CERT-In

Indian Computer Emergency Response Team
Handling
Computer Security Incidents

IT Security Policy

Department of Information Technology
Ministry of Communications and Information Technology
Government of India

What is an IT Security Policy?

The Information Security Program for an organization can be broken down into specific stages as follows:

(a) Adoption of a security policy
(b) Security risk analysis
(c) Development and implementation of a information classification system
(d) Development and implementation of the security standards manual
(e) Implementation of the management security self-assessment process
(f) On-going security programme maintenance and enforcement
(g) Training.

A security policy defines the rules that regulate how an organization manages and protects its information and computing resources to achieve security objectives. One of the policy's primary purposes in detecting signs of intrusion is to document important information assets and the threats to those assets that an organization chooses to address.

Preparation procedures include the actions necessary to observe systems and networks for signs of unexpected behavior, including intrusion. Observation can take the form of monitoring, inspecting, and auditing. From these procedures, all concerned parties are able to determine the operational steps they need to take to comply with the policy. These steps will thereby uphold the security of an organization's information and networked systems.

Security policies and procedures that are documented, well known, and visibly enforced establish expected user behavior and serve to inform users of their obligations for protecting computing assets. Users include all those who access, administer, and manage the systems and have authorized accounts on the systems. They play a vital role in detecting signs of intrusion.

This is the first in a series of security guidelines that will be issued by CERT-In to help the System Administrators of various organizations in the country secure their computer systems. The present set comprises very preliminary guidelines and tries to focus the attention of the system administrators on security. More detailed guidelines will follow in due course.

An IT Security Policy is the most critical element of an IT security program. A security policy identifies the rules and procedures that all persons accessing computer resources must adhere to in order to ensure the confidentiality, integrity, and availability of data and resources.

An IT Security Policy

- Communicates clear and concise information and is realistic;
- Includes defined scope and applicability;
- Makes enforceability possible;

- Identifies the areas of responsibility for users, administrators, and management;
- Provides sufficient guidance for development of specific procedures
- Balances protection with productivity;
- Identifies how incidents will be handled; and
- Is enacted by a senior official with support of top management

Development of a security policy should be a team effort with involvement of IT User departments, IT department, security officials, senior management, and those who have a thorough understanding of the business rules of the organization so as to enable commitment to implementation. A security policy should not impede an organization from meeting its mission and goals. It should provide the organization with the assurance and the "acceptable" level of asset protection from external and internal threats.

A key point to consider is to develop a security policy that is flexible and adaptable as technology changes. Additionally, a security policy should be a living document routinely updated as new technology and procedures are established to support the mission of the organization.

The following framework is designed to provide the basis for an organization to develop its own IT Security Policy. This is based on the BS 7799 Security standards and the security policy guidelines issued by NIST, SANS, BSI and other similar agencies. Templates of how to write a security policy can be seen at SANS website. References to these websites are given at the end of this document. .

All items listed under different headings need not be applicable to each and every organization. This framework is meant as guideline to assist an organization in determining its security needs and in laying down the policies, and subsequently the procedures to meet those needs.

The implementation of Security Policy, duly adopted by an organization must be audited to ensure compliance. It is recommended that security audit should be done by independent auditors atleast once a year. CERT-In will try to establish a Panel of Information Security Auditors for this purpose.

Information Technology Security Policy – areas of control

1. Policy

- Scope
- Terms and definitions
- Security policy
- Information security policy document

2. Organisational Information Protection

Review and evaluate

- Specification of responsibilities and of requirements documents for IT users

Security organization (including BCP)

- Security mechanisms and their enforcement
- Resource management
  - People,
  - Broad security functions
  - Access rights/authorizations (Granting of site access authorizations; Granting of access rights)
  - Division of responsibilities and separation of functions
  - Assignment of responsibility for information, applications and IT components
  - Enforcement of policies
  - Response to violations of security policies

Information security infrastructure

- Identification of components in the entire organization
- Business Continuity Planning
- Infrastructure setup
- Classification of components
- Correct disposal of resources requiring protection
  - Maintenance regulations

3. Control and Sensitivity of assets

- Asset classification and control
  - Systems: (Name, access controls)
  - Information systems (Name, access controls)
- Accountability for assets
  - Systems: (owner(s))
  - Information systems (owner(s))
- Information classification – Public; Confidential
  - Criticality/Sensitivity – Minimal, More, Most.

4. People Issues

- Personnel security – background checking

- Security in job definition and resourcing
- Roles and responsibilities
- User training including compliance with relevant laws, regulations and provisions
- Arrangements for substitution
- Training for IT applications and assigned roles
- Education on IT security measures
- Regulated procedure as regards termination of employment
- Outsourced Personnel
- Contracting requirements
- Control and Security Issues

5. Physical Protection

Physical and environmental security

Building Protection

- Identification of Secure Areas and General Controls
- Access Control
- Intruder and fire detection devices
- Protection against entering and breaking
- Fire safety inspection
- Supervising or escorting outside staff/visitors
- Entry regulations and controls
- Alert plan and fire drills
- Waste Disposal

Fire Protection

- Compliance with fire-protection regulations/requirements imposed by the local fire department
- Hand-held fire extinguishers
- Fire sealing of trays
- Use of safety doors

Power Supply

- Compliance with relevant standards/specifications
- Regulations governing access to distributors
- Adapted segmentation of circuits

- Lightning protection devices
- Galvanic separation of external lines

Cabling

- Physical protection of lines and distributors
- Prevention of transient currents on shielding
- Removal, or short-circuiting and grounding, of unneeded lines
- Documentation on, and marking of, cabling
- Provision of redundant lines

Server room

- Intruder and fire detection devices
- Locked doors
- Avoidance of water pipes
- Over voltage protection
- Emergency circuit-breakers
- Air conditioning
- Local uninterruptible power supply
- Remote indication of malfunctions
- Redundancies in the technical infrastructure
- Technical and organizational requirements for server rooms

Protective Cabinets as archive for data media

- Secure Locking
- Fire proofing

6. System and Infrastructure management

Communications and operations management

- Establishment of networks
- Establishment of sub networks, if any
- Redundant communication links, if any
- Use of encryption procedures for network communications, if installed
- Agreement regarding connection to third party networks
- Agreement regarding the exchange of data with third parties

Operational procedures and responsibilities

- Software acceptance and approval procedure
- Data media control
- Ban on using non-approved software
- Survey of the software held
- Provisions governing the use of passwords
- Procedure for Checking the log files

- Continuous documentation of information processing (especially administration)
- Guidelines for access control
- Change management
- Regular checking of technical IT security measures
- Security objectives for the use of standard software
- Procedures regarding the use of outside staff

Protection against computer viruses

- Identification of IT systems potentially threatened by computer viruses
- Selection of a suitable computer virus scanning program
- Updating the computer virus scanning programs used
- Periodic runs of a virus detection program
- Checking of incoming data for macro viruses
- Reporting computer virus infections
- Procedure in case of computer virus infection
- Use of a virus scanning program when exchanging of data media and data transmission Ban on using non-approved software
- Documentation on changes made to an existing IT system
- Obtaining information on security weaknesses of the system
- Use of BIOS security mechanisms
- PC emergency floppy disk
- Regular data backup

System planning and acceptance

- Approval of Standard software
- Developing a test plan for Standard Software
- Testing Standard software
- Deciding on and developing the installation instructions for standard software
- Installation and configuration of Standard software
- Guaranteeing the integrity of Standard software
- De-installation of standard software
- Licence management and version control of Standard software
- Obtaining information on security weaknesses of the system

Housekeeping

Network management

- Survey of the existing network environment
- Analysis of the existing network environment
- Documentation on the system configuration
- Development of a network management concept
- Developing a system management strategy
- Requirements to be met by a system management system

- Selection of a suitable system management product
- Documentation on the system configuration
- Selection of a suitable network management protocol
- Secure configuration of active network components
- Regular backup of configuration data of active network components
- Resource management
- Segmentation of a network
- Identification of critical areas
- Redundant arrangement of network components
- Backup of configuration files
- Survey of load factors and analysis of traffic flow
- Determination of network bottlenecks
- Use of a network management software package
- Obtaining information on security weaknesses of the system
- Change management procedures
- Documentation on changes made to an existing IT system
- Division of administrator roles in PC networks
- Checking the log files
- Secure access mechanisms for local administration
- Auditing and logging of activities in a network
- Auditing of a network
- Sporadic checks of the restorability of backups

Media handling and security

- Backup copy of the software used

Exchanges of information and software

- Exchange of Data/Media
- Safekeeping of data media before and after dispatch
- Adequate labeling of data media for dispatch
- Secure packaging of data media
- Controlling the exchange of data media
- Physical deletion of data media before and after usage
- Use of a virus scanning program when exchanging of data media and data transmission
- Using encryption, checksums or digital signatures
- Pre-dispatch verification of the data to be transferred
- Checking of incoming data for macro viruses

Incident Handling

- Establishment of a management system for handling security incidents
- Specification of responsibilities for dealing with security incidents

- Procedural rules and reporting channels for security incidents
- Escalation strategy for security incidents
- Specifying priorities for handling security incidents
- Investigation and assessment of a security incident
- Remedial action in connection with security incidents
- Notification of parties affected
- Evaluation of security incidents
- Use of detection measures for security incidents
- Testing the effectiveness of the management system for the handling of security incidents

7. System Access Control

- Access control
- Business requirement for access control
- User access management
- User responsibilities
- Network access control

Firewall

- Selecting the communications requirements
- Selection of Services
- Establishing and implementation of filter rules
- Regular checks
- Adaptation to changes and tests
- Logging of firewall activities
- Contingency planning for the firewall
- Data backup

Intrusion Detection System

- Selecting the requirements – host / network based
- Selection of Services
- Establishing and implementation of detection rules
- Action on detection of exploits
- Regular checks
- Adaptation to changes and tests
- Logging of activities on IDS
- Checking of IDS logs for detecting attacks

- Action on security alerts
- Contingency planning for the IDS
- Data backup

Remote Access

- Resource management
- Documentation on the system configuration
- Performing a RAS requirements analysis
- Development of a RAS concept
- Selection of a suitable RAS system architecture
- Selection of a suitable RAS product
- Definition of a set of RAS security guidelines
- Use of an authentication server within RAS access
- Use of encryption procedures for network communications
- Use of suitable tunnel protocols for RAS communication
- Creation of a contingency plan for failure of the RAS system

- Operating system access control
- Application access control
- Monitoring system access and use
- Mobile computing and teleworking

8. Systems Development and Maintenance

- Systems development and maintenance
- Security requirements of systems; Issues relating to
  - Access
  - User Roles
  - Logging and security
  - Contingency Planning
  - Survey of the software held
  - Documentation on the system configuration
  - Designation of an administrator and his deputy
  - Provisions governing the designation of users and of user groups
  - Documentation on authorised users and on rights profiles
  - Establishment of a restricted user environment
  - Division of administrator roles under Unix
  - Access to the system
  - Allocation of attributes
- Security in application systems:

- Identify applications such as e-mail, web, databases etc
- Determination of a security policy for the application
- Use of a virus scanning program when exchanging of data media and data transmission
- Using encryption, checksums or digital signatures
- Checking of incoming data for macro viruses
- Use of a time stamp service
- Secure operation of servers
- Selection of a suitable Internet service provider
- Verification of data before transmission / elimination of residual information
- Documentation on the system configuration
- Documentation on authorised users and on rights profiles
- Change management procedures
- Documentation on changes made to an existing IT system
- Drawing up a requirements catalogue for standard software
- Ensuring the integrity of databases
- Password protection
- Regular data backup
- Procedures in case of a loss of database integrity
- Data backup in a database
- Archiving database
- Restoring a database
- Security of system files
- Security in development and support processes

Cryptographic controls

- Determining the need to use cryptographic procedures and products
- Selection of a suitable cryptographic procedure
- Selection of a suitable cryptographic product

- Obtaining information on security weaknesses of the system
- Response to violations of security policies
- Documentation of usage of Public Key Infrastructure and/or Symmetric Key Cryptography (external and internal)
- Encryption keys (Organisational/Departmental/Individual) – measures for BCP
- Appropriate key management – protection of private key for PKI
- Design of suitable interfaces for crypto modules Secure separation of roles and configuration with crypto modules
- Physical security of crypto modules
- Operating system security requirements when using crypto modules

9. Business Continuity Planning

- Business continuity management
- Business continuity management process
- Definition of "emergency", person-in-charge in an "emergency"
- Development of an Emergency Procedure Manual
- Study of internally and externally available alternatives
- Responsibilities in an emergency
- Alert plan
- Contingency plans for selected incidents
- Development of a post-incident recovery plan
- Development of a data backup plan
- Procurement of a suitable data backup system
- Development of a data backup policy
- Stipulating data backup procedures
- Training data reconstruction
- Taking out insurance
- Redundant communication links
- Emergency preparedness exercises
- Implementing planned measures after an emergency situation arises

10. Compliance

- Compliance

- Compliance with legal requirements
- Reviews of security policy and technical compliance
- System audit considerations

11. References

- BS7799 Code of Practice for Information Security Management
  www.dti.gov.uk/cii/bs7799
- ISO 17799 A code of practice for Information Security Management
- IT Baseline Protection Manual of BSI Germany
  www.bsi.bund.de/gshb/english/menue.htm
- "European Orange Book" ITSEC Information Technology Security Evaluation Criteria
  www.itsec.gov.uk/docs /introgds.htm
- Common Criteria
  www.radium.ne.sc.mil/tpep
- SANS Sample Policy Templates
  www.sans.org.resources/policies/
- Site Security Handbook RFC 2196 from IETF
- Different security related documents at NIST
  http://csrc.nist.gov
- Security Recommendation Guides
  http://nsa1.www.conxion.com