HPOL#13
Internet and Electronic Mail Security

(Version 1.0)

Table of Contents

13.1. SCOPE AND OBJECTIVES

The government organization should utilise the Internet as an important resource for information and knowledge to carry on the functions of the organization more efficiently. Towards this direction, the government organization should develop systems and procedures to ensure that the Internet is used only for organizational purposes in a secure manner, within a uniform code of conduct.

The government organization should develop effective systems and procedures to ensure that Electronic mails (E-mails) are used as an efficient mode of business communication and implement control procedures so that the E-mail facility is not misused. The government organization should ensure that E-mail services and operations remain secure and efficient while communicating within the intranet as well as through the Internet.

The purpose of the policy is to minimize risk associated with Internet and E-mail services, and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

13.2. POLICY STATEMENT

13.2.1. INTERNET SECURITY POLICIES

13.2.1.1. Reliance on Information Downloaded from the Internet

13.2.1.1.1. Information taken from the Internet must not be relied on until confirmed by separate information from another source.

13.2.1.2. Release of Information over the Internet

13.2.1.2.1. Users must not release any government organization information over the Internet.

Explanatory Notes

Further, users must not place government organization material (software, internal memos, etc.) on any publicly accessible Internet computer.

13.2.1.2.2. Web page content and page layout must be in accordance with specific government organization directives.

13.2.1.3. Information Protection

13.2.1.3.1. The government organization's sensitive and confidential information must never be sent over the Internet unless it has first been encrypted by approved methods.

13.2.1.3.2. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

13.2.1.3.3. Parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form.

Explanatory Notes

Parameters that can be used to gain access to goods or services include but is not limited to credit card numbers, telephone calling card numbers, and login passwords. An encryption algorithm approved by the government organization must be used to protect these parameters as they traverse the Internet.

13.2.1.4. Reporting Security Problems

13.2.1.4.1. Each user has the responsibility to notify designated management personnel immediately of any evidence of security violation involving Internet connectivity.

Explanatory Notes

Evidence of security violations involving Internet connectivity would include but not be limited to:

- *Unauthorized access to network, telecommunications, or computer systems;*
- *Apparent transmittal of a virus or worm via networking technologies; and*
- *Apparent tampering with any file for which the user established restrictive discretionary access controls.*

13.2.1.5. Expectation of Privacy

13.2.1.5.1. Users of the government organization's information assets and/or the Internet must not send private information over the Internet, unless it is encrypted.

13.2.1.5.2. At any time and without prior notice, the government organization reserves the right to examine E-mail, personal file directories, and other information stored on government organization computers.

Explanatory Notes

This examination assures compliance with government organization policies, supports the performance of internal investigations, and assists with the management of government organization information systems.

13.2.1.6. Resource Utilization

13.2.1.6.1. Use of Internet services will be limited to government organization related activities; users must not utilize the government organization's limited network resources for other purposes.

13.2.1.7. Public Representations

13.2.1.7.1. Government organization employees, personnel, or third party contractors using government organization facilities must not indicate their affiliation with the government organization.

Explanatory Notes

Possible avenues for indicating affiliation with the government organization will include but not be limited to bulletin board discussions and chat sessions.

13.2.1.7.2. Government organization employees, personnel, or third party contractors using government organization facilities must not publicly disclose internal government organization information via the Internet.

Explanatory Notes

Public disclosure of internal government organization information via the Internet may adversely affect the government organization, the government organization's citizen relations, and its public image.

13.2.1.7.3. Users must not post network or server configuration information about any government organization information systems to public newsgroups or mailing lists.

Explanatory Notes

Network or server configuration information includes but is not limited to internal machine addresses, server names, server types, and software version numbers.

13.2.1.7.4. Users must ensure that postings on to mailing lists, public news groups and related websites do not reveal details of

the government organization's internal functioning, infrastructure or potential vulnerabilities in the government organization's Information Security infrastructure.

13.2.1.7.5. All users wishing to establish a trusted connection with the government organization must authenticate themselves at the firewall before gaining access to the government organization's internal network.

13.2.1.7.6. Only authorized government organization personnel, or third party contractors may establish Internet or other external network connections.

13.2.1.8. Configuration Management

13.2.1.8.1. All configuration details of Internet connectivity network architecture must be completely documented and maintained.

Explanatory Notes

Configuration details would include but not be limited to hardware devices / components, operating system and application software, firmware components, physical and logical network addresses, and connecting circuit numbers.

13.2.2. INTERNET USAGE

13.2.2.1. User Authorization and Verification

13.2.2.1.1. Each person who has log-in access to the Internet connection must have a unique user ID and password.

13.2.2.2. Password Access Requirements

13.2.2.2.1. The password must meet the government organization's password requirements as described in the Logical Access Control Policy.

13.2.2.3. Viruses and Malicious Software Protection

13.2.2.3.1. Viruses and malicious software protection shall be governed by the "Virus and Malicious Software Protection" Policy.

Explanatory Notes

Users are not allowed to run programs obtained from external sources (via the WWW or other non-trusted source) without prior permission from designated personnel of the government organization and virus protection checks.

Users should never download files directly into a network server or production machine. Downloads should be directed to a separated (isolated) environment or removable storage media. Moves to the production machine (or equivalent) can only be performed with documented approval from designated personnel of the government organization.

13.2.2.4. Confidentiality

13.2.2.4.1. No sensitive information must be transmitted over the Internet and the World Wide Web (for example through Web based E-mail systems) without first being encrypted.

13.2.2.5. Internet User Guidelines

13.2.2.5.1. Internet Acceptable User Guidelines shall be distributed to each Internet user upon the assignment of their Internet account. Each user shall acknowledge receipt and that he/she understands the Guidelines.

13.2.2.6. Review of Logs

13.2.2.6.1. Routine logs of Web sites visited, files downloaded, time spent on the Internet, and related information must be maintained and reviewed on a periodic basis by designated personnel of the government organization.

Explanatory Notes

Unusual activities should be investigated and appropriate follow-up action taken.

13.2.3. INTERNET NETWORK SERVICES

13.2.3.1. File Transfer Protocol (FTP)

13.2.3.1.1. Only users that have a business need to use FTP will be authorized to use FTP.

13.2.3.1.2. No inbound FTP will be allowed under any circumstances from the Internet to the firewall or internal Local Area Network (LAN).

13.2.3.1.3. Outbound FTP will be allowed only via proxy accounts on the firewall system.

13.2.3.1.4. Users will not use FTP services to any remote host machine on which they do not have accounts.

Explanatory Notes

This does not apply to sites that offer or advertise an anonymous FTP service.

13.2.3.1.5. All files that are downloaded via FTP must undergo a virus check on a machine which is not directly connected to the Internet or the internal network.

13.2.3.2. Telnet Services

13.2.3.2.1. No inbound Telnet access from the Internet will be allowed.

13.2.3.2.2. All outbound Telnet access will be from a proxy account on the firewall.

13.2.3.2.3. All authorized Telnet sessions will be logged.

13.2.3.2.4. Users will not Telnet into ports other than the standard Telnet port.

Explanatory Notes

Telnets into ports designated for mail, FTP or WWW or other Internet services are strictly forbidden.

13.2.3.3. Network News

13.2.3.3.1. Inbound News feeds must be by subscription to selected newsgroups for designated user IDs.

13.2.3.3.2. No posting to news groups will be allowed from the government organization networks.

13.2.4. GENERAL E-MAIL POLICY

13.2.4.1. E-mail Usage

13.2.4.1.1. E-mail usage shall be governed by the "Internet and Electronic Mail Security" Policy.

Explanatory Notes

The government organization provides electronic information and communications systems to facilitate the organization's business needs and interests. These systems include individual computers, the computer network, E-mail, voice mail, and access to the Internet (collectively, the "Systems").

The usage of the E-mail system is subject to the following:

- *E-mail must be used in compliance with the government organization's Security Policies and associated procedures, standards, and guidelines.*
- *All access to electronic messages must be limited to properly authorized personnel.*
- *Personal or non-business use of the Systems is not permitted.*

13.2.4.1.2. All E-Mail must be in compliance with the government organization's standards regarding decency and appropriate content.

Explanatory Notes

Message content restrictions include:

- *The government organization's information resources should not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.*

- *The Systems should not be used to communicate statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be construed as harassing, offensive, or insulting to others based on race, religion, national origin, colour, marital status, citizenship status, age, disability, or physical appearance.*

- *Any statements or comments made via E-mail that could in any way be construed as an action of the government organization must bear a disclaimer such as "These statements are solely my own opinion, and do not necessarily reflect the views of my employer." Even with this disclaimer, all practices regarding decency and appropriate conduct still apply.*

13.2.4.1.3. Any use of E-mail from the network is easily traceable to the government organization. Personnel must thus conduct their activities with the reputation of the government organization in mind.

Explanatory Notes

Staff must exercise the same care in drafting E-mail, as they would for any other written communication that bears the government organization name.

13.2.4.1.4. The government organization E-mail systems should not be used to produce or distribute "chain mail," operate a business, or make solicitations for personal gain, political or religious causes, or outside organizations.

Explanatory Notes

Users must not forward or otherwise propagate, to individuals or groups, chain letters or any other types of data that may unnecessarily consume system resources or otherwise interfere with the work of others.

13.2.4.1.5. To maintain the security of the government organization's E-mail system, it is important to control access to the system.

Explanatory Notes

Users should not provide other unauthorized persons with their E-mail ID and personal password.

13.2.4.1.6. Users must utilize only their own government organization official E-mail account and must not allow anyone else access to their account.

Explanatory Notes

Impersonation is not permitted. Users must identify themselves by their real name; pseudonyms that are not readily attributable to actual users must not be allowed. Users must not represent themselves as another user. Each user must take precautions to prevent unauthorized use of the E-Mail account. Forging of header information in E-Mails (including source address, destination address, and timestamps) is not permitted.

13.2.4.1.7. Users must not publish or distribute internal mailing lists to non-staff members.

13.2.4.1.8. The government organization Systems should not be used to transmit or receive trade secrets, copyrighted materials, or proprietary or confidential information.

13.2.4.1.9. Confidential information must not be communicated through E-mail.

Explanatory Notes

Confidential information includes but is not limited to legal or contractual agreements, and technical information related to the government organization's operations or security.

13.2.4.1.10. Users must not post network or server configuration information about any government organization machines to public newsgroups or mailing lists.

Explanatory Notes

Network or server configuration information includes but is not limited to internal machine addresses, server names, server types, and software version numbers.

13.2.4.1.11. Under no circumstances is information received through unsecured E-mail to be considered private or secure.

Explanatory Notes

Clear text information in transit may be vulnerable to interception. Secure communication through E-mail can be ensured only by using encryption and digital signatures.

13.2.4.1.12. Attachments from unknown or untrusted sources must not be opened.

Explanatory Notes

All E-mail attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any government organization computer system. Personnel must perform a virus scan on all material that is transmitted to other users via E-mail prior to sending it.

13.2.4.1.13. Users must not send unsolicited bulk mail messages (also known as "junk mail" or "spam").

Explanatory Notes

This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-mail, including but not limited to "mail bombing," is prohibited.

13.2.4.1.14. Users must not execute any programs that are received via E-mail.

Explanatory Notes

Users must not install any upgrades or patches received via E-mail.

13.2.4.1.15. The Systems and all information contained in the systems are the government organization's property.

Explanatory Notes

Information contained in the systems includes but is not limited to computer files, E-mail and voice mail messages, and Internet access logs. At any time, with or without notice, this information may be monitored, searched, reviewed, disclosed, or intercepted by the government organization for any legitimate purpose, including but not limited to the following:

- *To monitor performance;*
- *Ensure compliance with government organization policies;*
- *Prevent misuse of the Systems;*
- *Troubleshoot hardware and software problems;*
- *Comply with legal and regulatory requests for information; and*
- *Investigate disclosure of confidential business, proprietary information, or conduct that may be illegal or adversely affect the government organization or its associates.*

The government organization may also gain access to communications deleted from the Systems.

13.2.4.2. E-mail Security Systems

13.2.4.2.1. The government organization employees, personnel, or third party contractors using the government organization facilities should not modify the security parameters within the government organization E-mail system.

13.2.4.3. E-mail Retention

13.2.4.3.1. Information on the government organization's E-mail system must be backed up and should be available for recovery for a predetermined number of days.

Explanatory Notes

Information on the government organization's E-mail system includes but is not limited to mail messages and attachments.

13.2.4.3.2. The destruction of both the logs and the referenced E-mail messages must be postponed whenever a legal notice is received. Such destruction must also be postponed if the material might be required for an imminent legal action.

13.2.4.4. Monitoring of E-mail

13.2.4.4.1. The government organization should periodically review the Security logs generated by the E-mail Systems.

Explanatory Notes

Unusual entries should be investigated and appropriate follow-up action taken.

13.2.4.5. E-mail Attachments

13.2.4.5.1. All attachments to mails must be limited and compressed using file compression utilities, before sending them.

13.2.4.5.2. Attachments greater than a predefined number or mega bytes should be restricted by external gateways.

Explanatory Notes

Non-business related E-mail containing large file attachments, such as graphics and multimedia files, should not be sent via the government organization's E-mail systems. A feature of E-mail is the ability to send and receive attachments. However, sending large attachments causes mail servers and gateways to external services (such as the Internet) to run slower and can cause significant delay in the delivery of E-mail. To prevent the degradation of the government organization's E-mail systems,

employees should limit the transmission of large attachments.

13.2.4.6. Automatic Forwarding of E-mail

13.2.4.6.1. Users should not automatically forward their E-mails to any address outside the government organization networks.

Explanatory Notes

Automatic forwarding of e-mails within the government organization for business purposes, may be allowed with the prior approval of designated personnel of the government organization.

13.2.5. FIREWALL CONFIGURATION

13.2.5.1. Firewall Policy

13.2.5.1.1. The government organization's firewalls will be configured in accordance with the government organization's Firewall Configuration Standards and Procedures document.

Explanatory Notes

The following must be complied with during configuration of the government organization's Internet firewalls:

- *All non-essential networking or system services must be eliminated or removed from the firewall.*
- *The system logs generated from the firewall must be reviewed on a continuing basis to detect any unauthorized entry attempts.*
- *All unauthorized access through the firewall must be reported to designated personnel of the government organization.*
- *Proxy accounts must be used on the firewall at all times.*

- *Networking traffic will be subject to filtering based on current security requirements.*

13.2.6. LEGAL

13.2.6.1. Legal Compliance

13.2.6.1.1. The government organization must be in compliance with all applicable laws regarding electronic commerce and the Internet.

13.2.7. WORLD WIDE WEB (WWW) POLICY

13.2.7.1. Security Administration of Web Pages

13.2.7.1.1. Responsibility for the security administration of the government organization's World Wide Web presence will be borne by designated personnel of the government organization. In cases where the government organization's World Wide Web presence is hosted by a third party, the host site must adhere to the policies defined in this document.

Explanatory Notes

The government organization's World Wide Web presence represents a growth opportunity, but also imposes threats to system security. Distributed computing and client/server architecture requires World Wide Web security to be applied at various levels of the government organization's systems and network resources.

13.2.7.1.2. The government organization's WWW resources shall be physically secured and appropriately configured.

Explanatory Notes

The objective of physically securing and appropriately configuring the government organization's WWW resources is to provide:

- *Access level security*
- *Secure hardening of operating systems*
- *Load balancing and high availability*

- *Secure network architecture (Perimeter security, Firewall, Intrusion Detection System, De-Militarized Zone, etc.)*

- *Associated application and database security*

13.2.7.2. Content

13.2.7.2.1. Web applications and content that is placed on the government organization Web server or servers must be approved by designated personnel of the government organization.

13.2.8. PROPRIETARY INFORMATION

13.2.8.1. Copyright Clearance

13.2.8.1.1. No proprietary material obtained via the World Wide Web shall be used by the government organization without the proper copyright clearance.

Explanatory Notes

Clearance should be obtained from the author or copyright owner. Most programs provide information on copyright issues on their documentation (disclaimers) or installation instructions.