Sample Internet and Email Security Policy

GUARDIAN NETWORK SOLUTIONS - DOCUMENT CENTER

by: Cody Faldyn

Purpose

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.

Scope

This policy applies to all users of information assets including <Organization-Name> employees, employees of temporary employment agencies, vendors, business partners, and contractor personnel and functional units regardless of geographic location.

This Policy covers all Information Systems environments operated by <Organization-Name> or contracted with a third party by <Organization-Name>. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, software, and information.

Although this Policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other <Organization-Name> Information Security policies, standards, and procedures define additional responsibilities. All users are required to read, understand and comply with the other Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he should consult with his systems administrator, business or functional manager, or human resources department, as applicable, who will contact the Information Security Department.

The Information Security Department shall resolve any conflicts arising from this Policy.

Responsibilities

- The sponsor of this policy is the Information Security ;Manager.
- The Security department is responsible for maintenance and accuracy of the policy.
- Any questions regarding this policy should be directed to the Security Department.

Definitions

Definition of some of the common terms:**Accountability:** The guarantee that an action can be linked to an identified subject and that this subject is made accountable for all selected actions.

Authentication: The identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system and can be associated with an individual’s authorization and system activities.

Availability: Ensuring that authorized users have access to information and associated assets when required.

Confidentiality: Ensuring that information is accessible only to those authorized to have access.

Privacy: Information provided by employees, customers and others is protected such that it is used solely for the stated purposes of the enterprise’s customer privacy policies, the provider has authorized such use, and its use is in compliance with all local government privacy regulations.

Private Information: Information classification that relates to their “privacy” type. This could be either customer related information or private information related to staff (like medical records).

Sensitive: concerned with highly classified information or involving discretionary authority over important official matters.

Sensitive Information: Information requiring some protection, not generally available internally. Security requirements include single-factor authentication (logon ID and password), authorization required on an “as needed” basis, and a mandated 128-bit encrypted work session using Secure Sockets Layer (SSL) and a minimum web browser version requirement or equivalent.

Policy Statement

The new resources, services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes <Organization-Name>'s official practices regarding Internet and Electronic Mail (EMail) security.

Internet Security Policies

Reliance on Information Downloaded from the Internet

Information taken from the Internet must not be relied on until confirmed by separate information from another source.**Description**
There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Unless tools and solutions like Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP), and Public Key Infrastructures (PKI – certificate authority based solutions) are used, it is also relatively easy to spoof another user on the Internet.

Release of <Organization-Name> Information over the Internet Users must not release any <Organization-Name> information over the Internet. Further, users must not place <Organization-Name> material (software, internal memos, etc.) on any publicly accessible Internet computer.

Web page content must be in accordance with specific company directives, and the page layout must follow the policies/guidelines defined.

Information Protection

<Organization-Name>'s sensitive and confidential information must never be sent over the Internet unless it has first been encrypted by approved methods.

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

Credit card numbers, telephone calling card numbers, log-in passwords, and other parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form.

Reporting Security Problems

Each user has the responsibility to notify the Information Security Department immediately of any evidence of any security violation involving Internet connectivity with regard 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.

Expectation of Privacy

Users of <Organization-Name>'s information assets and/or the Internet must not send private information over the Internet, unless it is encrypted.

At any time and without prior notice, <Organization-Name> authorized team reserves the right to examine E-Mail, personal file directories, and other information stored on <Organization-Name> computers.**Description**
This examination assures compliance with company policies, supports the performance of internal investigations, and assists with the management of <Organization-Name> information systems.

Resource Utilization

Use of Internet services will be limited to company-related activities; users must not utilize the company’s limited network resources for other purposes rather than company related activities.

Public Representations

<Organization-Name> employees, personnel, or third party contractors using <Organization-Name> facilities must not indicate their affiliation with <Organization-Name> in bulletin board discussions, chat sessions, and other offerings on the Internet. Only the Corporate Communication may speak about or produce a news announcement.

<Organization-Name> employees, personnel, or third party contractors using <Organization-Name> facilities must not publicly disclose internal <Organization-Name> information via the Internet that may adversely affect <Organization-Name>, <Organization-Name>’s customer relations, or public image.

Users must not post network or server configuration information about any <Organization-Name> information systems to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

Users must ensure that postings on to mailing lists, public news groups and related websites do not reveal details of <Organization-Name>’s internal functioning, infrastructure or potential vulnerabilities in <Organization-Name>’s Information Security infrastructure.

All users wishing to establish a trusted connection with <Organization-Name> must authenticate themselves at the firewall before gaining access to <Organization-Name> internal network.

Only authorized <Organization-Name> personnel, or third party contractors may establish Internet or other external network connections. These connections include the establishment of multi-computer file systems.

Configuration Management

All configuration details (All hardware devices/components, all operating system and application software, all firmware components, physical and logical network addresses, and connecting circuit numbers) of Internet connectivity network architecture must be completely documented and maintained.

Periodic Review of Authorized Accounts

The security administrator must periodically reconfirm the validity of all log-ins and electronic mail alias authorizations. The period between reconfirmation must not exceed six months.

Audit and Accountability of Internet Connections

The Security Audit Team must review the Internet connection audit reports created on the firewall for any suspicious activities against two or more connections. The period between reviews must not exceed one (1) month. Reports of the findings must be given to the Information Security Manager.

Internet Usage

Password Access Requirements

The password must meet <Organization-Name> password requirements as described in the Password Policy. The user must comply with the most restrictive of the password formats specified.

User Authorization & Verification

Each person who has log-in access to the Internet connection must have a unique User ID.

Requesting and Granting User Authorization

Each personnel requesting a User ID must provide a written authorization from the head of his business unit.

Requests for an Internet connection must be accompanied by a justification for such access. The request must be authorized by the Users Manager.

An associate that requires only the inclusion of an electronic mail alias entry must establish authorization in the same manner as that described for a login user.

Viruses and Malicious Software Protection

Users are not allowed to run programs obtained from external sources (via the WWW or other non-trusted source) without prior permission from Information Security Department 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. Upon successful completion of the procedures described on the previous paragraph, users might move the downloaded files to their working directories. Moves to production machine (or equivalent) can only be performed with documented approval from Machine Owner.

Confidentiality

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.

Internet User Guidelines

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 understands the Guidelines.

Usage of circumvention methods for purposefully bypassing the monitoring or filtering processes and any effort on such direction is prohibited.

Internet Networking Services

The following Policies will apply to Internet services:

File Transfer Protocol (FTP)

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

No inbound FTP will be allowed under any circumstances from the Internet to the firewall or internal LAN.

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

Users will not use FTP services to any remote host machine on which they do not have accounts. This does not apply to sites that offer or advertise an anonymous FTP service.

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.

Telnet Services

No inbound Telnet access from the Internet will be allowed.

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

All authorized Telnet sessions will be logged.

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

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

Network News

Inbound News feeds must be by subscription to only selected newsgroups for selected User IDs.

No posting to news groups will be allowed from <Organization-Name> Networks.

General E-Mail Policy

<Organization-Name> provides electronic information and communications systems to facilitate the companies' business needs and interests. These systems include individual computers, the computer network, electronic mail ("E-Mail"), voice mail, and access to the Internet (collectively, the "Systems").

E-Mail Usage

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

- E-Mail must be used in compliance with the Corporate Security Policy and associated Supplementary Information Security Policies. All access to electronic messages must be limited to properly authorized personnel.
- Usage of E-mail system is limited to business needs or any helpful messages.

All E-Mails must be in compliance with <Organization-Name> standards regarding decency and appropriate content. Message content restrictions include: -

- <Organization-Name> 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, color, 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 <Organization-Name> 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.

Any use of E-Mail from the network is easily traceable to <Organization-Name>. Personnel must conduct these activities with the reputation of <Organization-Name> in mind. Staff must exercise the same care in drafting E-Mail, as they would for any other written communication that bears <Organization-Name> name.

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

To maintain the security of <Organization-Name>'s E-Mail system, it is important to control access to the system. Users should not provide other unauthorized persons with their E-Mail ID and personal password.

Users must use only their own <Organization-Name> official E-Mail account and must not allow anyone else access to their account. 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-Mail (including source address, destination address, and timestamps) is not permitted.

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

<Organization-Name> Systems should not be used to transmit or receive trade secrets, copyrighted materials, or proprietary or confidential information unless it is digitally signed and encrypted.

Any information regarded as confidential including legal or contractual agreements, technical information related to <Organization-Name>'s operations or security etc. must not be communicated through E-Mail unless it is digitally signed and encrypted.

Users must not post network or server configuration information about any <Organization-Name> machines to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, software version numbers, etc.

Under no circumstances is information received through unsecured Email to be considered private or secure.**Description**
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.

Attachments from unknown or untrusted sources must not be opened. 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 <Organization-Name> computer system. Personnel must perform a virus scan on all material that is transmitted to other users via E-Mail prior to sending it.

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

Users must not execute or install any programs, upgrades or patches that are received via E-Mail or download from the Internet unless the Information Security Department approves it.

The Systems and all information contained in the systems (including computer files, E-Mail and voice mail messages, Internet access logs, etc.) are <Organization-Name>'s property. At any time, with or without notice, this information may be monitored, searched, reviewed, disclosed, or intercepted by <Organization-Name> for any legitimate purpose, including the following:

- To monitor performance,
- Ensure compliance with <Organization-Name> 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 <Organization-Name> or its associates.

<Organization-Name> may also gain access to communications deleted from the Systems.

All distributed lists Emails should not include an active link to an Internet website unless approved by Information Security Department.

All distributed Lists Emails must contain contact information for the receivers in case they want to ask questions or discuss any issues regarding the Email.

E-Mail Security Settings

<Organization-Name> employees, personnel, or third party contractors using <Organization-Name> facilities should not modify the security parameters within <Organization-Name> E-Mail system. Users making unauthorized changes to the E-Mail security parameters are in violation of this policy.

E-Mail Retention

Information (mail messages and attachments) on <Organization-Name>'s Email system must be backed up and should be available for recovery for a period of 7 days.

E-Mail Attachments

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

Attachments greater than 3MB are restricted by external gateways. Non-business related E-Mail containing large file attachments, such as graphics and multimedia files, should not be sent via <Organization-Name>'s E-Mail systems.

Firewall Configuration

Firewall Policy

<Organization-Name>'s Firewalls will be configured in accordance with <Organization-Name>'s Firewall Configuration Standards and Procedures document. The following high-level policies must be complied with during configuration of <Organization-Name>'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 the security manager and network administrator.
- Proxy accounts must be used on the firewall at all times.
- Networking traffic will be subject to filtering based on current security requirements.

Legal

<Organization-Name> must be in compliance with all existing laws of the country regarding electronic commerce and the Internet.

World Wide Web Policy (WWW)

<Organization-Name> World-Wide Web presence represents a growth opportunity, but also imposes some threats to system security. Distributed computing and client-server architecture requires World-Wide Web security to be applied at various levels of <Organization-Name> systems and network resources.

Security Administration of <Organization-Name>'s Web Pages Responsibility for the security administration of <Organization-Name>'s World-Wide Web presence will be borne by the e-Business. In cases where <Organization-Name>'s World-Wide Web (WWW) presence is hosted by a third party, the host site must adhere to the policies defined in this document as well.

<Organization-Name>'s WWW resources shall be physically secured and appropriately configured to provide:-

- Access level security
- Secure hardening of operating systems
- Load balancing and high availability
- Secure network architecture (Perimeter security, Firewall, IDS, DMZ, etc.)
- Associated application and database security

Content

Web applications and content that is placed on <Organization-Name> Web server or servers must be approved by the designated <Organization-Name> management.

Proprietary information

Copyright Clearance

No proprietary material obtained via the World-Wide Web shall be used company-wide without the proper copyright clearance.

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

Compliance Measurement

Compliance with Internet Email Security Policy is mandatory. <Organization-Name> managers must ensure continuous compliance monitoring within their organizations. Compliance with Internet Email Security Policy will be a matter for periodic review by Information Security Audit team as per the audit guidelines and procedures mentioned in Security Control Framework and the Security Auditing Guidelines. Compliance measurement should also include periodic review for Security Quality Assurance. Violations of the policies, standards, and procedures of <Organization-Name> will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

Waiver Criteria

This Policy is intended to address information security requirements. Requested waivers must be formally submitted to the Information Security Department, including justification and benefits attributed to the waiver, and must be approved by the Information Security Manager. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time. At the completion of the time period the need for the waiver should be reassessed and re-approved, if necessary. No policy should be provided waiver for more than three consecutive terms.

The waiver should be monitored to ensure its concurrence with the specified period of time and exception.

All exceptions to this policy must be communicated through the Policy Waiver Request Form.