Sam Noble Museum

Privacy, Information Security and Confidentiality

Contents

1. State of Oklahoma Information Security Policy (pages 2-3)
2. Approved & Prohibited Software Applications Statement (page 4)
3. Computer user responsibilities (pages 5-7)
4. Policy Statement on Privacy, Information Security and Confidentiality (pages 8-9)
5. Verification Form; Initial for each section above and sign, return (page 10)

This document can be reviewed anytime, while on the museum network, via a web browser at:

http://intranet.snomnh.ou.edu/docs/security-confidentiality.pdf

1. State of Oklahoma Information Security Policy, Information and Guidelines

Information Security Policy

Information is a critical State asset. Information is comparable with other assets in that there is a cost in obtaining it and a value in using it. However, unlike many other assets, the value of reliable and accurate information appreciates over time as opposed to depreciating. Shared information is a powerful tool and loss or misuse can be costly, if not illegal. The intent of this Security Policy is to protect the information assets of the State.

This Security Policy governs all aspects of hardware, software, communications and information. It covers all State Agencies as well as contractors or other entities who may be given permission to log in, view or access State information.

Definitions:

Information includes any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

The Owner of the information is the State Agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

The Hosting State Agency has physical and operational control of the hardware, software, communications and data bases (files) of the owning Agency. The Hosting Agency can also be an Owner.

The confidentiality of all information created or hosted by a State Agency is the responsibility of that State Agency and its respective employees. Disclosure is governed by legislation, regulatory protections and rules as well as policies and procedures of the owning State Agency. The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

All information content is owned by the State Agency responsible for collecting and maintaining the authenticity, integrity and accuracy of the information. The objective of the owning State Agency is to protect the information from inadvertent or intentional damage, unauthorized disclosure or use according to the owning Agency's defined classification standards and procedural guidelines.

Information access is subject to legal restrictions and to the appropriate approval processes of the owning State Agency. The owning State Agency is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the State Agency hosting the information. The hosting State Agency has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning State Agencies in a timely manner.

Information security:

The State Agency Director whose agency collects and maintains (owns) the information is responsible for interpreting confidentiality restrictions imposed by laws and statutes, establishing information classification and approving information access. The hosting State Agency will staff a security function whose responsibility will be operational control and timely implementation of access privileges. This will include access authorization, termination of access privileges, monitoring of usage and audit of incidents. The State Agencies that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

Information availability is the responsibility of the hosting State Agency. Access to information will be granted as needed to all State Agencies to support their required processes, functions and timelines. Proven backup and recovery procedures for all data elements to cover the possible loss or corruption of system information are the responsibility of the hosting State Agency.

The hosting State Agency is responsible for securing strategic and operational control of its hardware, software and telecommunication facilities. Included in this mandate is the implementation of effective safeguards and firewalls to prevent unauthorized access to system processes and computing / telecommunication operational centers. Recovery plans are mandatory and will be periodically tested to ensure the continued availability of services in the event of loss to any of the facilities.

Development, control and communication of Information Security Policy, Procedures and Guidelines for the State of Oklahoma are the responsibility of the Office of State Finance. This Policy represents the minimum requirements for information security at all State Agencies. Individual agency standards for information security may be more specific than these state-wide requirements but shall in no case be less than the minimum requirements.

The entire Information Security Policy, Procedures, Guidelines can be accessed on the web at:
http://www.ok.gov/OSF/documents/StateOfOklahomaInfoSecPPG_osf_12012008.pdf

2. Approved and Prohibited Software

Approved Software

Software should be installed only by SNOMNH IT staff unless otherwise arranged. SNOMNH IT should be consulted and subsequently approve the addition of software for your computer(s).

Prohibited Software

Departmental policy prohibits the installation of spyware on university-owned computers. Spyware software is known to negatively impact campus computing in one or more of the following ways:

- Causes conflicts with work-related software
- Poses a potential security risk by opening unnecessary TCP/IP ports
- May cause computers to boot slowly or operate improperly.
- Violates privacy by sending user information to 3rd parties
- May cause increase of spam and pornographic materials via email
- May cause conflicts with vital operations such as printing
- Impacts system resources causing to act sluggish (memory, CPU)
- Conflicts with or may alter critical operating system files
- May cause the computer to crash often
- Creates unnecessary bandwidth limitation
- May increase presence of pop-ups
- Creates or increases vulnerability of entire network through source of propagation

SNOMNH IT will provide and assist with maintaining anti-spyware applications. If spyware is detected and you are not convinced of its removal/mitigation, IT should be contacted.

3. User Responsibilities

A. Proactive Computer Security

1. Windows XP Users (assumes OS: XP Service Pack 3/Windows 7)

As a user of a University-owned computer, it is important that you report any suspicious computer behavior/activity immediately to either SNOMNH IT, your supervisor, or if neither are available, the OU IT helpdesk at 325-4357. The sooner you report a problem (such as erratic behavior or a new toolbar or program that you did not intend to install), the less likely the problem will result in consequences for your PC or the University network.

A. Every time you start your computer it is important to recognize that you have adequate protection from internet threats. At a glance, you should confirm the following protective applications are running in your system tray (the area in the bottom, right corner of your screen):

Symantec EndPoint (anti-virus) protection

On a regular basis, usually monthly, Windows patches are released by Microsoft to better-protect your computer. If you see the following icon in your system tray you should click it and answer affirmatively any questions presented. This process will install updates that may or may not require you to reboot the computer.

Microsoft Updates protection

B. On a monthly basis you should verify that your Windows Firewall is active. To do this, go to Start—Control Panel—Security Center (W7 ->Firewall). The Windows Firewall should indicate that it is turned “ON.” If it is not and/or you need assistance, please contact SNOMNH IT.

Microsoft Security Center 

Windows 7 Firewall

2. Macintosh OS X Users (assumes OS: 10.4 – 10.6)

A. Every time you start your computer it is important to recognize that you have adequate protection from internet threats. With a few steps, you can quickly confirm the following protective applications are running on your system:

Near the top right of your screen you should see the Symantec Antivirus icon. Upon clicking it the second icon showing its status should show a yellow shield with a green check mark in it.

Symantec icon, and icon showing protection "on"

On a regular basis Mac OS patches are released by Apple to better-protect your computer. The frequency by which your computer checks for updates can be adjusted. Typical setting is for a weekly check. Included with this feature is a date stamp for your last update. A manual check can be run from here as well as setting up automatic checks. This process will install updates that may or may not require you to reboot the computer.

To check the status of your OS X updates, click the blue Apple icon at the top left corner of your screen and select System Preferences, then click Software Update.

Apple icon and software Update

B. On a regular basis you should verify that your OS X Firewall is active. To do this, go to the blue Apple icon at the top left corner of your screen and select System Preferences, then click Sharing. There will be a three-tab window; the second tab will allow you to check the status of or turn on your firewall. If it is not on and/or you need assistance, please contact SNOMNH IT.

Apple icon and Security Preferences

3. Passwords

In keeping with SNOMNH IT policy (Computer Use 1.15) users are reminded to change their passwords at least every 60 days.

B. Policy Compliance

OU IT policies can be accessed at http://www.ou.edu/committees/itc/policy/. Current policies include Information Systems Security, Acceptable Use of Information Resources, E-mail (including mass email) and Password Sharing. It is your responsibility to review and understand each policy as well as to check the policy website on a regular basis to keep-up-to date with any changes or additions.

4. Policy Statement on Privacy, Information Security and Confidentiality

The University of Oklahoma places a high priority on maintaining the confidentiality of its records, documents, and all other sensitive information.

In the course of your duties, you may be given access to confidential information about students, faculty, staff, and other individuals or events both on campus and in the surrounding community itself

By signing this statement, you acknowledge that your access to confidential information is for the purpose of performing your responsibilities for the University of Oklahoma and for no other purpose.

1. I will look at and use only the information I need to perform the duties of my job. I will not look at *confidential information* that I do not need to perform my job. I understand that the University of Oklahoma has the ability to determine whether I have followed this rule.

2. I understand that *confidential information* is not to be shared with anyone who does not have an official need to know. I will be especially careful not to share this information with others in casual conversation.

3. I have read and understand the individual student information release policy (FERPA), aka “Buckley Amendment” as printed on the most current class schedule from the Registration office http://www.ou.edu/admissions/home.html.

4. I will handle all records—both paper and electronic—with care to prevent unauthorized use or disclosure of *confidential information.* I understand that I am not permitted to remove *confidential information* from my work area without written permission from my supervisor. I also understand that I may not copy *confidential information* or remove them from the premises except in performing my job duties.

5. If I no longer need *confidential information,* I will dispose of it in a way that ensures that others will not see it. I recognize that the appropriate disposal method will depend upon the type of information in question.

6. Any passwords, verification codes, or electronic signature codes assigned to me are equivalent to my personal signature:

- They are intended for my use only
- I will not share them with anyone nor let anyone else use them
- I will not attempt to learn or use the passwords, verification codes, or electronic signature codes of others.
- They are complex (at least alphanumeric and not found in the dictionary) and should be changed every 60 days.

7. If I find that someone else has been using my passwords or codes, or if I learn that someone else is using passwords or codes improperly, I will immediately notify my management.

8. I understand that if I allow another person to use my codes, I will be held accountable and subject to appropriate action.

9. I will not abuse my rights to use my institution's computers, information systems, Intranet, and the Internet. They are intended to be used specifically in performing my assigned job responsibilities

10. I will not copy or download software prior to approval by SNOMNH IT staff.

11. I will handle all *confidential information* stored on a computer or downloaded to a storage media with care to prevent unauthorized access to, disclosure of, or loss of this information.

12. I understand that the *confidential information* and software I use for my job are not to be used for personal benefit or to benefit another unauthorized person or organization. I also understand that the University of Oklahoma may inspect the computers it owns, as well as personal PCs used for work, to ensure that its data and software are used according to its policies and procedures.

13. I understand I am not to turn off, remove or otherwise alter, without express consent:

- Antivirus Software
- Antispyware Software
- Computer security measures, e.g. screen locking and password protection

Sam Noble Museum

5. Verification Form; Initial for each section above and sign, return

Privacy, Information Security and Confidentiality

(Initial)

____ I have reviewed the State of Oklahoma Information Security Policy, Information and Guidelines.

____ I have read and understand the Approved & Prohibited Software statement.

____ I have read and understand the User Responsibilities. I will notify SNOMNH IT for help if I am unable to set or confirm the software settings listed above.

I hereby acknowledge that:

I understand the contents of this Policy Statement on Privacy, Information Security, and Confidentiality. I understand that if I do not follow these rules, I could receive disciplinary action, up to and including being dismissed from my position.

Name (Print): _____

Signature: _____

Today's Date: _____

Internal Department: _____

All individuals who use museum computers or have access to confidential information in the museum must read the document, complete this form (item 5) and return it to the HR/Payroll Staff Assistant.