



Interested in learning
more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Acceptable Use Policy Document

This paper provides an example of an acceptable use policy for information resources.

Copyright SANS Institute
Author Retains Full Rights

AD

Veriato

Unmatched visibility into the computer
activity of employees and contractors



RAYMOND IANDOLO

ACCEPTABLE USE POLICY DOCUMENT

VERSION..... 1.0

ACCEPTABLE USE

POLICY..... 2

ROLES AND RESPONSIBILITIES..... 2

 Chief Privacy Officer..... 2

 Executive Sponsors..... 2

 All Managers..... 2

 System Administrators..... 2

 Chief Information Security Officer..... 2

 All Personnel..... 2

 Auditors..... 3

ENSURING COMPLIANCE 3

HARDWARE AND SOFTWARE 3

 Acquiring Hardware and Software 3

 Complying with Copyright and Licensing..... 4

 Using Personally-owned Software 4

 Protecting Intellectual Property..... 4

ELECTRONIC MAIL AND MESSAGING..... 4

 Acceptable Use 4

 Prohibited Use..... 4

 Encryption 5

 Authorized Monitoring..... 5

INTERNET 5

 Acceptable Use 5

 Prohibited Use..... 5

GENERALLY PROHIBITED USES OF INFORMATION RESOURCES..... 6

ACCEPTABLE USE

POLICY

Corporate information and information resources shall be used in an approved, ethical, and lawful manner to avoid loss or damage to Corporate operations, image, or financial interests and to comply with official acceptable use policies and procedures. Personnel shall contact the chief information security officer (CISO) prior to engaging in any activities not explicitly covered by these policies.

ROLES AND RESPONSIBILITIES

The roles and responsibilities for acceptable use are defined in the following sections and depicted in Exhibit 1.

CHIEF PRIVACY OFFICER

The chief privacy officer shall be responsible for developing policy on corporate privacy issues.

EXECUTIVE SPONSORS

Executive sponsors shall be responsible for the following:

- a) Informing personnel of corporate policies on acceptable use of information resources.
- b) Ensuring that application development personnel under their supervision comply with these policies and procedures.
- c) Ensuring that contract personnel under their supervision comply with these policies and procedures.

ALL MANAGERS

Managers at all levels shall be responsible for the following:

- a) Informing personnel of corporate policies on acceptable use of information resources.
- b) Ensuring that personnel under their supervision comply with these policies and procedures.

SYSTEM ADMINISTRATORS

System administrators shall be responsible for the following:

- a) Monitoring systems for misuse.
- b) Promptly reporting suspicion or occurrence of any unauthorized activity.

CHIEF INFORMATION SECURITY OFFICER

The chief information security officer (CISO) shall be responsible for the following:

- a) Developing acceptable use policy.
- b) Developing awareness and training materials.

ALL PERSONNEL

All personnel shall be responsible for the following:

- a) Abiding by official corporate policies on acceptable use of information resources.
- b) Promptly reporting suspicion or occurrence of any unauthorized activities.
- c) Any use made of their accounts, logon IDs, passwords, PINs, and tokens.

AUDITORS

Auditors shall be responsible for compliance auditing.

Exhibit 1, Acceptable Use Responsibilities

Activity	Executive Sponsors	All Managers	System Admins	CISO	All Personnel	Auditors
In form Users	X	X		X		A
Implement User Sanctions	X	X		C		A
Acquire Hardware and Software Properly	X	X		C		X/A
Comply with Copyright and Licensing	X	X	X	X	X	X/A
Comply with Personally-owned Software Policy	X	X	X	X	X	X/A
Protect Intellectual Property	X	X	X	X	X	X/A
Comply with Electronic Mail Policy	X	X	X	X	X	X/A
Comply with Electronic Mail Encryption Policy	X	X	X	X	X	X/A
Comply with Internet Policy	X	X	X	X	X	X/A
Comply with Information Resources Policy	X	X	X	X	X	X/A

X = Responsible for Accomplishment
C = Consulting Support as Required
A = Independent Compliance Auditing

ENSURING COMPLIANCE

The Corporation owns all Corporate information resources; use of such resources constitutes consent for the Corporation to monitor, inspect, audit, collect, and remove any information without permission or further notice. Personnel shall be trained in what use is acceptable and what is prohibited. Any infraction of corporate acceptable use policies shall constitute a security violation. Personnel shall be held personally accountable and may be subject to disciplinary action or criminal prosecution.

HARDWARE AND SOFTWARE

ACQUIRING HARDWARE AND SOFTWARE

To prevent the introduction of malicious code and protect the integrity of corporate information resources, all hardware and software shall be obtained from official corporate sources.

COMPLYING WITH COPYRIGHT AND LICENSING

All software used on corporate information resources shall be procured in accordance with official corporate policies and procedures, and shall be licensed, and registered in

the name of the corporation. All personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements.

USING PERSONALLY OWNED SOFTWARE

To protect the integrity of the corporate information resources, personnel shall not use personally owned software on corporate information resources. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally-owned or controlled software.

PROTECTING INTELLECTUAL PROPERTY

To ensure the integrity of corporate developed software, all personnel shall abide by the intellectual property protection contract provisions of the corporation.

ELECTRONIC MAIL AND MESSAGING

Access to the corporate electronic mail (email) system is provided to personnel whose duties require it for the conduct of corporate business. Since email may be monitored, all personnel using corporate resources for the transmission or receipt of email shall have no expectation of privacy.

ACCEPTABLE USE

The corporate provides email to facilitate the conduct of corporate business. Occasional and incidental personal email use shall be permitted if it does not interfere with the corporation's ability to perform its mission and meets the conditions outlined in official corporate directives. However, while they remain in the system, personal messages shall be considered to be in the possession and control of the corporation.

PROHIBITED USE

Prohibited activities when using corporate electronic mail shall include, but not be limited to, sending or arranging to receive the following:

- a) Information that violates state or federal laws, or corporate regulations.
- b) Unsolicited commercial announcements or advertising material, unless approved by management in advance.
- c) Any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the corporation, the recipient, the sender, or any other person.
- d) Pornographic, racist or offensive material, chain letters, unauthorized mass mailings, or malicious code.

ENCRYPTION

Encrypting electronic mail or messages shall comply with the following:

- a) Use encryption software and the methods approved by official corporate sources.
- b) Place the key or other similar file for all encrypted electronic mail in a directory or file system that can be accessed by management personnel prior to encrypting email.

- c) Supply the key or other device needed to decrypt the electronic mail upon request by authorized corporate management.

AUTHORIZED MONITORING

System administrators and other personnel with unrestricted access to email and similar services shall receive management approval prior to decrypting or reading the email traffic of other personnel. If management approval is not immediately available, then system administrators and other personnel that intercept, read, or restrict email accounts shall document their actions and provide that documentation to management personnel within twenty-four (24) hours.

INTERNET

Access to the Internet is available to employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of corporate business. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy.

ACCEPTABLE USE

The corporation provides Internet access to facilitate the conduct of corporate business. Occasional and incidental personal Internet use shall be permitted if it does not interfere with the work of personnel, the corporation's ability to perform its mission, and meets the conditions outlined in official corporate directives.

PROHIBITED USE

Prohibited activities when using the Internet include, but are not limited to, the following:

- a) Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the corporation has determined to be off-limits.
- b) Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material determined to be off-limits.
- c) Posting or sending sensitive information outside of the corporation without management authorization.
- d) Using other services available on the Internet, such as FTP or Telnet, on systems for which the user does not have an account, or on systems that have no guest or anonymous account for the service being used.
- e) Posting commercial announcements or advertising material.
- f) Promoting or maintaining a personal or private business.
- g) Receiving news feeds and push data updates, unless the material is required for corporate business.
- h) Using non-work related applications or software that occupy excess workstation or network processing time (e.g., processing in conjunction with screen savers).

GENERALLY PROHIBITED USES OF INFORMATION RESOURCES

Generally prohibited activities when using corporate information resources shall include, but are not limited to, the following:

- a) Stealing or copying of electronic files without permission.
- b) Violating copyright laws.
- c) Browsing the private files or accounts of others, except as provided by appropriate authority.

- d) Performing unofficial activities that may degrade the performance of systems, such as the playing of electronic games.
- e) Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.
- f) Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any corporate computer, network, or information.
- g) Accessing the corporate network via modem or other remote access service without the approval of corporate management.
- h) Bringing discredit to the corporation, its personnel or business partners.
- i) Promoting or maintaining a personal or private business, or using corporate information resources for personal gain.
- j) Using someone else's logon ID and password.
- k) Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any corporate or non-corporate computer.
- l) Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity.
- m) Disclosing any corporate information that is not otherwise public.
- n) Performing any act that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the corporation or any person.

REFERENCES:

GSA	Office of Government Wide Policy
CIO Council	Federal Information Security Assessment Framework
NIST	Publication 800-12
NASA	Procedure and Guidelines, Security of Information Technology

© SANS Institute 2003, Author retains full rights



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Amsterdam May 2018	OnlineNL	May 28, 2018 - Jun 02, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced