



## **Internet usage Policy**

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to [policy-resources@sans.org](mailto:policy-resources@sans.org).*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

**Last Update Status:** *Retired*

### **1. Overview**

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

### **2. Purpose**

The purpose of this policy is to define the appropriate uses of the Internet by <Company Name> employees and affiliates.

### **3. Scope**

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

#### **3.1 Internet Services Allowed**



*Internet access is to be used for business purposes only.* Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
- Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.
- File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
- Telnet -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.

Management reserves the right to add or delete services as business needs change or conditions warrant.

***All other services will be considered unauthorized access to/from the Internet and will not be allowed.***

### 3.2 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

#### 3.2.1 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy. The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

#### 3.2.2 Approval

Internet access is requested by the user or user's manager submitting an ***IT Access Request*** form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

#### 3.2.3 Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and



only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

## 4. Policy

### 4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

### 4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information.
- Research

### 4.3 Personal Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is



not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

#### 4.4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:



- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.
- Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

#### 4.5 Software License

The company strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

#### 4.6 Review of Public Information

All publicly-writeable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with company business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.



### 4.7 Expectation of Privacy

#### 4.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

#### 4.7.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

### 4.8 Maintaining Corporate Image

#### 4.8.1 Representation

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.

#### 4.8.2 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee's manager and the public relations department and will be placed by an authorized individual.

#### 4.8.3 Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Corporate Communications Directors for initial approval to continue. All company pages are



owned by, and are the ultimate responsibility of, the Corporate Communications Directors.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

### 4.9 Periodic Reviews

#### 4.9.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

#### 4.9.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

## 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.

Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the Internet via company network is approved, the potential Internet user is required to read this Internet usage Policy and sign an acknowledgment form (located on the last page of this document). The signed acknowledgment form should be turned in and will be kept on file at the facility granting the access. For questions on the Internet usage Policy, contact the Information Technology (IT) Department.



## **6 Related Standards, Policies and Processes**

### **6. INTERNET USAGE COVERAGE ACKNOWLEDGMENT FORM**

After reading this policy, please sign the coverage form and submit it to your facility's IT department or granting facility's IT department for filing.

By signing below, the individual requesting Internet access through company computing resources hereby acknowledges receipt of and compliance with the Internet Usage Policy. Furthermore, the undersigned also acknowledges that he/she has read and understands this policy before signing this form.

Internet access will not be granted until this acknowledgment form is signed by the individual's manager. After completion, the form is filed in the individual's human resources file (for permanent employees), or in a folder specifically dedicated to Internet access (for contract workers, etc.), and maintained by the IT department. These acknowledgment forms are subject to internal audit.

#### **ACKNOWLEDGMENT**

I have read the *Internet Usage Policy*. I understand the contents, and I agree to comply with the said *Policy*.

Location (Location and address)

Business Purpose

Name

Signature \_\_\_\_\_ Date \_\_\_\_\_

Manager/Supervisor Signature \_\_\_\_\_ Date \_\_\_\_\_

## **7 Definitions and Terms**

None.





## 8 Revision History

<b>Date of Change</b>	<b>Responsible</b>	<b>Summary of Change</b>
Dec 2013	SANS Policy Team	Converted format and retired.