources and data
- Acquired information technology services, systems, and/or application hosted in an environment, also known as "cloud" or "software as a service"
- Internet-based Information technology resources and applications used to conduct business on behalf of or otherwise engage, collaborate, and/or communicate with the public, partners, or other employees. This may include but is not limited to social media, streaming media, media sharing, online storage, and other internet-based tools.

9.2 Organization Ownership

Information systems and capabilities are provided to TNEB users for the facilitation of TNEB business. These systems and resources are explicitly owned by TNEB. The TNEB owns all property rights in any content or other matter created, received, transmitted, stored on, or deleted from, any information system. Any information stored on a user's personal mobile communications device or fixed device also is TNEB property and may be viewed, accessed, retrieved, copied or disseminated by the TNEB at any time.

9.3 User Privacy

Users of TNEB information system shall not have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by their use of these systems. All user activity on TNEB information system and approved mobile communications or fixed devices is subject to monitoring, logging, auditing, review, dissemination and archiving by Department of IT. Internet traffic over TNEB information systems shall be proxied and inspected for malicious code or inappropriate content prior to delivery to the user. Filters shall track user Internet activity, and be monitored for violations of this Acceptable Use Policy, as well as any other applicable laws, regulations, and policies and procedures.

Storage of user personal information on TNEB information systems is done at the user's risk. Personally-owned mobile communication devices which have been approved for access to TNEB information or technology resources may be subject to confiscation by Department of IT, and/or may be released to law enforcement, in the event of an information-system or data security breach, or other investigation.

9.4 Confidential Information

Users shall comply with all laws, regulations, and TNEB policies and procedures prohibiting or limiting the disclosure of confidential information, including but not limited to TNEB client personal information. Users shall take all steps necessary to protect the privacy of confidential information maintained by the TNEB from unauthorized access. These measures include, but are not limited to, enabling password protection on any fixed or mobile system, or otherwise locking and closing computer screens when leaving even for brief period, and logging off or terminating a system session when access is no longer needed or the user is leaving for the day. Users shall follow TNEB policies and guidelines defining data classification and protection requirements. These requirements include, but are not limited to, the following:

Information classified as Confidential or Sensitive shall only be stored on approved storage devices that use encryption.

- ❖ Users shall not use non-TNEB information systems or devices to send, forward, receive or store information classified as Confidential, Sensitive, or for Internal Use, unless approved by Department of IT in writing.
- ❖ Users shall not use non-TNEB messaging utilities such as Hotmail, Yahoo Mail, AOL Mail, and Google Mail to send, forward, or receive information classified as Confidential, Sensitive or for Internal Use.
- ❖ Information classified as sensitive being sent outside of any TNEB information system shall be specifically labelled as such and shall have restricted distribution only to those recipients who are authorized to receive such Sensitive information.

- Information classified as Confidential or Sensitive transmitted to external networks shall be encrypted in accordance with Department of IT encryption standards.

Refer to the considerations outlined in Password Protection Policy.

9.5 Incidental Personal Use

Personal use of any TNEB information system is use that is not related to the purpose for which the TNEB has granted the user authorized access. In general, incidental personal use of the TNEB information systems, such as Internet access and email, is permitted, unless the agency in which the user works restricts all incidental personal use of information systems.

Personal use of information systems is prohibited when it:
Interferes with the user's productivity or work performance, or with the productivity or work performance of other users.

- Adversely affects the efficient operation of the information system or the TNEB or is illegal, or violates this Acceptable Use Policy, the TNEB Executive's Information Technology Security Policy Memorandum Number 70-05, or any other policy or procedure.

Users must present their personal communications using TNEB information systems in such a way as to make clear that these communications are personal, and not communications from their agency or the TNEB or from the user in his or her capacity as a representative of the TNEB.

Storage of personal email messages, voice messages, files, and documents on TNEB information systems shall be kept to a minimum. Any such storage which Department of IT determines interferes with the efficient operation of the TNEB information systems is subject to removal by Department of IT without the notice or consent of the user.

9.6 Prohibited Use

Certain activities are prohibited when using TNEB information systems, applications, data and resources, whether on TNEB–owned or personally–owned devices, except when TNEB management has determined such activities are necessary for the performance of a user's official duties. These prohibited activities include, but are not limited to, the following:

- Accessing, downloading, transmitting, printing, or storing information with sexually explicit content.
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, violent, harassing, or discriminatory messages or images.
- Accessing or downloading gambling sites.
- Pursuing personal profit or gain or engaging in outside employment or personal business, unauthorized fundraising or political activities.
- Unauthorized downloading, printing, or transmitting of information protected by TNEB.
- Misusing or misapplying TNEB information system privileges.
- Using software in violation of TNEB.

9.7 Information System Security

Users shall respect the confidentiality and integrity of any TNEB information system, be familiar with TNEB information-system security policies and procedures, and report any security weaknesses or breaches in TNEB information systems to Department of IT.

Users shall respect security controls for TNEB information systems and not attempt to or circumvent those controls. Users shall not access or attempt to access any TNEB information system without authorization from Department of IT to do so.

Users shall refrain from activities that intentionally or inadvertently disrupt, impair, or undermine the performance of TNEB information systems. These activities include, but are not limited to, the following

- Intentionally causing physical or logical damage to a TNEB owned information system or resource
- Downloading computer viruses or malware or otherwise introducing malicious code into a information system
- Using Internet-based proxy servers or anonymizers, or any other tool, device or action that makes Internet activity untraceable, to bypass Web-filtering security mechanisms established on TNEB information systems
- Downloading, installing, or running security programs or utilities that reveal weaknesses in the security of a TNEB information system, including but not limited to password cracking programs, network reconnaissance and discovery applications,

key loggers, packet sniffers, network mapping tools, and port scanners, without prior approval from Department of IT in writing; or

- Consuming excessive bandwidth through actions including but not limited to placing a program in an endless loop, printing excessive amounts of paper, and sending chain letters and unsolicited mass emails.

Files and other content downloaded from the Internet, including but not limited to non-standard shareware, free software, peer-to-peer software, and information-sharing software, is subject to prior approval from Department of IT in writing. This approval may be conditioned upon Department of IT checking the downloaded files or content for viruses, Trojans, malware, or other potentially malicious content. Users shall refrain from divulging to unauthorized persons any details regarding TNEB information systems or architecture unless previously authorized.

The use of passwords to access information systems and TNEB-approved mobile communications devices is for the protection of the TNEB, and not any user. Users shall take reasonable steps to prevent the disclosure of their usernames, passwords, security tokens, or other similar information to unauthorized users. Users shall take all steps necessary to complete logoff or other termination procedures when finished using any information system. At a minimum, users should take such steps to logoff of terminate from a TNEB Information system at the end or every workday.

Users shall not connect personally-owned or other non-TNEB owned, equipment or devices, including, but not limited to, USB or other storage or memory devices, iPads or iPods, PDAs, tablets, BlackBerry devices, mobile phones or cameras, to the network infrastructure in any manner without proper approval. These devices should not be connected to systems for purposes of charging power, transferring personal audio, video, or images as non-TNEB owned electronic devices may introduce unnecessary risk to systems and data.

9.7.1 Electronic Messaging Systems

TNEB users are responsible for the content of all text, audio-video or images stored, transmitted, or received over the electronic messaging (i.e., email) and other collaboration systems, such as instant messaging. All messages communicated on email systems shall contain the sender’s name. Email or other electronic communications shall not be sent on email systems which mask or attempt to mask the identity of the sender. Users of TNEB email systems shall not give the impression in their communications to persons receiving such emails that they are representing, giving opinions, or otherwise making statements on behalf of the TNEB or any agency of the TNEB, unless otherwise authorized to do so. Where appropriate, a disclaimer shall be included, unless it is clear from the context that the email's author or sender is not representing the TNEB.

Refer to the considerations outlined in E-Mail Policy and Procedural Memorandum for E-Mail Management.

9.7.2 Internet and Intranet

TNEB web sites which include the external facing public WEB sites and content, and, the Intranet site for internal applications and services access and other collaboration tools, are for TNEB business purposes. The TNEB provides general access to the Internet from TNEB networks and devices to include Social Media. By accessing the Internet from any TNEB IT resource, users are identified as connecting from TNEB. Web filtering technologies are implemented that governs policy and access to the Internet from TNEB network(s) and devices to protect the technology systems and data from exposures to malicious code, excessive bandwidth uses, and also to block content and internet sites deemed to present in its use significant risk, inappropriate or illegal. Users shall not try to circumvent the implemented WEB filters or otherwise tunnel through authorized sites to gain access to unauthorized sites.

Users shall not download or paste any application, service or inappropriate data from the Internet site to Internet or Intranet sites without authorization.

9.7.3 Remote Access

Remote access to information systems shall only be permissible through Department of IT-provided and supported remote access software or services. Remote access shall be provided after a determination has been made that access is required to perform assigned duties, or the user is defined as "essential" personnel.

Refer to the considerations outlined in Security Response Plan Policy and Remote Access Policy.

9.8 Violations

Engaging in prohibited uses of the TNEB information systems shall be considered a violation of this Acceptable Use Policy and the Standards of Conduct, and may subject the violator to discipline, up to and including dismissal. The TNEB reserves the right to deny further access to its information systems when it believes such action is necessary to protect system security and performance. Denial of access may include, but not be limited to, revocation of accounts, passwords, software, and hardware.

10 Acceptable Encryption Policy

1 Overview

Encryption usage requirements shall consider the type and classification level of information, laws that govern protection requirements, storage location or media type, transmission medium, and internal requirements for the timely and continued availability of information.

2 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

3 Scope

This policy applies to all TNEB employees and affiliates.

4 Policy

4.1 Algorithm Requirements

- The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
- The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
- Signature Algorithms

4.2 Hash Function Requirements

In general, TNEB adheres to the Department of Electronics & Information Technology (DeitY) eGovernance standard.

4.3 Key Agreement and Authentication

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- End points must be authenticated prior to the exchange or derivation of session keys.

- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

11 Risk Assessment Policy

1 Overview

Risk assessment program that addresses the purpose, scope, roles and responsibilities, management commitment, technical controls and procedures, and adequate coordination among TNEB agencies to ensure adequate security controls consistent with applicable directives, policies, regulations, standards, and guidance.

2 Purpose

To empower Infosec to perform periodic information security risk assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

3 Scope

Risk assessments can be conducted on any entity within TNEB. Risk Assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

4 Policy

The execution, development and implementation of remediation programs are the joint responsibility of Infosec and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the Infosec Risk Assessment Team in the development of a remediation plan.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

12 Clean Desk Policy

1 Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2 Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site.

3 Scope

This policy applies to all TNEB employees and affiliates.

4 Policy

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and

locked when not in use or when not attended.

- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

13 Digital Signature Acceptance Policy

1 Overview

Organisation shall establish standards and procedures that address when encryption, digital signatures, and digital certificates shall be used in accordance with local laws and policies and guidance.

2 Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in TNEB electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

3 Scope

This policy applies to all TNEB employees and affiliates. This policy applies to all TNEB employees, contractors, and other agents conducting TNEB business with a TNEB-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non- TNEB affiliated persons or organizations.

4 Policy

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence. Digital signatures must apply to individuals only

4.1 Signer Responsibilities

- Signers must obtain a signing key pair from <TNEB identity management group>. This key pair will be generated using TNEB Public Key Infrastructure (PKI) and the public key will be signed by the TNEB's Certificate Authority (CA), <CA Name>
- Signers must sign documents and correspondence using software approved by TNEB IT organization.
- Signers must protect their private key and keep it secret.
- If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact TNEB Identity Management Group immediately to have the signer's digital key pair revoked.

4.2 Recipient Responsibilities

- Recipients must read documents and correspondence using software approved by TNEB IT department.

- Recipients must verify that the signer's public key was signed by the TNEB's Certificate Authority (CA), <CA Name>, by viewing the details about the signed key using the software they are using to read the document or correspondence.

- If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.

- If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to TNEBIdentity Management Group.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

14 Disaster Recovery Policy

1 Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives TNEB a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2 Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by TNEB that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3 Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

4 Policy

4.1 Contingency Plans

- Computer Emergency Response Team – India through Appendix A: Security Incident Reporting form to the below said details.

E-mail	: incident@cert-in.org.in
Helpdesk	: +91-1800-11-4949
Fax	: +91-1800-11-6969

- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences. The plan, at a minimum, should be reviewed an updated on an annual basis.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

15 Email Policy

1 Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2 Purpose

The purpose of this email policy is to ensure the proper use of TNEB email system and make users aware of what TNEB deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within TNEB Network.

3 Scope

This policy covers appropriate use of any email sent from a TNEB email address and applies to all employees, vendors, and agents operating on behalf of TNEB.

4 Policy

- All use of email must be consistent with TNEB policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- TNEB email account should be used primarily for TNEB business-related purposes; personal communication is permitted on a limited basis, but non-TNEB related commercial uses are prohibited.
- TNEB data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- Email should be retained only if it qualifies as a TNEB business record. Email is a TNEB business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a TNEB business record shall be retained according to TNEB Record Retention Schedule.
- The TNEB email system shall not to be used for the creation or distribution of

any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any TNEB employee should report the matter to their supervisor immediately.

- ❖ Users are prohibited from automatically forwarding TNEB email to a third-party email system (noted in below). Individual messages which are forwarded by the user must not contain TNEB confidential or above information.
- ❖ Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct TNEB business, to create or memorialize any binding transactions, or to store or retain email on behalf of TNEB. Such communications and transactions should be conducted through proper channels using TNEB-approved documentation.
- ❖ Using a reasonable amount of resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a TNEB email account is prohibited.
- ❖ TNEB employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- ❖ TNEB may monitor messages without prior notice. TNEB is not obliged to monitor email messages.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

16 End User Encryption Key Protection Policy

1 Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys use to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

2 Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

3 Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by TNEB
- encryption keys used for TNEB business
- encryption keys used to protect data owned by TNEB

The public keys contained in digital certificates are specifically exempted from this policy.

4 Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

4.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in TNEB Acceptable Encryption Policy. If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

4.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.2.1 TNEB's Public Key Infrastructure (PKI) Keys

❖ The public-private key pairs used by the TNEB's public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents the Infosec Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with TNEB policies.

- Access to the private keys stored on a TNEB issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.2.2 Other Public Key Encryption Keys

- Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with TNEB PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.
- The Infosec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with TNEB Password Policy. Infosec representatives will store and protect the escrowed keys as described in the TNEB Certificate Practice Statement Policy.

4.2.2.1 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.2.2.2 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in TNEB's Physical Security policy, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users travelling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

4.4 Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in TNEB's Password Policy.

4.5 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to The Infuse Team. Infosec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

17 Password Protection Policy

1 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of TNEB's resources. All users, including contractors and vendors with access to TNEB systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any TNEB facility, has access to the TNEB network, or stores any non-public TNEB information.

4 Policy

4.1 Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Users must not use the same password for TNEB accounts as for other non-TNEB access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various TNEB access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change

All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to follow the Password Construction Guidelines.

4.3 Password Protection

Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential TNEB information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

- Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share TNEB passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers). Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.

- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

- Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.
- Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."
- A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

18 Security Response Plan Policy

1 Overview

Remote access to our organization network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our organization network.

2 Purpose

The purpose of this policy is to define rules and requirements for connecting to TNEB's network from any host. These rules and requirements are designed to minimize the potential exposure to TNEB from damages which may result from unauthorized use of TNEB resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical TNEB internal systems, and fines or other financial liabilities incurred as a result of those losses.

3 Scope

This policy applies to all TNEB employees, contractors, vendors and agents with a TNEB-owned or personally-owned computer or workstation used to connect to the TNEB network. This policy applies to remote access connections used to do work on behalf of TNEB, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to TNEB networks.

4 Policy

It is the responsibility of TNEB employees, contractors, vendors and agents with remote access privileges to TNEB's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to TNEB.

General access to the Internet for recreational use through the TNEB network is strictly limited to TNEB employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the TNEB network from a personal computer, Authorized Users are responsible for preventing access to any TNEB computer resources or data by non-Authorized Users. Performance of illegal activities through the TNEB network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. Authorized Users will not use TNEB networks to access the Internet for outside business interests.

For additional information regarding TNEB's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company url).

4.1 Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.
- Authorized Users shall protect their login and password, even from family members.
- While using a TNEB-owned computer to remotely connect to TNEB's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct TNEB business must be approved in advance by InfoSec and the appropriate business unit manager.
- All hosts that are connected to TNEB internal networks via remote access

technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.

- ❖ Personal equipment used to connect to TNEB's networks must meet the requirements of TNEB-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to TNEB Networks.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

19 Remote Access Policy

1 Overview

Remote access to our organization network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our organization network.

2 Purpose

The purpose of this policy is to define rules and requirements for connecting to TNEB's network from any host. These rules and requirements are designed to minimize the potential exposure to TNEB from damages which may result from unauthorized use of TNEB resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical TNEB internal systems, and fines or other financial liabilities incurred as a result of those losses.

3 Scope

This policy applies to all TNEB employees, contractors, vendors and agents with a TNEB-owned or personally-owned computer or workstation used to connect to the TNEB network. This policy applies to remote access connections used to do work on behalf of TNEB, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to TNEB networks.

4 Policy

It is the responsibility of TNEB employees, contractors, vendors and agents with remote access privileges to TNEB's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to TNEB.

General access to the Internet for recreational use through the TNEB network is strictly limited to TNEB employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the TNEB network from a personal computer, Authorized Users are responsible for preventing access to any TNEB computer resources or data by non-Authorized Users. Performance of illegal activities through the TNEB network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. Authorized Users will not use TNEB networks to access the Internet for outside business interests.

For additional information regarding TNEB's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company url).

4.1 Requirements

- ❖ Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.
- ❖ Authorized Users shall protect their login and password, even from family members.
- ❖ While using a TNEB-owned computer to remotely connect to TNEB's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- ❖ Use of external resources to conduct TNEB business must be approved in advance by InfoSec and the appropriate business unit manager.
- ❖ All hosts that are connected to TNEB internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.
- ❖ Personal equipment used to connect to TNEB's networks must meet the requirements of TNEB-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to TNEB Networks.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

20 Router and Switch Security Policy

1 Overview

Department of IT shall be responsible for all aspects of the TNEB network infrastructure and will manage and administer all future developments, implementations, and enhancements to this infrastructure. Modifications, additions, and the removal of network management devices and configurations shall not be made without the approval of Department of IT and shall be governed by Configuration and Change Management processes and procedures. Department of IT will establish operational and technical methods of protecting against unauthorized connections to the enterprise IT environment.

2 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of TNEB.

3 Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. All routers and switches connected to Cisco production networks are affected.

4 Policy

- ❖ Every router must meet the following configuration standards:
  - ✓ No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
  - ✓ The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

- ❖ The following services or features must be disabled:
  - ✓ IP directed broadcasts
  - ✓ Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
  - ✓ TCP small services
  - ✓ UDP small services
  - ✓ All source routing and switching
  - ✓ All web services running on router
  - ✓ Cisco discovery protocol on Internet connected interfaces
  - ✓ Telnet, FTP, and HTTP services
  - ✓ Auto-configuration

❖ The following services should be disabled unless a business justification is provided:

  - ✓ Cisco discovery protocol and other discovery protocols
  - ✓ Dynamic trunking
  - ✓ Scripting environments, such as the TCL shell

❖ The following services must be configured:

  - ✓ Password-encryption
  - ✓ NTP configured to a corporate standard source
  - ✓ All routing updates shall be done using secure routing updates.
  - ✓ Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
  - ✓ Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
  - ✓ Access control lists for transiting the device are to be added as business needs arise.
  - ✓ The router must be included in the corporate enterprise management system with a designated point of contact.
  - ✓ Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED"

❖ You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

❖ Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

- ❖ Dynamic routing protocols must use authentication in routing updates sent to neighbours. Password hashing for the authentication string must be enabled when supported.

- ❖ The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

  - ✓ IP access list accounting
  - ✓ Device logging
  - ✓ Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
  - ✓ Router console and modem access must be restricted by additional security controls

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

21 Wireless Communication Policy

1 Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2 Purpose

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to TNEB network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a TNEB network.

3 Scope

All employees, contractors, consultants, temporary and other workers at TNEB, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of TNEB must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a TNEB network or reside on a TNEB site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4 Policy

4.1 General Requirements

- All wireless infrastructure devices that reside at a TNEB site and connect to a TNEB network, or provide access to information classified as TNEB Confidential, or above must:
- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use TNEB approved authentication protocols and infrastructure.

- Use TNEB approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations

4.2 Lab and Isolated Wireless Device Requirements

- All lab wireless infrastructure devices that provide access to TNEB Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the TNEB network must:
- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

- Wireless infrastructure devices that provide direct access to the TNEB corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.
- Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the TNEB corporate network. Access to the

TNEB corporate network through this device must use standard remote access authentication.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

22 Web Application Security Policy

1 Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

2 Purpose

The purpose of this policy is to define web application security assessments within TNEB. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of TNEB services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3 Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at TNEB.

All web application security assessments will be performed by delegated security personnel either employed or contracted by TNEB. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of TNEB is strictly prohibited unless approved by the Chief Information Officer. Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4 Policy

4.1 Web applications are subject to security assessments based on the following criteria:

- ❖ New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- ❖ Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
- ❖ Point Releases – will be subject to an appropriate assessment level

based on the risk of the changes in the application functionality and/or architecture.

- Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

- High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
- Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

- Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

23 Information Logging policy

1 Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

2 Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3 Scope

This policy applies to all production systems on TNEB Network.

4 Policy

4.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

- ❖ What activity was performed?
- ❖ Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- ❖ What the activity was performed on (object)?
- ❖ When was the activity performed?
- ❖ What tool(s) was the activity was performed with?

- What was the status (such as success vs. failure), outcome, or result of the activity?

4.2 Activities to be logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
- Create, update, or delete information not covered in #1;
- Initiate a network connection;
- Accept a network connection;
- User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
- Application process start-up, shutdown, or restart;
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

- Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.
- Type of action – examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action – examples includes process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Before and after values when action involves updating a data element, if feasible.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

- The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

- Microsoft Windows Event Logs collected by a centralized log management system;

- Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system;
- Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
- Other open logging mechanisms supporting the above requirements including those based on Checkpoint OpSec, Arc Sight CEF, and IDMEF.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

24 Server Security Policy

1 Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by TNEB. Effective implementation of this policy will minimize unauthorized access to TNEB proprietary information and technology.

3 Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Cisco or registered under a Cisco-owned internal network domain.

This policy specifies requirements for equipment on the internal Cisco network. For secure configuration of equipment external to Cisco on the DMZ, see the Internet DMZ Equipment Policy.

4 Policy

4.1 General Requirements

All internal servers deployed at TNEB must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

  - ✓ Server contact(s) and location, and a backup contact
  - ✓ Hardware and Operating System/Version
  - ✓ Main functions and applications, if applicable

- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit Policy.

24.2 Configuration Requirements

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Does not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g.,

encrypted network connections using SSH or IPSec).

- Servers should be physically located in an access-controlled environment. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

25 Software Installation Policy

1 Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

2 Purpose

The purpose of this policy is to outline the requirements around installation software on computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within TNEB's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3 Scope

This policy applies to all TNEB employees, contractors, vendors and agents with TNEB-owned mobile devices. This policy covers all computers, servers, smart phones, tablets and other computing devices operating within TNEB.

4 Policy

- ❖ Employees may not install software on TNEB's computing devices operated within the TNEB network.
- ❖ Software requests must first be approved by the requester's manager and

then be made to the Information Technology department or Help Desk in writing or via email.

- Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester’s need.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation. Organizations.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

26 Technology Equipment Disposal Policy

1 Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of TNEB data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

2 Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by TNEB.

3 Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within TNEB including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

4 Policy

4.1 Technology Equipment Disposal

- ❖ When Technology assets have reached the end of their useful life they should be sent to the IT_Maintaince team for proper disposal.
- ❖ The IT_Maintaince team will securely erase all storage mediums in accordance with current industry best practices.
- ❖ All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media

overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defence standards.

- No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around TNEB. These can be used to dispose of equipment. The IT_Maintaince team will properly remove all data prior to final disposal.
- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or net book computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- The IT_Maintaince team will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

4.2 Employee Purchase of Disposed Equipment

- Equipment which is working, but reached the end of its useful life to TNEB, will be made available for purchase by employees.
- A lottery system will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.
- Finance and Information Technology will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with

any equipment sold.

- Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines.
- Information Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
- Prior to leaving TNEB premises, all equipment must be removed from the Information Technology inventory system.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

27 Change Management and Control Policy

1 Overview

Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure.

2 Purpose

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed
- Computer performance being disrupted and/or degraded
- Productivity losses being incurred
- Exposure to reputational risk.

3 Scope

This policy applies to all parties operating within the company's network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company's data networks. No employee is exempt from this policy.

4 Policy

4.1 Preamble

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner and that the status of each proposed change is monitored.

In order to fulfil this policy, the following statements shall be adhered to:

4.2 Operational Procedures

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

At a minimum the change control process should include the following phases:

- Logged Change Requests
- Identification, prioritisation and initiation of change
- Proper authorisation of change
- Requirements analysis
- Inter-dependency and compliance analysis
- Impact Assessment
- Change approach
- Change testing
- User acceptance testing and approval
- Implementation and release planning
- Documentation
- Change monitoring
- Defined responsibilities and authorities of all users and IT personnel
- Emergency change classification parameters.

4.3 Documented Change

All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

4.4 Risk Management

A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.

The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

4.5 Change Classification

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

4.6 Testing

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. (For more information see System Development Life Cycle [citation here]).

4.7 Changes affecting SLA ‘s

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

4.8 Version control

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies. (For more information see System Development Life Cycle [citation here])

4.9 Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user; the impact assessment was performed and proposed changes were tested.

4.10 Communicating changes

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

4.11 Implementation

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see System Development Life Cycle [citation here])

4.12 Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

4.13 Documentation

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

4.14 Business Continuity Plans (BCP)

Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

4.15 Emergency Changes

Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

4.16 Change Monitoring

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

28 Software Development Policy

1 Overview

Specific measures will be implemented to ensure that system and application software performs as intended to maintain information integrity, confidentiality, and availability.

2 Purpose

The purpose of this Policy is to standardize software development for all enterprise-level centrally-managed mission critical web applications and web services through the use of Industry leading practices. These applications and services typically deal with sensitive data and / or HR, finance, public, or course related data, and due diligence in protecting this data is required. Standardizing the development approach and coding techniques for critical systems will ensure their maintainability, security, protection against cyber-attacks and accessibility.

3 Scope

This Policy applies to all employees' staff, consultants and / or contractors involved in the development or modification of enterprise-level centrally-managed mission critical applications that support TNEB.

4 Policy

- ❖ The Request for Development forms must be used to make any requests for software development. Software developers should never be contacted directly to perform development tasks. Requests for changes to existing systems may only be made by the system owner or a party who has been granted specific authority to do so. This form should be used for any of the following requests:

    - ✓ Modification, feature addition, or enhancement to an existing system or web page
    - ✓ Creation of a new system
    - ✓ Request for a new report or data extraction
    - ✓ Request to access an existing report
    - ✓ Request Approval Process

- ❖ Information Technology Services (ITS) is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for TNEB web projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this Policy addresses the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design specification; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for sensitive TNEB information.

- All enterprise-level centrally-managed mission critical applications developed at or for TNEB must adhere to development standards and procedures documented in the ITS Application Development Standards guide. These standards include: coding techniques, testing strategies, documentation requirements and software release processes that align with industry standards and regulatory requirements.
- There must be a separation between the production, development and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

29 Acceptable Use Policy

1 Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to TNEB's established culture of openness, trust and integrity. Infosec is committed to protecting TNEB's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of TNEB. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every TNEB employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at TNEB. These rules are in place to protect the employee and TNEB. Inappropriate use exposes TNEB to risks including virus attacks, compromise of network systems and services, and legal issues.

3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct TNEB business or interact with internal networks and business systems, whether owned or leased by TNEB, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at TNEB and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with TNEB policies and standards, and local laws and regulation. Exceptions to this policy are documented. This policy applies to employees, contractors, consultants, temporaries, and other workers at TNEB, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by TNEB.

4 Policy

- General Use and Ownership

  - ✓ TNEB proprietary information stored on electronic and computing devices whether owned or leased by TNEB, the employee or a third party, remains the sole property of TNEB. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
  - ✓ You have a responsibility to promptly report the theft, loss or unauthorized disclosure of TNEB proprietary information.
  - ✓ You may access, use or share TNEB proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.
  - ✓ Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet / Intranet / Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
  - ✓ For security and network maintenance purposes, authorized individuals within TNEB may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.
  - ✓ TNEB reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

- Security and Proprietary Information
  - ✓ All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
  - ✓ System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
  - ✓ All computing devices must be secured with a password-protected

screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

- ✓ Postings by employees from a TNEB email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of TNEB, unless posting is in the course of business duties.
- ✓ Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

- ➢ Unacceptable Use

    - ✓ The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
    - ✓ Under no circumstances is an employee of TNEB authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TNEB-owned resources.
    - ✓ The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

- ➢ System and Network Activities (The following activities are strictly prohibited, with no exceptions)
    - ✓ Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by TNEB.
    - ✓ Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music,

and the installation of any copyrighted software for which TNEB or the end user does not have an active license is strictly prohibited.

- ✓ Accessing data, a server or an account for any purpose other than conducting TNEB business, even if you have authorized access, is prohibited.
- ✓ Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- ✓ Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- ✓ Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- ✓ Using a TNEB computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- ✓ Making fraudulent offers of products, items, or services originating from any TNEB account.
- ✓ Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- ✓ Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this Section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- ✓ Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
- ✓ Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of

the employee's normal job/duty.

- ✓ Circumventing user authentication or security of any host, network or account.
- ✓ Introducing honey pots, honey nets, or similar technology on the TNEB network.
- ✓ Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- ✓ Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- ✓ Providing information about, or lists of, <Company Name> employees to parties outside TNEB.

- ➢ Email and Communication Activities when using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

- ✓ Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- ✓ Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- ✓ Unauthorized use, or forging, of email header information.
- ✓ Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- ✓ Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- ✓ Use of unsolicited email originating from within TNEB's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by TNEB or connected via TNEB's network.

- ✓ Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

- ➢ Blogging and Social Media

  - ✓ Blogging by employees, whether using TNEB's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of TNEB's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate TNEB's policy, is not detrimental to TNEB's best interests, and does not interfere with an employee's regular work duties. Blogging from TNEB's systems is also subject to monitoring.
  - ✓ TNEB's Confidential Information policy also applies to blogging. As such,

    Employees are prohibited from revealing any TNEB confidential or proprietary information, trade secrets or any other material covered by TNEB's Confidential Information policy when engaged in blogging.
  - ✓ Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of TNEB and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by TNEB's Non-Discrimination and Anti-Harassment policy.
  - ✓ Employees may also not attribute personal statements, opinions or beliefs to TNEB when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of TNEB. Employees assume any and all risk associated with blogging.
  - ✓ Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, TNEB's trademarks, logos and any other TNEB intellectual property may

also not be used in connection with any blogging activity.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of change	Responsible	Summary of change

30 Procedure Memorandum for E-mail Management

Electronic mail (email) is the most popularly used system for exchanging information over the Internet (or any other computer network). After Web servers, mail servers are the hosts on an organization’s network that are most often targeted by attackers. This document is intended to assist organizations in installing, configuring, and maintaining secure mail servers and mail clients. This document discusses about –

- ✓ Planning of mail server: This section suggests about client access methods, preferred location of mail servers, encryption technologies etc.
- ✓ Configuration and Installation: Which includes hardening the operating system, mail server application, mail client application and network to prevent malicious entities from directly attacking the mail server.
- ✓ Maintenance and Incident handling of mail servers.

1 Planning

- ❖ Organizations should carefully plan and address the security aspects of the deployment of a Mail server. The plan must include selection of mail server, selection of client access protocols, location of mail server in the network, antivirus policy, network security policy etc.

1.1 Location of Mail Server

- ❖ It is important to properly plan the location of a mail server within the network of an organization.
- ❖ A typical position of Mail server will be to place it in the DMZ. A two-firewall DMZ configuration offers superior protection over a router-firewall DMZ since the dedicated firewalls can have a more complex and powerful security rule set. In addition, the dedicated firewall is often able to analyze incoming and outgoing mail traffic, it can detect and protect against application layer attacks aimed at the mail server. Depending on the configuration of the firewalls and the level of traffic the DMZ receives; this type of DMZ may result in some performance degradation.
- ❖ For organizations which desire the security of the two firewall DMZ but do not have the resources to purchase two firewalls, there exists another option called the “service leg” DMZ. In this configuration, a firewall is constructed with three (or more) network interfaces. One network interface attaches to the border router, another interface attaches to the internal network, and a third network interface connects to the DMZ.

1.2 Client access methods

- Several methods exist for users to access their mailboxes. That can be a command line access (using pine or mail etc) or can be on some standard protocol like POP3 or IMAP based client.
- Allowing users, to have access to a command-line interface is a significant security risk. Adoption of protocols like POP3 or IMAP can mitigate these risks.

1.3 Using a mail Gateway

- A mail gateway acts as a proxy between the real mail server and the Internet. All messages and communications must go through proxy before they are forwarded to the mail server. This breaks the direct line of communication between the Internet and the mail server making it much more difficult to attack the mail server. Since the mail gateway generally requires only limited functionality, it is much easier to harden and secure than a fully functional mail server.

1.4 Protecting Email from Malicious Code

1.4.1 Virus Scanning

- To protect against viruses and other malicious code, it will be necessary to implement scanning at one or more points within the email delivery process. Virus scanning can be implemented on the firewall as the mail data enters the organization's network, on the mail server or mail relay and/or on the end user's host. Scanning for viruses at the firewall (application proxy) or mail relay is a popular option In this instance, the firewall or mail relay intercepts messages before they reach the organization's mail server. The firewall or mail relay scans each message and if no viruses are found, forwards the message on to the organization's mail server for delivery. The firewall or mail relay listens on the TCP port 25 for SMTP connections, receives the message, scans the message, then forwards the message on to the mail server, which is configured to listen on an unprivileged, unused port, rather than the usual port 25.

1.4.2 Content Filtering

- ❖ Content filtering works in a similar manner to virus scanning at the firewall or mail server except that it takes this concept in a different direction. It looks at the content of emails for characteristics other than malicious code that might be of interest to the organization. When implementing file-type restrictions and virus scanning, only a certain level of security is provided. The contents of an email message or its attachments could prove much more damaging to an organization than a virus or rogue executable. For this case, some sort of content filtering mechanism should be employed.
- ❖ In general, rules are defined to forward, quarantine, park, clean, block or delete any data passing through the server depending the results of the scan. Typical items that would be caught by the filter and possible action taken on them could be as follows:
  - ✓ Email that contains suspicious active content (e.g., ActiveX, JavaScript) is stripped of the active code and forwarded to recipient.
  - ✓ Spam email may be deleted
  - ✓ Extra large files might be parked for delivery at off peak hours.

1.5 Adoption of Encryption Technologies

- ❖ Common factors that can influence the choice of an encryption algorithm include the following items

  - ✓ Required security

    Value of the data to the organization and/or other entities. The more valuable the data, the stronger the required encryption.

  - ✓ Time value of data.

    If data are valuable for only a short time period (e.g., days as opposed to years), then a weaker encryption algorithm can be used. An example would be passwords that are changed on a daily basis because the encryption needs to protect the password for only a 24-hour period.

- ✓ Threat to data.

  The higher the threat level, the stronger the required encryption.

- ✓ Required performance.

  Higher performance requirements may necessitate weaker encryption, but this is not normally a consideration with email. System resources. Less resources such as processor speed and memory size may necessitate weaker encryption, but are not typically a factor in email.

- ✓ Import, export, or usage restrictions.

  Encryption schemes supported by mail client applications and operating systems.

- ✓ Other protective measures may reduce the need for stronger encryption. An example would be using protected methods of communications such as dedicated circuits instead of the public Internet.

3 Configuration

The first step in securing a mail server is securing the underlying operating system. Most commonly available mail servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying mail servers are configured appropriately.

3.1 Securely Installing the Mail Server

- ❖ Install the server software on a dedicated host
- ❖ Install minimal Internet services required
- ❖ Apply all patches or upgrades to correct for known vulnerabilities
- ❖ Create a dedicated physical disk or logical partition (separate from operating system and server application) for mail boxes
- ❖ Remove or disable all services installed by the mail server application but not required (e.g. FTP, remote administration, etc)
- ❖ Remove all vendor documentation from server

- Remove any example or test files from server
- Reconfigure SMTP, POP, and IMAP service banner (and others as required) NOT to report mail server and operating system type and version (this may not be possible with all mail servers).
- Disable dangerous or unnecessary mail commands (e.g., VRFY and EXPN)

3.2 Configuring Operating System and Mail Server Access Controls

- Limit the access of the mail server application to a subset of computational resources
- Limit the access of users through additional access controls enforced by the mail server, where more detailed levels of access control are required.
- Apply proper access control List for the following file types
    - ✓ Application software and configuration files
    - ✓ Files directly related to security mechanisms:
    - ✓ Password hash files and other files used in authentication
    - ✓ Files containing authorization information used in controlling access
    - ✓ Cryptographic key material used in confidentiality, integrity, and non-repudiation services.
    - ✓ Server log and system audit files
    - ✓ System software and configuration files.
- To mitigate the effects of certain types of DoS attacks, configure the mail server to limit the amount of operating system resources it can consume. Some examples include:

    - ✓ Install users' mailboxes on a different hard drive or logical partition than the operating system and mail server application.
    - ✓ Limit the size of attachments that are allowed.
    - ✓ Ensure log files are stored in a location that is sized appropriately.
- Protecting Email from Malicious Code Filter potentially dangerous attachment types (e.g., .vbs, .ws, .wsc file extensions) at the mail server or mail gateway, while conducting virus scans on allowed file types.

3.3 Authenticate Mail Relaying

❖ Two methods are available for controlling mail relay.

  ✓ The first is to control the subnet or domain from which messages are being sent. This method is effective if the perimeter of the messaging system resides within known address ranges.
  ✓ The second method is to apply Authenticated relaying (SMTPAUTH) which is the SMTP extension that supports user authentication.

3.4 Unsolicited Bulk Email (Spam mail)

❖ To control spammed messages, administrators must address two concerns:
  ✓ Ensure that UCE (Unsolicited Bulk Email) cannot be sent from mail servers they control and Implement inbound message control
  ✓ Mail server administrators can block the inbound mails from mail servers that are often used to send unsolicited email messages.

3.5 Securing network infrastructure

Router/Firewall Configuration

❖ A firewall or router (acting as a firewall) that is protecting a mail server should be configured to block all access to the mail server from the Internet except TCP port 25 (SMTP), TCP port 110 (POP3), TCP port 143 (IMAP), TCP port 398 (Lightweight Directory Access Protocol [LDAP]), and TCP port 636 (Secure LDAP).

❖ To successfully protect a mail server using a firewall, ensure that it is capable of and configured to support the following:
  ✓ Control all traffic between the Internet and the mail server
  ✓ Block all inbound traffic to the mail server except that traffic which is required. This usually includes one or more of the following protocols:
    - TCP port 80 and 443 (Web mail)
    - TCP port 25 (SMTP)
    - TCP port 110 (POP3)
    - TCP port 143 (IMAP)
    - TCP port 389 (LDAP)
    - TCP port 636 (secure LDAP)

- ✓ Block (in conjunction with the intrusion detection system IP addresses or subnets that the IDS reports are attacking the organizational network Notify the network or mail server administrator of suspicious activity through an appropriate means (e.g., page, email, network trap)

    - Provide content filtering
    - Provide virus scanning
    - Protect against DoS/DDoS attacks
    - Log critical events, including the following details:
        - Time/date
        - Interface IP address
        - Vendor specific event name
        - Standard attack event (if exists)
        - Source and destination IP address
        - Source and destination port numbers
        - Network protocol used by attack.

3.6 Secure Mail Client

- ❖ The most important step in securing an email client is to ensure that all users are using the latest and/or most secure version of the mail client with all necessary patches applied. A secured mail client should adhere to the following

    - ✓ Disable automatic message preview.
    - ✓ Disable automatic opening of next message.
    - ✓ Disable processing of active content.
    - ✓ Disable automatic login (remember password and user name)

4 Operations and Maintenance

- ❖ Mail server administrators are system architects responsible for the overall design, implementation, and maintenance of a mail server. Mail server and network administrators must address the security requirements of the specific system(s) for which they are responsible.

4.1 Logging

- ❖ Logging is a cornerstone of a sound security posture. Logging the correct data and then monitoring those logs is critical. Reviews should take place on a daily to weekly basis and when a suspicious activity has been noted or a threat warning has been issued. Automated Log File Analysis Tools can be used for analysis.
- ❖ The following generic type of logging is recommended. Set logging on the mail server to the most detailed level available.

  - ✓ Local host related logging
    Mail server configuration errors (e.g., mismatch with DNS: local configuration error, out of date alias database)
    Lack of system resources (disk space, memory, CPU)

  - ✓ Connection related logging
    Logons (successful and failed)
    Security problems (e.g., spamming)
    Lost communications (network problems)
    Protocol failures
    Connection timeouts
    Connection rejections
    Use of VRFY and EXPN commands

- ✓ Message-related logging

  Malformed addresses

  Creation of error messages

  Delivery failures (permanent errors)

  Messages being deferred (transient errors).

4.2 Backup and recovery

- ❖ A proper backup policy should be in place keeping in consideration of the organizations need. Backup should be taken on the following types

  - ✓ Configuration files
  - ✓ Mail Boxes
  - ✓ Mail queues at specified time interval
  - ✓ Logs

4.3 Security Testing

- ❖ Vulnerability Scanning

  Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfiguration of hosts. Many vulnerability scanners also provide information about mitigating discovered vulnerabilities.
- ❖ Penetration Testing

  The purpose of penetration testing is to exercise system protections (particularly human response to attack indications) by using common tools and techniques developed by hackers. This testing is highly recommended for complex or critical systems.

5 Incident Handling

- ❖ The first step in recovering from a compromise is to create and document the required policies and procedures for responding to successful intrusions prior to an intrusion. The response procedures should outline the actions that are required to respond to a successful compromise of the mail server and the appropriate sequence of these actions

- ❖ A mail server administrator should take the following steps after discovering a successful compromise:

  - ✓ Report incident to CERT-In.
  - ✓ Consult the organization’s security policy.
  - ✓ Isolate compromised system(s) or take steps to contain attack so additional evidence can be collected
  - ✓ Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously
  - ✓ Investigate “similar” hosts to determine if the attacker also has compromised other systems
  - ✓ Analyze the intrusion, including:
    - o Modifications made to the system’s software and configuration
    - o Modifications made to the data
    - o Tools or data left behind by intruder
    - o Review system logs, intrusion detection, and firewall log files.
  - ✓ Restore the system

    Install clean version of operating system, or Restore from backups (this option can be riskier, as the backups may have been made after the compromise and restoring from a comprised back may still allow the attacker access to the system).
  - ✓ Disable unnecessary services
  - ✓ Apply all patches
  - ✓ Change all passwords (even on uncompromised hosts as required)
  - ✓ Reconfigure network security elements (firewall, router, IDS) to provide additional protection and notification.
  - ✓ Test system to ensure security
  - ✓ Reconnect system to network
  - ✓ Monitor system and network for signs that the attacker is attempting to access the system or network again.
  - ✓ Document lessons learned.

31 Procedural Memorandum for Information Logging

System-level and infrastructure administrators should follow standard processes for managing the logs for which they are responsible, major operational processes for log management are:

1. Configure Log Sources:

System-level administrators need to configure log sources so that they capture the necessary information in the desired format and locations, as well as retain the information for the appropriate period of time.

2. Log generation:

System-level administrators need to consider the likely effect of the log source configuration not only on the logging host, but also on other log management infrastructure components—for example, excessive logging can cause significantly more usage of network bandwidth and centralized log storage.

3. Log Storage and Disposal:

System-level administrators need to determine how each log source should store its data. This should be driven primarily by organizational policies regarding log storage, particularly requirements to forward entries to a log management infrastructure.

4. Log Security:

- ❖ Infrastructure and system-level administrators need to protect the integrity and availability of log data, and often protect its confidentiality as well.
  - ✓ Limit access to log files
  - ✓ Avoid recording unneeded sensitive data
  - ✓ Protect archived log files
  - ✓ Secure the processes that generate the log entries
  - ✓ Configure each log source to behave appropriately when logging errors occur

- ✓ Implement secure mechanisms for transporting log data from the system to the centralized log management servers

5. Analyze Log Data & Prioritizing Log Entries:

Effective analysis of log data is often the most challenging aspect of log management, but is also usually the most important.

6. Respond to Identified Events:

Log analysis, infrastructure and system-level administrators may identify events of significance, such as incidents and operational problems, that necessitate some type of response. When an administrator identifies a likely computer security incident, as defined by the organization's incident response policies, the administrator should follow the organization's incident response procedures to ensure that it is addressed appropriately.

7. Manage Long-Term Log Data Storage:

Administrators typically are responsible for managing the storage of their logs. They should be aware of the organization's requirements and guidelines for log data storage, so that logs are retained for the required period of time. If log data has already been transferred to the log management infrastructure, system-level administrators might not need to do any long-term storage of log data. If administrators need to store the log data for a retention period, and this period is relatively short (days or weeks), it might be adequate to keep them online and capture them in regular system backups.

32 Procedural Memorandum for Firewall

- ❖ Deny all traffic by default, and only enable those services that are needed.
- ❖ Disable or uninstall any unnecessary services and software on the firewall that are not specifically required.
- ❖ Limit the number of applications that run on the firewall in order to let the firewall do what it's best at doing. Consider running antivirus, content filtering, VPN, DHCP and authentication software on other dedicated systems behind the firewall.

- If possible, run the firewall service as a unique user ID instead of administrator or root.
- Change the default firewall administrator or root password. The password should not be found in a dictionary and should be a minimum of eight characters long using a combination of uppercase and lowercase letters, numbers and other characters such as $, % and @, and it needs to be changed frequently.
- Ensure that you're filtering packets for correct addresses based upon the Top 20 Vulnerabilities List section titled Not filtering packets for correct incoming and outgoing addresses.
- Ensure that you're filtering or disabling all unnecessary ports and common vulnerable ports based upon the Top 20 Vulnerabilities List sections titled Large number of open ports and Common Vulnerable Ports.
- If a malicious user can obtain physical access to the firewall, anything can happen. Ensure that physical access to the firewall is controlled.
- A lot of times, firewalls are doing less (or more) than what they should be doing based on your business needs and information flow requirements. Keep your firewall configuration as simple as possible, and eliminate unneeded or redundant rules to ensure that the firewall is configured to support your specific needs.
- Make sure the security rule set on the firewall remains consistent with the organization's written information security policy.
- Consider using the following in conjunction with a firewall:
    - ✓ Network-based intrusion-detection system (IDS)
    - ✓ Hosted-based personal firewall/intrusion-prevention products to protect workstations and servers from malicious traffic coming in over the allowed ports on the firewall
    - ✓ Antivirus software that is regularly updated
    - ✓ E-mail and Web content-filtering software
    - ✓ URL filtering software
    - ✓ Third-party authentication systems
- Run the firewall on a hardened and routinely patched operating system. An insecure and non-hardened operating system can render the firewall completely useless.

- If possible, use a firewall in conjunction with a router when connecting to the Internet to help prevent denial-of-service attacks and successful penetrations.
- Patch the firewall's operating system and application software with the latest code on a regular basis. However, make sure you test these updates in a controlled, non-production environment whenever possible.
- Use firewalls internally to segment networks and permit access control based upon business needs.
- Enable firewall logging and alerting if possible.
- Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious user.
- Regularly monitor the firewall logs. Treat the logs as business records and include them in your data retention policy.
- Note any firewall log entries that don't look right, and investigate them immediately.
- Periodically backup the firewall logs (preferably onto write-once media such as CD-R) and store for future reference and/or legal protection in the case of an intrusion that must be investigated.
- Consider outsourcing your firewall management to leverage the managed security service providers' aggregation of expertise, network trending analysis and intelligence, and to save time and money.
- Use change-management practices for the firewall to approve changes needed, assess the reason(s) for the changes, document the changes made and describe the necessary back-out procedures in case the changes fail.
- Perform vulnerability assessments on your firewall on an ongoing basis to test for known software flaws and weaknesses. New exploits are continuously discovered and must be tested for on a consistent basis. In addition, the slightest firewall system or rule set modifications can completely change the firewall's security capabilities. Perform these tests on every interface of the firewall in all directions. Also, perform these tests with and without the firewall rules enabled to determine how vulnerable you will be when the firewall is not functioning properly.

- Perform ongoing audits, at least yearly, on the firewall to compare what you say you're doing in your security policy with what's actually being done and to ensure adherence to any government regulations that pertain to your organization.
- Require users to run antivirus and personal firewall/intrusion-prevention software on all remote computers. This will help prevent malicious code or an attacker from penetrating the corporate network in the event that the remote computer is compromised. Make this something that cannot be easily disabled. No exceptions.
- Regularly backup the firewall configuration files, and keeps the backups offsite.
- Firewalls can be easily circumvented if using wireless network systems internally. Again, use personal firewalls/intrusion-prevention software on all internal hosts whenever possible.
- Remember that firewalls won't prevent attacks that originate from inside your network. An acceptable usage policy, personal firewalls/intrusion-prevention software, network monitoring, content filtering and access controls on all hosts can help lower these risks.

33 Procedural Memorandum for IDS/IPS

- One or more dedicated platforms (also called appliances) should be used for intrusion detection and prevention. The IDS/IPS should have the following security controls:

  - ✓ The IDS/IPS should operate on a hardware appliance dedicated to performing IDS/IPS and associated logging functions only.
  - ✓ The IDS/IPS should operate in a protected execution environment to protect itself from interference and tampering by other applications.
  - ✓ The platform should not permit any network-based user login.
  - ✓ The platform should contain the minimum number of administrative accounts necessary for the IDS/IPS administration. This can, and should, include separate administrative accounts for each individual

administering the IDS/IPS. The platform should not contain any other user accounts.

- ✓ The platform should have only the IDS/IPS and associated logging applications installed.
- ✓ The platform should only have the network services installed and active required for operation of IDS/IPS. All other network services should be either not installed or disabled.
- ✓ The IDS/IPS log should be protected from unauthorized examination and modification. The IDS/IPS log should be treated like the operating system log.

❖ At a minimum network-based IDS/IPS should be used with the following capabilities:

- ✓ Information gathering
- ✓ Detection
- ✓ Blacklisting
- ✓ Passive prevention

❖ Network architecture for IDS and IPS could be any one of the following, however, the IDS/IPS data must be managed so as to not reveal voter choices.

- ✓ Inline
- ✓ Passive
- ✓ Tap
- ✓ Load Balance

❖ Network IDS and IPS should be able to at a minimum terminate an offending TCP session. Other actions maybe also be used: firewalling (i.e., drop or reject suspicious network activity); throttling bandwidth usage; and sanitizing packets to remove malicious content.

- ✓ Network IDS and IPS may optionally perform NBA, which examines network traffic to identify threats that generate unusual traffic flows, such as DDoS attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems).

34 Procedural Memorandum for Securing the Web Server

- A web server is a program, which listens for http requests on a TCP/IP port (Normally either port 80 or port 443) and serves html pages in response.

  There are several web servers currently in the market. The most popular are:

  - ✓ Apache
  - ✓ SunONE
  - ✓ Internet Information Server (IIS)
  - ✓ NCSA

- Specific methods for securing a web server largely depend on the operating system (OS) and web server software used. Apache can run on the Windows platform, but usually runs on Linux or some other flavor of Unix. IIS runs on the Windows server platforms. SunONE is the sum of sites running iPlanet-Enterprise, Netscape-Enterprise, Netscape-FastTrack, Netscape-Commerce, Netscape-Communications, NetsiteCommerce & Netsite-Communications.
- Once a web server is set up, it is an invitation to the world to connect to it. The users may include potential hackers as well. The attackers may deface the web site, causing embarrassment. Or they may download confidential information, or steal credit card information. Or they may use the host as part of a distributed denial-of-service (DDOS) attack on another host.
- In a defacing incident, the Web Manager may come to know that the web site has been hacked. But in other cases, it may not even be known that the site has been compromised. Hence, the security of a Web Server is of prime importance.
- Before going into the specifics of securing computers and their services, we need to define the policies for how and by whom the Web Server will be used. This includes an acceptable use policy (AUP) for all users and a security policy. This policy is intended to define the rights and responsibilities of both the users and system administrators as well as define who these people are. This is really the first step in the security of any server as it sets out the rules

that everyone is to follow. And when the rules are broken, the AUP also defines what happens to those who have broken them.

1 Planning

- The organization should include explicit security requirements when selecting servers. There are many server vendors, and the security capabilities of their products vary accordingly. Many of the known and frequently exploited network server vulnerabilities apply only to certain products and platforms. If one considers security requirements when selecting servers, then it is possible to choose products with fewer vulnerabilities or select better security-related features, which can result in a substantially more secure site. This makes the long-term operation of web site more economical because by reducing the costs associated with administration tasks (such as patching systems) as well reduce costs caused by intrusions and their effects.
- The Web Servers are tempting targets for intruders because of the following reasons:
    - ✓ Public servers often have publicly known host names and IP addresses.
    - ✓ Public servers may be deployed outside an organization's firewall or other perimeter defences.
    - ✓ Servers usually actively listen for requests for services on known ports, and they try to process such requests.
- The vulnerabilities are exploited by the intruders due to the operational issues not addressed by the System Administrators. Improper configuration or operation of the Web server can result in the inadvertent disclosure or alteration of confidential information.

  Some of the effects of Web Server being compromised are as follows.

    - ✓ Information assets of the organization are at risk.
    - ✓ Information about the configuration of the server or network could be exploited for subsequent attacks
    - ✓ Information about who requested which documents from the server is known
    - ✓ Sensitive customer or user information is at risk

- ✓ The intruder may change the information stored on the Web server host machine, particularly the information intended to publish
- ✓ Execute unauthorized commands or programs on the server host machine including ones that the intruder has installed
- ✓ Gain unauthorized access to resources elsewhere in the organization's computer network
- ✓ Launch attacks on external sites from the server host machine, thus concealing the intruders' identities, and perhaps making the organization liable for damages
- ✓ Users can be disabled from accessing the Web site if all of its resources are consumed by a denial-of-service attack.

It is therefore essential to secure a Web Server through the following steps:

- ✓ Installing a Secure Server
- ✓ Configuring Web Server Software and the underlying Web Server host operating system
- ✓ Maintaining the Web Server's Integrity

2 Installation & Configuration

- ❖ It is recommended that a web server deployment plan be developed. It should take into consideration security issues related to the network architecture and the location of the Web servers. The deployment plan also involves following practices for increased security:

  - ✓ Determining how the Web Server will be connected to the network
  - ✓ Identifying the security concerns related to day-to-day administration of the Server.
  - ✓ Identifying the services offered by the server.
  - ✓ Identifying the network services that will be provided on the server.
  - ✓ Identifying the users or categories of users of the Web Server
  - ✓ Deciding how users will be authenticated and how authentication data will be protected

- ✓ Developing intrusion detection strategies for the server
- ✓ Documenting procedures for backup and recovery of information resources stored on the server.
- ✓ Determining how network services will be maintained or restored after various kinds of faults

Practices that should be adopted by organization for installing and configuring web server are as follows:

2.1 Isolate the Web server from public networks and the organization's internal networks.

- ❖ Care must be taken while placing a public Web server on an organization's network. It is highly recommended that the server be placed on a separate, protected sub network. This will ensure that traffic between the Internet and the server does not traverse any part of the private internal network and that no internal network traffic is visible to the server. To accomplish this, following steps may be taken:
    - ✓ Place the web server on a subnet isolated from public and internal network.
    - ✓ Use firewall technology to restrict traffic between a public network and the web server and between the web server and the internal network.
    - ✓ Place the servers providing email, directory and database services in support of the web site on a protected subnetwork.
    - ✓ Disable all source routing functions in the firewalls and routers protecting the public web server.
    - ✓ Disable IP forwarding and source routing on the web server and the server hosts that provide supporting services.

2.2 Configure the Web server with appropriate object, device, and file access controls. This is necessary for the following reasons

- ✓ To limit access to the Web server software

- ✓ To apply access controls specific to the Web server where more detailed levels of access control are required

To configure this, following steps may be taken:

- ✓ The web server should be configured to execute under a unique individual user and group identity. This is important for implementing access controls on various files, viz. Server log files, system software and configuration files, password files etc.
- ✓ The protection needed for various files, devices and objects specific to the web server should be identified.
- ✓ Time-outs and other controls to mitigate the effects of DOS attacks should be configured.
- ✓ The file serving of web server file listings should be disabled.

2.3 Identify and enable Web-server-specific logging mechanisms.

Web server logs are needed to:

- ✓ Alert about suspicious activity that requires further investigation
- ✓ Determine the extent of an intruder's activity
- ✓ Help to recover the systems
- ✓ Help to conduct an investigation
- ✓ Provide information required for legal proceedings

This can be accomplished by

- ✓ Identifying the web server software information to be logged, viz. Transfer log, Error log, Agent log, Referer log etc.
- ✓ Logging mechanism may also be required for capturing the performance of various programs, scripts, and plug-ins supported by the web server.

2.4 Consider security implications before selecting programs, scripts, and plug-ins for the Web server. To overcome the vulnerabilities following steps may be undertaken:

- ✓ Programs, scripts and plug-ins should be selected from a trustworthy source.
- ✓ The functionality that the external programs provide should be well understood.

2.5 Configure the Web server to minimize the functionality of programs, scripts, and plug-ins.

- ❖ Security vulnerabilities can be easily introduced in the acquisition, installation, configuration, deployment, and operation of external programs (Programs, scripts, and plug-ins). To accomplish this following step may be taken:

  - ✓ Verification of the acquired copy of the external program to check if it is authentic.
  - ✓ The external program acquired should be tested prior to putting it on the public web server.
  - ✓ Security tools for checking vulnerabilities in these acquired programs should be used.
  - ✓ Server Side Include functionality use should be disabled or restricted.
  - ✓ Execution of external programs present in the web server should be disabled. These external programs may be present in the default web server configuration, they should be located and disabled if not essential.
  - ✓ Configure the web server host operating system and the web server software access controls to restrict access to external programs.

2.6 Configure the Web server to use authentication and encryption technologies, where required.

Without strong user authentication, one may not be able to restrict access to specific information by authorized users. Before placing any sensitive or restricted (i.e. not for public consumption) information on a public Web server, one needs to determine the specific security and protection requirements and confirm that the available technologies, like SSL (Secure Socket Layer), S/HTTP (Secure Hypertext Transport Protocol), and SET (Secure Electronic Transaction). can meet these requirements.

2.7 Install security tools like whisker, ISS Internet Scanner, Nikto (A more comprehensive web scanner), SPIKE Proxy an open source HTTP proxy for finding security flaws in web sites. These tools help in finding the flaws in the web site as well as web server.

3 Operations & Maintenance

3.1 Maintain an authoritative copy of the Web site content on a secure host. The authoritative (i.e., verified, correct, trusted) copy of the public Web site content needs to be stored on a host that is separate from (and more secure than) the public Web server. The more secure host should preferably be on the internal network of the organization and protected behind one or more firewalls.

- ❖ Protect the Web server against common attacks. To accomplish this following action are essential:
  - ✓ Install Security tools like IDS, Integrity Checkers, Blocking and Filtering tools.
  - ✓ Update the installed detection tools to detect new attack patterns or events
  - ✓ Reduce attacks by updating firewall filtering mechanisms to deny new attacks
  - ✓ Temporarily disable specific services that might be vulnerable to attack
  - ✓ Use secure methods for restoration

3.2 The best practices for the operation of a web server can be summarized as below:

- ✓ Place the web server(s) in a DMZ. Set the firewall to drop connections to the web server on all ports but http (port 80) or https (port 443).
- ✓ Remove all unneeded services from the web server, keeping FTP (but only if it is required) and a secure login capability such as secure shell. An unneeded service can become an avenue of attack.
- ✓ Disallow all remote administration as far as possible.

- ✓ Limit the number of persons having administrator or root level access. Keep a record of the persons allowed such access.
- ✓ Log all user activity and maintain those logs either in an encrypted form on the web server or store them on a separate machine on the Intranet of the organization.
- ✓ Monitor system logs regularly for any suspicious activity. Install some trap macros to watch for attacks on the server. Create macros that run every hour or so that it would check the integrity of passwd and other critical files. When the macros detect a change, they should send e-mail to the system manager.
- ✓ Remove ALL unnecessary files from the script's directory for example /cgi-bin in Unix.
- ✓ Remove the "default" document trees that are shipped with Web servers.
- ✓ Apply all relevant security patches as soon as they are announced.
- ✓ If the machine must be administered remotely, require that a secure capability such as secure shell is used to make a secure connection. Do not allow telnet or non-anonymous ftp (those requiring a username and password) connections to this machine from any untrusted site. It would also be good to limit these connections only to a minimum number of secure machines and have those machines reside within the Intranet of the organization.
- ✓ Run the web server in a safe part of the directory tree so it cannot access the real system files.
- ✓ Run the anonymous FTP server in a safe part of the directory tree that is different from the web server's tree.
- ✓ Do all updates from the Intranet. Maintain the web page originals on a server on the Intranet and make all changes and updates here; then "push" these updates to the public server through an SSL connection. If this is done on an hourly basis, this practice will help avoid having a corrupted server exposed for a long period of time.
- ✓ Scan the web server periodically with tools to look for vulnerabilities.

- ✓ Have intrusion detection software monitor the connections to the server. Set the detector to alarm on known exploits and suspicious activities and to capture these sessions for review. This information can help recover from an intrusion and strengthen the defences.

4 Incident Handling

- ❖ A web server administrator should take the following steps after discovering a successful compromise:
  - ✓ Isolate compromised system(s) or take steps to contain attack so additional evidence can be collected
  - ✓ Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously and consult the organization's security policy.
  - ✓ Investigate "similar" hosts to determine if the attacker also has compromised other systems
  - ✓ Analyze the intrusion, including:
    - o Modifications made to the system's software and configuration
    - o Modifications made to the data
    - o Tools or data left behind by intruder
    - o Review system logs, intrusion detection, and firewall log files.
    - o Restore the system
  - ✓ Install clean version of operating system, or Restore from backups
    - o Disable unnecessary services
    - o Apply all patches
    - o Change all passwords (even on uncompromised hosts as required)
  - ✓ Reconfigure network security elements (firewall, router, IDS) to provide
    - o Additional protection and notification.
    - o Test system to ensure security
    - o Reconnect system to network
    - o Monitor system and network for signs that the attacker is attempting to access the system or network again.

- ✓ Report incident to CERT-In.
- ✓ Document lessons learned.

35 Procedural Memorandum for Sever Operating System

1 Planning

1.1 Identification of Server role

Before installation of server one should first identify role of the server. The server role means applications running on the server. The server can be deployed as a file server, print server, mail server, web server or database server. Based on the server role or applications running on it, System Administrator (SA) can categorize the server under low, medium or high threat perception. In all cases the SA have to plan for adequate server security to ensure confidentiality, integrity and availability of data.

1.2 Identification of network services

Network services will depend upon the role of the server like Account server, Web server, Mail server, Database server etc. As a general rule, a network server should be dedicated to a single service. This usually simplifies the configuration, which reduces the likelihood of configuration errors. It also eliminates unexpected and unsafe interactions among the services that present opportunities for intruders. In some cases, it may be appropriate to offer more than one service on a single host computer. For example, the server software from many vendors combines the file transfer protocol (FTP) and the hypertext transfer protocol (HTTP) services in a single package. For some organizations, it may be appropriate to provide access to public information via both protocols from the same server host, but it is not recommended since it is a less secure configuration.

1.3Physical Security

- ❖ Access to a server is very important, physical access to a server should be limited to only administrator and other server operators for backup etc. There should be no free access to servers. In general, following guidelines should be adhered to

- ✓ Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office
- ✓ Keep portable equipment secure
- ✓ Position monitor and printers so that others cannot see sensitive data
- ✓ Keep floppy disks and other media in a secure place
- ✓ Seek advice on disposing of equipment
- ✓ Report any loss of data or accessories to the SA
- ✓ Keep the system and sensitive data secure from outsiders
- ✓ Get authorization before taking equipment off-site
- ✓ Take care when moving equipment
- ✓ Log out, shut down or lock the system when leaving office
- ✓ Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure

1.4Methods of authentication

- ❖ Depending on the level of threat exposure to the server, authentication method should be chosen
- ❖ For Low Threat Exposure in build user/password mechanism available with the OS is an acceptable practice.
- ❖ For Medium Threat Exposure a choice could be made from user/password combination implemented by sever only with strong password policy or an external authentication server like TACKAC, RADIUS or KERBOUS may be implemented. For example, an external POP mail server may have radius server authenticating the user access.
- ❖ For High Threat Exposure a choice could be made from tokens, smart cards and biometrics devices (devices that recognize a person based on biological characteristics such as fingerprints or patterns of the retinal blood vessels.

2 Installation & Configuration

- ❖ The installation should be carried out from the original media, supplied by the vendor. The OS hardening should be done following the steps listed in the guidelines provided by the vendor for this purpose. This includes installation of patches, disabling of unwanted ports, etc. Care should be taken to match the release of patches with the OS version number.

2.1OS Hardening

2.1.1 Patches

- One of the most important tasks of the SA is to keep the most current patches for the OS and application software installed on a server. Many of these patches fix security vulnerabilities that are well known to intruders. There are two types of patches in general viz. Service Packs and Hotfixes. Installing these patches in order is important. Service Packs must be installed before the Hotfixes.
- Service packs are used to patch a wide range of vulnerabilities and bugs. The latest service pack that has been tested to work in one's environment should always be applied after installing the operating system. Service packs are cumulative; users need to install the latest Service Pack.
- Hotfixes are released more frequently than service packs and are meant to patch a more specific problem. Not all hotfixes may be needed for a particular system. Before installing these fixes on critical systems or installing them on a large number of devices, hotfixes should be tested to ensure that there is no conflict with other third-party drivers.

2.1.2 Disabling unwanted services and protocols

- Only required network services should be installed in the server. There are many default services with the standard OS software. Depending upon the role of server one should load only required network services, like on a mail server DNS service is not required.
- Disable unneeded network protocols, as each installed protocol takes server resources. Only essential protocols should be loaded on the server. Each network protocol should be configured for security settings, like in case of TCP/IP protocol only essential ports should be enabled.
- Security scanner tools like NMAP, NESSUS should be run to know which ports or services are currently open or running on the server. Any unwanted port/service should be stopped.

2.2 Protecting server against unauthorized network access

Firewalls and Intrusion Detection System (IDS) should be used on network infrastructure of the organization. The attacks like Denial of Service (DOS) can be avoided with the deployment of firewalls & IDS. For further details on firewalls refer to Firewall Security Guidelines.

2.3 Encryption

Encryption technologies on servers and networking equipment should be used for remote server administration. It prevents administrator passwords and other sensitive information from crossing one's network in clear-text. Use strong authentication when accessing hosts in one's domain to reduce the risk of a security breach due to false credentials, like in UNIX based systems SSH protocol employs public key cryptography and provides both encryption and strong authentication.

2.4 File system security

2.4.1.1 General

All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set. Any default shares should be removed. Only required file and object shares should be enabled on the server.

2.4.2 File permissions and access control

- ❖ Configure access controls for all protected files, directories, devices, and every change or decision not to change each object's permission should be documented along with the rationale
- ❖ Disable write/modify access permissions for all executable and binary files
- ❖ Restrict access of operating system source files, configuration files, and their directories to authorized administrators
- ❖ For UNIX systems, there should be no group/world-writable files unless specifically required by necessary application programs
- ❖ For NT systems, there should be no permissions set such that "the Everyone group has Modify permissions to files"
- ❖ Assign minimum level of access permission to all kernel files

- Establish all log files as “append only” if that option is available
- As a goal, preclude users from installing, removing, or editing scripts without administrative review. Proper procedure for enabling and enforcing the same may be established and fully documented
- Pay attention to access control inheritance when defining categories of files and users. Ensure that operating system should be configured so as newly created files and directories inherit appropriate access controls, and that access controls propagate down the directory hierarchies as intended when one assigns them
- Administrators should disable a subdirectory's ability to override top-level security directives unless that override is required

2.4.3 Tools

- Install tools for checking integrity of files on the server. This will also help in analyzing and tracking intruders, in case of an intrusion. For UNIX, file integrity and analysis tools like Tiger, Tripwire, Coroner’s Toolkit can be used.
- After configuring the server OS file checksum should be generated and stored on a removable media safely. SA should run file checksum utility 2-3 times a day to compare with the configured checksum, any differences should be analyzed suitably. Whenever server is reconfigured, a new checksum should be generated, discarding the old checksum.

2.5 Account Policy

2.5.1 User privileges & Rights

- Document the categories of users that will be allowed access to the provided services. Categorize users by their organizational department, physical location, or job responsibilities. A category of administrative users who will need access to administer the network server and a category for backup operators needs to be created. Normally, access to network servers should be restricted to only those administrators responsible for operating and maintaining the server. Determine the privileges that each category of user will have on the computer. To document privileges, create a matrix that shows the users or user categories cross-listed with the privileges they will possess. The privileges are customarily placed in groups that define what system resources or services a user can read, write, change, execute, create, delete, install, remove, turn on, or turn off. For many resources, such as program and data files, the access controls provided by the OS are the most obvious means to enforce access privileges. Also, consider using encryption technologies to protect the confidentiality of sensitive information.

2.5.2 Passwords

- There should be password policy in the organization. The most common method of authentication is password. The responsibility of selecting a password that is hard to guess generally falls on users. To decrease the chances of guessing password, user must select a hard-to-guess or strong password.
- A strong password must:
  - ✓ Be as long as possible
  - ✓ Include mixed-case letters.
  - ✓ Include digits and punctuation marks.
  - ✓ Not be based on any personal information.
  - ✓ Not be based on any dictionary word, in any language.
- While most shared systems can enforce at least some of these rules, almost none have features to enforce all of them. Despite all these efforts the passwords could be guessed given enough time. Thus, a user must also:
  - ✓ Change his/her password regularly, in order to limit the amount of time available to persons to guess it. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed regularly.
  - ✓ Never use the same password twice.

- Some systems have a password expiry feature, which forces user to change his password periodically. Some systems incorporate a password history feature, which disallows user from reusing one of his last n passwords. When faced with a password history mechanism, some users may change their password n times, and return it to its original value, so as to avoid having to remember a new password value. To prevent this, systems should either have an unlimited-length password history, or prevent users from changing their password more than once daily.

2.6 Operation & Maintenance

2.6.1 Patches

- The server should be updated regularly for any latest service packs and hotfixes. With this some of the known attacks can be avoided. Server software like mail server, web server, database server etc. should always be updated for latest patches or software versions. The application software installed on server (if any) like web browser should also be regularly updated with latest patches. This keeps the server secure, from any attacker to exploit bugs or vulnerabilities in the server software. All new patches should be tested offline and then only put on the actual servers. After the patches are applied OS hardening should be redone.

2.6.2 Anti-virus

- Computer viruses spread easily through floppy disks, email, or programs downloaded from the Internet. Potential problems range from changing data to reformatting system hard drive. Once created, viruses can spread without help from their creators. One can get them from computers at the office, from using computer at home, or from an email. To protect the systems, it is recommended that a virus scanning/detecting/cleaning program must be installed on the computer systems and It should be regularly updated.
- New viruses are created continuously, and vendors of virus detection software offer updates to detect them. To get the latest updates, check the vendor web page. Some virus detection software allows getting the updates automatically via the Internet. The anti-virus software should be configured to schedule these updates at least twice a week.
- It is recommended that computers do a quick scan when the system is booted, as programs are loaded into memory, and when new data is detected (from email, removable media). Computers should get a full

system scan periodically which can be scheduled to run when the users are away for the evening.

- ❖ Prior to making software available to many machines on a network, install it on a stand-alone device and scan it for computer viruses.

2.6.3 System monitoring

2.6.3.1 Performance

- ❖ Server performance should be monitored on regular basis. There are built-in tools in the server OS. These tools can monitor server health for hardware components like CPU, memory, hard disk, I/O etc. and also application software on the server like web server application, database server application etc. Any degradation in the server performance can also be linked with triggers and alarms, which sends warning or alert messages to the SA, who can take necessary remedial actions. Server performance monitoring also helps in detecting attacks, like when a hacker misuses some server to launch attacks, the processes running to accomplish attack may degrade server performance.

2.6.3.2 Audit & logs

- ❖ Server should be regularly audited and log files scanned for knowing any attacks and intrusions, preferably daily. For small organizations separate logging server with hardened OS should be implemented. Server to logging server communication should also take place over a secure i.e. encrypted channel. Additionally, the logs must also be encrypted & access to it should be highly restricted. For very high threat exposure IDS should be installed.

The following guidelines should also be followed

- ✓ Make use of facilities provided with server OS to assist with disseminating log files e.g. FreeBSD emails a summary of important system and security information to root as part of its pre-configured crontab
- ✓ Use a reliable mechanism for log rotation. This may include replacing an existing logging daemon/service with a more secure or full-featured one.

- ✓ Implement automated reporting facilities so that scans of one's network are reported immediately to the SA.
- ✓ Keep a logbook of all system administration activities on each server.

2.6.4 Incident detection tools

- ❖ Appropriate Tools for Incident Detection must be installed on the server. The reports generated by the tools should be monitored regularly to check any change in the system, unauthorized access, DoS attacks etc. The alarms and event notifications should also be set appropriately.

Some of the tools are:

Windows based servers	: SamSpade, Retina, Fport, NBTScan
Unix based server	: NMAP, SAINT, SARA, THC-Amap, THC-Hydra

These tools are very helpful in detecting server compromise and similar attacks.

2.6.5 Backups

- ❖ For the purpose of data safety, Backup policy must be made. It should cover methods like cold, warm and hot backups, role of backup operators and their access rights. All users must recognize that all forms of data storage are subject to data loss. For example, a disk crash may result in loss of server data. Users must therefore take steps to ensure there are copies of important data, called backups. Users should ensure security of data on the equipment including backups of important data held on it. Information stored on central servers is to be backed up regularly by the System Administrator.

All users should follow the following guidelines:

- ➢ Wherever possible, save important data onto centrally managed network drives, which are generally backed up daily
- ➢ Keep paper copy of server configuration file
- ➢ Keep the DATs or other removable media in a secure location away from the computer
- ➢ Regularly check that another system can read the removable media

2.6.6 Recovery

There could arise the situation when server crashes due to some hardware faults like disk failures, network failures, etc. For such failures, recovery methods of running server without affecting server services should be defined like disk mirroring, disk arrays or recovery from backup media. In case of software failures also, steps should be defined to reload the server services or OS accordingly. Recovery tools should be installed on the server like hard disk recovery software. With the help of such tool's server OS is recovered without loss of time. For critical applications fault tolerant systems may be installed.

3 Incident Handling

3.1 What is an Incident?

❖ An Incident is an act of violating an explicit or implied security policy, assuming there exists security policy in the organization. The types of activity considered as violation of a typical security policy are characterized below. These activities include but are not limited to:

- ✓ security violation in which a system resource is exposed or is potentially exposed to unauthorized access
- ✓ unwanted disruption or denial of service
- ✓ any adverse event which compromises some aspect of computer or network security
- ✓ the unauthorized use of a system for the processing or storage of data
- ✓ changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent

3.2 Incident detection

Tools installed for monitoring server performance and incident detection helps in detecting an incident. The symptoms of an incident could be like sudden degradation in server performance, server compromise, failure of service(s), defacement of web site contents, spam mails, mail route abuse etc.

3.3 Safeguard measures after incident

- ❖ When a SA finds that some abnormal behaviour in server performance or alarms through incident detection tools are noted the following steps should be taken

  - ✓ Change administrator password of the server
  - ✓ Disconnect the server from network, depending upon the severity of Incident
  - ✓ Or stop server services like web server, mail server etc.
  - ✓ Or worst is switch off server

3.4 Incident reporting

An Incident should immediately be informed to CERT-In by means of telephone, fax, email or web. The site address of CERT-In is www.cert-in.org.in. After reporting the incident to CERT-In, advisory notes of CERT-In should be followed for recovering from incident.

36 Procedural Memorandum for Workstation Operating System Security

The word "workstation" is used in this module to mean the combination of the hardware, operating system, application software, and network connection.

Workstations must be configured and used in a secure manner. To secure a workstation, a staged approach is recommended for implementation of security practices in the following areas:

- ✓ Planning and executing the deployment of workstation.
- ✓ Configuring workstation to help make them less vulnerable to attack.
- ✓ Maintaining the integrity of deployed workstation.
- ✓ Improving user awareness of security issues.

1 Planning

Securing desktop workstations should be a significant part of the network and information-security strategy because sensitive information is often stored on workstations, which are connected to the rest of the networked world. It can eliminate many networked systems vulnerabilities and prevent many security problems if workstation is configured securely before its deployment. Vendors typically set computer defaults to maximise available functions, so usually there is a need to change defaults to meet the organisation's security requirements.

1.1 Purpose of workstation

❖ Following points should be considered to secure a workstation:

- ✓ What categories of information will be stored on the workstation?
- ✓ What categories of information will be processed on the workstation (but retrieved from and stored on another workstation)?

- ✓ What are the security requirements for that information?
- ✓ What network service(s) will be provided by the workstation?
- ✓ What are the security requirements for those services?

1.2 Network service software

❖ Many operating system vendors bundle network service software for both clients and servers. For major services, however, third party vendors may provide products that offer much better security. When making a choice, special attention should be paid to the ability of candidate packages to meet the organisation’s security requirements, and the same should be documented. Also identify other applications or utility software that are required to be installed on the computer. Include not only user-oriented application software, but also system-related software and security-related software.

1.3 User Categorisation

For workstations, the categories of users should be defined. The categories should be based on user roles that reflect their authorised activity. The roles are often based on similar work assignments and similar needs for access to particular information resources-system administrators, software developers, data entry personnel, etc. If appropriate, remote users should be categorised as temporary or guest users.

1.4 User Privileges

During installation of Operating System, all the steps made to implement the security policy of the organisation, should be documented and all the parameters that are set should be described. The installation procedure should also specify the vendor's security-related updates or patches that are to be applied to the operating system. If possible, have a single person perform the installation procedure for each workstation and capture each installation step in a documented manner such as through using a checklist.

1.5 Develop and follow a Documented procedure for installing an Operating

- One of the most important tasks of the SA is to keep the most current patches for the OS and application software installed on a server. Many of these patches fix security vulnerabilities that are well known to intruders. There are two types of patches in general viz. Service Packs and Hotfixes. Installing these patches in order is important. Service Packs must be installed before the Hotfixes.
- Service packs are used to patch a wide range of vulnerabilities and bugs. The latest service pack that has been tested to work in one’s environment should always be applied after installing the operating system. Service packs are cumulative; users need to install the latest Service Pack.
- Hotfixes are released more frequently than service packs and are meant to patch a more specific problem. Not all hotfixes may be needed for a particular system. Before installing these fixes on critical systems or installing them on a large number of devices, hotfixes should be tested to ensure that there is no conflict with other third-party drivers.

2 Installation and Configuration

2.1 OS and Application S/W Hardening

- ❖ OS media should be procured only from an authorised vendor of the manufacturer.
- ❖ To patch up the vulnerabilities and loopholes of the OS, install all the latest service packs, security patches, hot-fixes, OS updates, etc. as available and applicable for this version at the time of installation. These patches/updates etc. are available from the vendors as well as from their websites.
- ❖ Boot on "OS banner" should be disabled, if possible.
- ❖ Initially, all the ports should be closed/disabled and may be enabled/opened as and when required.
- ❖ Turn off all network services that are not needed.
- ❖ Define how long the computer or application can be used. Create a mandatory automated logoff policy based on inactivity or time of day.
- ❖ Disable application features that expose vulnerability through configuration changes.
- ❖ Control access to settings, control panels and run functions. Define who has access to applications by location, time of day or time period.

2.2 Stick to Essentials on the Network

- ❖ Most desktop workstations do not need all the settings enabled by default, so the operating system should be configured to provide only the services specified in the deployment plan.

  - ✓ Disable and remove all the network services that are not required by the deployment plan. It is recommended that workstation should be configured to offer only the services as per the deployment plan.
  - ✓ It is recommended to use the configuration principle "deny first, and then allow", that is, turn off as many services and applications as possible and then selectively turn on those that are essential.

2.3 Configure multiple computers using a tested model replication procedure

- ❖ When deploying several computers, especially desktop workstations, across an organisation, it is better to configure one appropriately and then propagate that configuration to all the others. It should be ensured that this is done in a secure manner, especially if a network is used for propagation. This helps in establishing a consistent level of security on all the computers to LAN. It also facilitates consistent updating of all computers as and when necessary.

2.4 Configure Network Service clients to Enhance Security

For the network services, organisation's deployment plan should include electronic mail, access to the Web, Domain name services, file transfers, and access to corporate databases. For each service, the workstation should be configured as a client or as a server mode. Workstations are normally configured as clients for several network services. Therefore, these should be configured for the planned behavior of those clients: the levels of access required, the type of access (read, write, etc.), and other aspects of the configurations required for client software.

2.5 Access to Information

For many resources, such as program and data files, the access controls provided by the operating system are the most obvious means to enforce access privileges. Also, consider using encryption technologies to protect the confidentiality of sensitive information. In some cases, protection mechanisms will need to be augmented by policies that guide user's behaviour related to their workstations.

2.6 LAN Security

- ❖ Many organisations use a broadcast technology such as Ethernet for their local area networks. In these cases, information traversing a network segment can be seen by any computer on that segment. So, only trusted computers should be placed on the same network segment, or else the information should be encrypted before transmitting it.

For securing LAN, the guidelines, to be followed, are:

- ✓ If, a workstation is connected to LAN, users should not be allowed to use a modem.
- ✓ Unauthorised copies of software should be removed from all the systems connected through LAN.
- ✓ If users are allowed to install personal software on their workstations, ensure that: the software is licensed; and the software does not compromise any security mechanisms implemented on the LAN. For example, software that can be used to "sniff" network traffic should not be permitted on the LAN.

2.7 Password

There should be a password policy in the organisation. The most common method of authentication is password. The responsibility of selecting a password, that is hard to guess, falls on users. To decrease the chances of guessing password, user must select a hard-to-guess or strong password. Detailed procedure for password selection has been provided in the Server OS Guidelines.

3 Maintenance & Operations

- ❖ Keep the operating system and application software up to date. Updates are available from vendors on a regular basis.
- ❖ Delete all un-sanctioned programs and directories from the workstation. They can be cleverly renamed as keystroke-capturing programs, network sniffer programs, or viruses.
- ❖ To prevent the last logged-in user name from being displayed, use security procedures at installation stage. For example, in Windows based systems when Ctrl-Alt-Del is pressed, a login dialog box appears which displays the name of the last user who logged in to the computer, and makes it easier to know a user's name that can later be used in a password-guessing attack.

This can be disabled using the security templates provided on the installation CD.

- ❖ Enforce system file hardening and configuration against attack from virus, worms, Trojan horse or other malicious software.

Use keywords to restrict data from being sent or received through the Internet.

- ✓ Lock folders and files to prevent unwanted access.
- ✓ Prevent rename, delete, copy, move or changes to file attributes.
- ✓ Customise application to show only desired menu options.
- ✓ Restrict access to dialog boxes such as print, save, import, etc.

3.1 Protection from Viruses, Trojan Horse and Malicious scripts

- ❖ Install virus protection software on the workstation, and update it on a regular basis. Updates for the new viruses are generally made available every week. Configure the Anti-virus software properly, so that it actively scans all incoming objects for virus infections.

- ✓ Never execute a program (".exe" file) if one does not know what it is/does. This is particularly the case for files that are received via e-mail as attachments, or are downloaded from a website that cannot be trusted.
- ✓ Make sure that on every occasion, whenever diskettes and other media are brought in, they are checked for viruses.
- ✓ Do not install / use illegal or "pirated" software.
- ✓ Do not use shareware unless absolutely sure that the software is free of viruses.
- ✓ Do not install any software without permission of the System Administrator.
- ✓ If any program is downloaded from Bulletin Board or the Internet, scan it for viruses before using.
- ✓ Do not install or play games on the computers. Games are commonly used as a way to spread viruses.

- ✓ Make sure that diskettes used to store software programs are write-protected. This prevents viruses from being copied onto such diskettes.
- ✓ If a computer has come with pre-loaded software or its hard drive is preformatted, scan the hard drive for viruses before using the computer.
- ✓ Do not boot computers with any diskette that has not been scanned for viruses.
- ✓ Public-domain software should not be used until it is tested and allowed by SA.

3.2 Deployment of Personal Firewall/IDS

- ❖ To prevent intruders from hacking into systems via LAN / Internet connection firewall must be installed & configured.
- ❖ The "intruder alert" facility, should be activated and all alerts should be acted upon.
- ❖ To detect unauthorised access of a system, IDS must be installed & configured.

3.3 System Access Control

- ❖ Allow file sharing on machines after securing them, and that too only to authorised users only. Make sure that object, device, and file access controls are appropriate. Protect files and folders by making them as read-only for shared use.
- ❖ Do not allow anonymous access of any kind (e.g., FTP, dial-up) to a workstation

3.4 Internet access, S/w Download & E-mail Attachments

- ❖ Only allow users' access to approved websites.
- ❖ Do not open e-mail received from Unknown person.
- ❖ Define the time period of Internet access and email usage.

3.5 Audit Trails & Logs

- ❖ Log files may be the only record of suspicious behaviour. These should be activated. Log files are required for the following:
  - ✓ To alert for the suspicious activity that requires further investigation.
  - ✓ To determine the extent of an intruder's activity.
  - ✓ To recover operating system software.
  - ✓ To provide information required for legal proceedings
  - ✓ To investigate workstation hard disks on a regular basis for suspicious files. Use a naming convention for files and directories. Be sure to look for hidden files and directories.

Security audits should be done periodically to expose system vulnerabilities.

3.6 Data Encryption

- ❖ Consider employing a file encryption program if the information stored on a workstation is highly confidential. Similarly, consider a mail program that supports encryption (S/MIME or PGP), if sending highly confidential information in messages.
- ❖ Enable Encrypting File System. This will help in preventing a hacker from accessing files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on Folders, and not files. All files that are placed in that folder will be encrypted automatically.

3.7 Backups

- ❖ Always backup files & folders periodically using standard backup utilities.
- ❖ Make separate backups of data files and software and store backup diskettes/tapes in a safe and secure location away from computer. Backups may be the only source to recover any destroyed file.
- ❖ Always backup the data before leaving the workstation.

3.8 Data recovery from Backups

Recovery tools should be installed on the workstation like hard disk recovery software. With the help of such tool's workstation OS is recovered without loss of time.

4 Incident Handling

In case of occurrence of any incident, like workstation Break-in, DoS attack, Trojan Horse attack, etc, steps should be defined how to know about incident, incident reporting and recovery thereafter.

4.1 What is an Incident?

- ❖ An Incident is an act of violating an explicit or implied security policy, assuming there exists a security policy in the organisation. The types of activity considered as violation of a typical security policy are characterised below:
  - ✓ Security violation in which a system resource is exposed or is potentially exposed to unauthorised access.
  - ✓ Unwanted disruption or denial of service.
  - ✓ Any adverse event which compromises some aspect of computer or network security.
  - ✓ Unauthorised use of a system for the processing or storage of data.
  - ✓ Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.

4.2 Incident detection

Tools installed for monitoring workstation performance and incident detection help in detecting an incident. The symptoms of an incident could be like sudden degradation in workstation performance, workstation compromise, failure of service(s), abuse etc.

4.3 Safeguard measures after incident

- ❖ When a system administrator finds some abnormal behavior in workstation performance; or alarms through incident detection tools are noted, the following steps should be taken:
  - ✓ Change administrator password of the workstation
  - ✓ Disconnect the workstation from network, depending upon the severity of the incident.

4.4 Incident reporting

An Incident should immediately be informed to CERT-In by means of telephone, fax, email or web. The site address of CERT-In is www.cert-in.org.in. After reporting the incident to CERT-In, advisory notes of CERT-In should be followed for recovering from incident

37 Conclusion

Although there are a number of information security standards available, an organisation can only benefit if those standards are implemented properly. Security is something that all parties should be involved in. Senior management, information security practitioners, IT professionals and users all have a role to play in securing the assets of an organisation. The success of information security can only be achieved by full cooperation at all levels of an organisation, both inside and outside.

38 Reference

http://www.cert-in.org.in/
https://www.sans.org/
https://www.pcisecuritystandards.org/
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
https://www.sans.org/security-resources/glossary-of-terms/
http://www.tnpsc.gov.in/tender/tender_rules.pdf
http://www.gswan.gov.in/PDF/Computer%20System%20Security%20Guidelines.pdf

39 Appendix A: Glossary and Acronyms

Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a disruption.

Business Continuity Plan: A plan which allows critical business functions to continue in the event that primary business facilities or resources are not available.

Business Impact Analysis: An analysis which identifies information, applications, processes, and systems required to support critical business processes and functions.

Chief Information Security Officer (CISO): The CISO is the internal and external point of contact for all information security matters. The designation of the Chief Information Security Officer is intended to establish clear accountability for development and maintenance of policy for information systems security management activities, provide for coordination and review of the information security program, and ensure greater visibility of such activities within and between agencies.

Computer Emergency Response Team (CERT): Personnel responsible for coordinating the response to computer security incidents in an organization.

Custodian: Guardian or caretaker; the holder of data, the agency or department charged with implementing the controls specified by the owner.

Department of Information Technology (DIT): The agency responsible for information systems, networking, and data management.

Disaster Recovery Plan: The preplanned sequence of events that allows for the recovery of an information system facility and information systems and applications.

Electronic Mail (email): Any message, image, form, attachment, data, or other communication sent, received or stored within an electronic mail system.

Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Firewall: A rule-based hardware or software control device that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Host: A computer system that provides computer service for a number of users.

Information: Any and all data, regardless of form, that is created, contained in, or processed by, information systems facilities, communications networks or storage media.

Information Attack: An attempt to bypass the physical or information security measures and controls protecting a system. The attack may alter, release or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information systems (IS): Any and all computer-related equipment and components involving g devices capable of managing, transmitting, receiving or storing information or data including, but not limited to, a USB drive, CD-R, laptop or personal computer, personal digital assistant (PDA), cell phone, handheld computer, servers and computer printouts. Additionally, it is the procedures, equipment, facilities, software and data that are designed, built, operated and maintained to create, collect, record, process, store, retrieve, display and transmit information.

Internal Auditor: Ensures that an agency's information systems are being adequately secured, based on risk management, as directed by the CISO acting on delegated authority for risk management decisions.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and educational institutions.

Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's Intranet is usually protected from external access by a firewall.

Local Area Network (LAN): A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Off-site Storage: Based on data criticality, off-site storage should be in a geographically different location from the campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it inanother secured location on the campus may be appropriate.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

Portable Computing Device: Any easily portable device that is capable of receiving and/or transmitting data to and from Information systems. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers and cell phones.

Production System: A computer system used to process an organization's daily work. Contrast with a system used only for development and testing or for ad hoc inquiries and analysis.

Risk Assessment: The process of evaluating threats and vulnerabilities, both known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Security Incident: A successful or unsuccessful unauthorized entry or information system attack. Security incidents may include unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. Ay incident may also include any violation of security policy or acceptable use agreements.

Server: A server is a system that provides services to client systems. The computer that a server program runs in is also frequently referred to as a server (though it may contain a number of servers and client programs).

Spam: Mass-delivered, unrequested advertising delivered via email.

System Administrator: Person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Systems Development Life Cycle Standards (SDLCS): A set of procedures to guide the development of production application software and data items. The SDLCS includes design, development, maintenance, quality assurance and acceptance testing.

Trojan: Destructive programs that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by email or on a removable media device, often from another unknowing victim, or may be urged to download a file from a Website.

User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

Vendor: Someone who exchanges goods or services for money.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive results. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in programs that allow users to generate macros.

Web Log (Blog): A public website where users post informal journals of their thoughts, comments, and philosophies, updated frequently and normally reflecting the views of the blog's creator.

Web Page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

Web Server: Information systems that host and deliver Internet services.

Website: A location on the World Wide Web, accessed by typing its address (Universal Resource Locator, or URL) into a Web browser. A Website always includes a home page and may contain additional documents or pages.

World Wide Web (WWW): A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Microsoft Internet Explorer.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

40 Appendix B: Incident Reporting Procedures

- The purpose of this procedure is to provide a computer incident reporting and response process will employ in the event of an intrusion to or an attack on government computer systems. This reporting and response process provide a coordinated approach to handling incidents across all levels of government. The intention of this coordinated process is to minimize or eliminate the propagation of an event to other computers and networks. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators. Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. Centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions.
- An Incident should immediately be informed to CERT-In by means of telephone, fax, email or web. The site address of CERT-In is www.cert-in.org.in. After reporting the incident to CERT-In, advisory notes of CERT-In should be followed for recovering from incident
- It is the responsibility of each agency to identify procedures, whereby its IT staff will determine if a computer or cyber incident has taken place and if it should be reported using this process.
- The Incident Reporting Form is attached.

Incident Reporting Form

Form to report Incidents to CERT-In

For official use only: Incident Tracking Number: CERTIn-

1. Contact Information for this Incident:

□

Name:	Organization:	Title:
Phone / Fax No:	Mobile:	Email:

Address:

2. Sector: (Please tick the appropriate choices)

Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum	InfoTech Other ______

3. Physical Location of Affected Computer/ Network and name of ISP. □			
4. Date and Time Incident Occurred:			
Date:		Time:	
5. Is the affected system/network critical to the organization's mission? (Yes / No). Details. □			
6. Information of Affected System:			
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Hardware Vendor/ Model

7. Type of Incident:

□

Phishing
Network scanning /Probing
Break-in/Root Compromise
Virus/Malicious Code
Website Defacement
System Misuse

Phishing Network scanning /Probing Break-in/Root Compromise Virus/Malicious Code Website Defacement System Misuse	Spam Bot/Botnet Email Spoofing Denial of Service (DoS) Distributed Denial of Service (DDoS) User Account Compromise	Website Intrusion Social Engineering Technical Vulnerability IP Spoofing Other_________________

8. Description of Incident:

9. Unusual behavior/symptoms (Tick the symptoms)

System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of	Anomalies Suspicious probes Suspicious browsing New files Changes in file lengths or dates Attempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns

privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Unusual log file entries Presence of new setuid or setgid files Changes in system directories and files Presence of cracking utilities Activity during non-working hours or holidays Other (Please specify)
10. Has this problem been experienced earlier? If yes, details. ☐	
11. Agencies notified?	

Law Enforcement	Private Agency	Affected Product Vendor	- Other___________ ________ □

12. When and How was the incident detected: □
13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)

Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION□
14. IP Address of Apparent or Suspected Source: □

Source IP address:	Other information available:

15. Security Infrastructure in place:

	Name	OS	Version/Release	Last patched/updated
Name OS Version/Release Last Patched /				

Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

16. How Many Host(s) are Affected

1 to 10	10 to 100	More than 100

17. Actions taken to mitigate the intrusion/attack: □

No action taken System Binaries checked	Log Files examined System(s) disconnected form network	Restored with a good backup - Other____________________ ________________________

Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident

Mail/Fax this Form to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax: +91-11-24368546 or email at: incident@cert-in.org.in