

## **Secure Desktop and Laptop – Best Practice**

This document outlines the University of Tennessee best practices for securing desktop and laptop resources.

**FINAL DRAFT – 8/07/2007**

### **OVERVIEW**

The purpose of this Best Practice is to establish the required protection measures for desktop and laptop systems owned by the University of Tennessee or that connect to university information or information technology resources. Desktop and laptop systems, including virtual systems, will be referenced as workstations throughout this document. This best practice provides guidance for the creation and maintenance of secure end user workstations using both wired and wireless network technologies, but does not apply to servers. Refer to the *Secure Server Best Practice* for more information on securing servers.

This best practice applies to all students, faculty, staff, and others, referred to as “users” throughout this policy, while accessing, using, or handling the university’s IT resources. In this policy, “users” includes but is not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities that are granted access as defined in *Acceptable Use of Information Technology Resources Policy (IT0110)*.

### **Information and System Classification**

University faculty, staff, students, and others have a business need to collect, transmit, store, or process information. Protecting the confidentiality, integrity, and availability of this information, and the workstation it resides on, is the responsibility of the entire university.

The *Information Classification Policy (IT0115)* and *Computer System Classification Policy (IT0116)* formalize this responsibility, define a framework for categorizing information and computer systems according to the perceived risk to the university, and determine how the following practices must be applied. Refer to those policies for definitions of ownership, responsibilities, system, and information classifications mentioned hereafter. The requirements and recommendations for workstation security best practices are defined according to the workstation classification level.

An *Information Classification Form* can be obtained at <http://security.tennessee.edu> to assist in defining these classifications.

University policies mentioned in this document can be found from the University of Tennessee Policy Search Page at <http://www.tennessee.edu/policy/>. Best practice documents are referenced from the Information Security Office home page at <http://security.tennessee.edu/>.

## **Compliance**

Any non-compliance of the university's *Information Technology Security Strategy* policies or best practices must be reported to the ISO. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. Reference the *Acceptable Use of Information Technology Resources Policy (IT0110)* for information concerning non-compliance issues.

## **Exceptions**

Compliance with the university's Information Technology Security Strategy, policies, and best practices are mandatory. In some instances, exceptions to policies and best practices must be made due to extenuating circumstances. Such exceptions must be documented and approved prior to implementation. The process for reviewing and approving/disapproving requests for exceptions and can be found at <http://security.tennessee.edu>.

## **Requirements and Recommendations**

Workstation configuration guides that satisfy university policies and best practices must be established by the POA for each campus/institute and reviewed by the ISO.

## **Initial Network Connections**

1. All workstations that connect to the university information technology network, wired and wireless, must be registered with the POA or their designee. At a minimum, the following information is required and must be maintained to provide accurate identification:
  - a. Workstation contact(s), a backup contact, and physical location
  - b. Definition of Information Manager, Information Custodian, Information Classification, and System Classification according to *Information Classification Policy (IT0115)* and *Computer System Classification Policy (IT0116)*
  - c. Hardware and operating system versions
  - d. Main functions
  - e. All associated IP Addresses and IP names
  - f. All associated wired and wireless MAC addresses
2. Workstations must have an approved and up-to-date information and system classification, as well as a defined Information Manager and Custodian as per *Information Classification Policy (IT0115)* and *Computer System Classification Policy (IT0116)*. To assist in defining these classifications, an *Information Classification Form* can be obtained at <http://security.tennessee.edu/>.
3. Users and managers must know and understand the requirements for classifying a workstation and the best practices that will maintain a workstation according to it's classification.

## **Installing and Updating Operating Systems and Applications**

4. A workstation must begin as a clean installation; whether as a new system that is pre-installed by a vendor or re-installation as the result of recovery from a compromise. Legal licensing must be obtained, documented, and retained in an organized manner. Refer to the *Acceptable Use of Information Technology Resources Policy (IT0110)* for more information regarding licensing.
5. Operating system, service, and application security software updates must be applied as soon as possible after the workstation is built.
  - a. Additional security software updates must be applied when they become available.
  - b. Where technically possible, patching processes should be automated to at least receive notification that security software updates are available.
  - c. Security software updates not applied within 30 days must be approved via the exception process defined earlier in this Best Practice.
6. After the operating system and all applications have been installed, a scan of the workstation must be requested at <http://security.tennessee.edu/>. This scan checks for security vulnerabilities that must be fixed and can be used to establish a baseline for the integrity of the workstation. See item #9 for additional details.

## **Compromise and Infection Protection**

7. Where technically possible, university provided antivirus software must be installed; the virus definition files kept up-to-date; and the automatic scanning of all files and services be operational on the workstation at all times as required by the *Acceptable Use of Information Technology Resources Policy (IT0110)*.
8. Where technically possible, additional software, commonly known as “anti-spyware” must be installed to decrease the risk of compromise. This software must be configured to keep the signature definition files up-to-date and be operational on the workstation at all times. This software is useful in providing personal confidentiality during internet usage and improving the integrity of the workstation as a whole.
9. Security scans of workstations must be scheduled to be performed regularly based on the classification of the workstation and the information residing on it. This practice provides a continuous investigation of a workstation’s operation, at any given time, that can be compared to the baseline obtained at the time of the original build or rebuild. Look for suspicious files, directories, folders, user accounts, hidden files, and directories that have not been seen before and not intentionally installed on the workstation. The idea is to find problems and get them fixed before they can be exploited. A security scan can be requested at <http://security.tennessee.edu/>. Refer to the chart below.

	Public	Proprietary	Confidential	Highly Confidential
Non-Critical	Optional	Recommended	Required	Contact ISO
Critical	Recommended	Required	Required	Contact ISO
Highly Critical	Required	Required	Required	Contact ISO

10. Where technically possible, a host-based firewall must be installed and operational on the workstation at all times.

Configure the firewall to:

- a. Set program permissions to allow only necessary inbound and outbound traffic.
- b. Deny access to insecure protocols such as FTP, Telnet, and ICMP.
- c. Log all traffic that traverses the firewall.

Acceptable alternatives to host-based firewalls are the implementation of TCP wrappers. In this manner, the standard security principle of least privileged access is applied effectively and protection of the confidentiality and integrity of the workstation is increased. For guidance or assistance with additional configuration of a firewall, contact the POA for each campus/institute or the ISO.

11. User accounts must not be shared. The standard security principle of least privileged access must be used when performing an operation. Administrative level user accounts must not be used unless the access is necessary to complete work requirements. This applies to workstations and all applications installed on the workstation.

- a. Accounts and identification must be uniquely assigned and separately auditable.
- b. User accounts with super-user or administrative privileges, such as root or Administrator, must not be used for daily operations and support work when a non-privileged account will provide sufficient access to perform required job functions.
- c. Where possible, all default account names must be changed, disabled or removed.
- d. Users must login with a non-privileged user account and password that provides sufficient access to perform job functions and no more.

12. Strong passwords or pass phrases must be used for all workstation accounts and applications. Choosing the strength of passwords and pass phrases includes considering:

- a. **Complexity** – passwords and pass phrases must have a minimum length and be composed of specific characteristics.
- b. **Change Frequency** - Required frequency of password changes is based on the classification of information.

Refer to the *Password Best Practice* for more information on constructing a strong password.

13. When web browsing, especially on workstations accessible by multiple users:
  - a. Always explicitly log out of any account that has been logged into. This ensures that the next user of a workstation does not obtain unauthorized access to accounts.
  - b. Do not download or execute programs from web sites that are not trusted.
  - c. Do not enter sensitive or personally identifiable information (PII) on a web page unless the company is hosting a secure web site. Look for indications of site security in the browser window.
  
14. When handling electronic mail (email) or instant messages (IM) on workstations:
  - a. Always exercise caution when opening correspondence from senders you do not know, trust, or are not expecting anything from.
  - b. Never distribute an executable program as an email or IM attachment.
  - c. Avoid using personal email accounts to conduct university business.
  - d. Do not execute programs or attachments in email or IM that are not properly described and referenced in the text of the message.
  - e. Do not accept file transfers in email or IM that are not expected without verification.
  - f. Do not click on links sent in bulk advertising (SPAM) or IM.
  - g. Do not reply to SPAM messages in any manner.
  - h. Report obscene, harassing, threatening, abusive, insulting, or offensive email, SPAM, or messages that ask for PII to <http://security.tennessee.edu>
  - i. Do not click on "Away" messages in IM, they can be a source of viruses.
  - j. Do not include PII in email or IM correspondence that is not encrypted in both directions of transport.
  - k. Be careful to not divulge PII in public or semi-public places during conversations or by entering PII on public workstations that are vulnerable to "shoulder surfing".
  - l. Disable the automatic execution of code embedded in documents and the auto-open or preview pane of messages in email clients.
  
15. If a security issue involving a workstation is suspected, the incident should be reported to the ISO at <http://security.tennessee.edu>. Appropriate action will be based on the *Incident Response Best Practice* for each campus/institute.
  
16. Based on the system/information classification, regular backups and recovery tests of files must be implemented for the workstation as defined by the *Availability Best Practice*. This aids in ensuring the integrity and availability of workstations and the information stored on them. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Optional	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

17. Workstations must be logged off and shut down at the end of the day. If a workstation must be left operational then the keyboard must be locked and require authentication to be activated.

## Configuration Requirements for All Workstations

### System Hardening

The operating system configuration should be hardened according to the appropriate Center for Internet Security Benchmark found at <http://www.cisecurity.org/>. Each of these guides provide detailed information on the best practices for optimally hardening a workstation against unauthorized access, thereby increasing the depth of defenses that are employed to protect the confidentiality, integrity, and availability of the workstation.

18. A login banner containing a warning message must be presented prior to the normal user login process. At a minimum, the banner should contain:
- the name of the organization that owns the workstation
  - the explicit prohibition of unauthorized use of the system
  - the notification of active workstation monitoring

This message could be vital to the successful prosecution of trespassers on the university's information technology network. Samples of appropriate login banners can be found at <http://security.tennessee.edu/login-banner.shtml>.

19. Login screen prompts must be configured **not** to display the account name of the last user logged into the workstation and **must require** a password that meets *Password Best Practice* standards for authentication.
20. Configure a password protected screensaver that is activated after a proscribed period of inactivity based on the system/information classification. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Optional	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

21. System auditing and logging must be enabled for application and operating system events. This includes, but is not limited to:
- user authentication attempts (successful and unsuccessful login attempts)
  - brute force attacks against firewalls
  - system restarts
  - hardware failure
22. Unused services and applications must be disabled or removed.
- Do not allow anonymous access of any kind.
  - Turn off all network services (programs) that are not used.
23. Web browsers must be configured to:
- clear the cache storage file after visiting web sites where sensitive or PII has been entered
  - forbid saving passwords in cache on the workstation
  - forbid pop-ups to activate without explicit permission
  - where technically possible, disable active scripting

24. Workstations configured to send/receive email or IM must be configured to:
- employ digital signatures and encryption where technically possible
  - drop messages with attachments that can't be scanned for viruses
  - set client-based filters to automatically delete SPAM or move it to a separate folder where technically possible
  - only allow or accept IM messages from people you know; disable any direct client connection that will allow anyone to connect to your IM client without your permission
  - turn off any IM function that automatically accepts file transfers

**System and Information Classification Protection Issues**

25. To prevent theft, workstations must be (Refer to the chart below):
- carried onto public transportation vehicles instead of checked as baggage
  - protected in public venues such as hotel rooms, rental vehicles, restaurant cloak-check rooms, etc.
  - physically secured to an unmovable object (The legs of a table that can be picked up and moved do not constitute an unmovable object)
  - physically secured with a physical lock to protect the internal components such as hard drives, memory devices, etc. (Plastic tie-wraps that can be cut with scissors or a knife do not constitute an appropriate physical lock.)
  - secured in a locked office where possible. Lost, misplaced, or stolen keys or other access devices must be reported immediately to the POA and the lock or access changed.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Recommended	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

26. Workstations external to the university campus, including home-based systems, that access restricted university information should be protected to the same level as campus-based workstations as defined by the *Acceptable Use of Information Technology Resources Policy (IT0110)* and *Protecting Restricted Information Best Practice*. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Optional	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

27. File integrity checking (with tools such as Tripwire) must be employed on workstations for any inappropriate or unauthorized modifications with reviews performed periodically. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Optional	Optional	Recommended	Contact ISO
<b>Critical</b>	Recommended	Recommended	Recommended	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

28. Remote access to workstations must be strictly controlled. Remote access implementations include but are not limited to dial-in, VPN, SSH, Remote Desktop, etc. Every method for access should be evaluated based on the impact if any or all of the processes were to be compromised. Refer to the chart below.
- Access must be limited to the fewest individuals necessary.
  - Access must require unique user IDs and password or pass phrase authentication.
  - Personal workstations that are used for university business must meet the requirements of the university's best practices and policies.
  - Virtual Private Networks (VPN) or SSH must be used when conducting university business from networks external to the university network.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Recommended	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

29. Do not allow file sharing on workstations without securing them to authorized users only and requiring encryption. If file-sharing applications are necessary on a workstation, they must be configured to:
- deny automatic out-bound file-serving functions
  - deny auto-start at boot time
  - deny service as an illegal distribution point for copyrighted material
  - automatically scan downloaded files for viruses or worms before the files are opened

30. Shut down file-serving services when not in immediate use. This reduces the risk of compromise and increases the integrity of the workstation. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Recommended	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly Critical</b>	Required	Required	Required	Contact ISO

31. Full disk or file level encryption of data, combined with transport encryption, must be employed where technically possible. Data is vulnerable to disclosure whether it is stored in a file, on a disk, or transmitted across the network. Several technologies can be used to protect data, such as PGP for individual files and email; SSL certificates for web service; and SSH as a replacement for insecure

protocols like TELNET and FTP for data transfers. Refer to the *Protecting Restricted Information Best Practice* for more in-depth requirements. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Optional	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly-Critical</b>	Contact ISO	Contact ISO	Contact ISO	Contact ISO

32. All traces of personal and business data should be securely removed from workstations before being re-assigned, transferred, or disposed of. Deleting files and reformatting a hard drive does not securely remove the data stored on a workstation. Software is provided by the university for fully sanitizing media and for sanitizing single files. All media must be sanitized as required in the *Media Sanitization Best Practice*. Refer to the chart below.

	<b>Public</b>	<b>Proprietary</b>	<b>Confidential</b>	<b>Highly Confidential</b>
<b>Non-Critical</b>	Optional	Recommended	Required	Contact ISO
<b>Critical</b>	Recommended	Required	Required	Contact ISO
<b>Highly-Critical</b>	Contact ISO	Contact ISO	Contact ISO	Contact ISO