Workstation Standard

<table>
<thead>
<tr>
<th>Document Number:</th>
<th>ISP-014</th>
<th>Version:</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Owner:</td>
<td>Director of Information Security</td>
<td>Effective Date:</td>
<td>08/03/2018</td>
</tr>
<tr>
<td>Responsible Office:</td>
<td>Information Technology</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TABLE OF CONTENTS**

Purpose  
Scope  
Standard  
Roles and Responsibilities  
Definitions  
Compliance  
References  
Authority  
Revision History

**PURPOSE**

The purpose of this standard is to establish the acceptable and unacceptable use and configuration of workstations (i.e., electronic devices). This standard seeks to ensure that University-owned workstations are secure and to provide an environment that supports the basic missions of Southern Illinois University Carbondale (SIUC). The University provides computer workstations and other electronic information systems to meet its mission, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This standard is in place to safeguard the University’s electronic information and the University itself and to ensure that workstations are used for their intended purpose. Inappropriate configuration exposes the University to risks including viruses, compromise of systems and services, and legal issues. This standard requires the users of information assets to comply with University policies, standards, and procedures and protects the University.
SCOPE

This standard applies to all University-owned workstations (e.g., desktops, laptops, tablets, mobile devices, etc.) and, in some cases, personally owned devices that use the University network. It is the responsibility of the University Chief Information Officer (CIO), or designee, to determine whether a particular use or configuration of a workstation conforms to University policy, standards, and guidelines.

STANDARD

All members of the University community have a responsibility to use University-owned workstations in an approved, ethical, secure, and lawful manner to avoid loss or damage to University operations, image, or financial interests and to comply with all official policies, standards, and procedures.

Under this responsibility, users of University-owned workstations shall abide by the standards in this document to establish the appropriate and acceptable use of workstations for protecting the University and to enable compliance with laws, regulations, policies, requirements, standards, and other appropriate criteria.

The University and the Office of Information Technology (OIT) reserve the right to modify, add or delete portions of this standard without notice, to protect students, staff, and the University from potential unknown or future security threats and to be in compliance with future regulations.

General Workstation Requirements

All workstations must meet the following criteria:

(a) Workstation baseline image.

The standard workstation operating system and software images supplied by OIT are mandatory for initial deployments of all University-issued workstations. Workstations requiring a custom or nonstandard image are subject to review and approval by OIT and are supported on a best-effort basis. Such workstations may be limited from accessing certain University resources.

(b) Software and hardware updates.
Workstations used to access, store, transmit, or receive data must use operating system and application software that is eligible and configured to receive ongoing security updates from its vendor. Workstations with unsupported or End-of-Life (EOL) software will be denied access to the University network. Users with workstations not owned or issued by the University may seek assistance from OIT for configuration if the intended use of the device is for University business.

(c) Patch management.

Security updates published by operating system vendors must be deployed within 30 days of their release if published within the vendor's patch release cycle, and within 15 days if published via an out-of-cycle update. If the patch addresses a critical time-sensitive issue, OIT will notify the departmental IT staff, through established communication channels, to install the patch immediately.

i. OIT will install the updates to the servers and workstations it manages.

ii. Departmental IT staff will install necessary updates to the servers (physical or virtual) and workstations they manage.

iii. Microsoft System Center Confirmation Manager (SCCM) should be used to patch all Microsoft Windows workstations.

(d) Workstation management tools.

To enhance the security and manageability of workstations and to ensure the appropriate use of workstation software, Microsoft SCCM must be installed on all University-issued Microsoft Windows workstations.

(e) Domain authentication.

The University's active directory domain (ad.siue.edu) is the foundation of the University's network security and network management capabilities. Except as directed by the University CIO, or designee, all University issued workstations that have the technical capability to authenticate to the SIUC domain must do so when present on the University's network. Except for designated guest
networks (i.e., SIU-Guest), all workstations must have the device's media access control ("MAC") address registered with OIT to access the University network. Any workstation without a registered "MAC" address may be removed from the campus network without notice.

(f) Anti-virus / Anti-malware protection.

To limit risk to University data from malicious software, all workstations based on the Microsoft Windows operating system platform used to access, store, transmit, or receive data must have an installed and running antivirus software with definitions not more than seven days old. Anti-virus protection is recommended but not required on other operating system platforms, such as Apple MacOS, Linux, or tablet/smartphone mobile device operating systems. OIT provides guidance and limited support on software for non-SIUC issued workstations if the intended use of the device is for University business.

(g) Encryption.

All workstations used for University business must use University approved encryption technology to secure data at rest.

All workstations not purchased, owned, or issued by the University, which contain confidential University data, must be encrypted. It is recommended that all other workstations not purchased, owned, or issued by the University be encrypted. The OIT provides guidance and limited support on encryption software for non-SIUC issued workstations when the intended use of the device is for University business. Exceptions for workstations where no feasible encryption technology exists may be made on a case-by-case basis and may be subject to compensating controls established by the University CIO, or designee.

(h) Physical security.

All workstations must be secured against loss, theft, and inappropriate access. Workstations which access, store, transmit, or receive data must be physically situated in a manner that prevents viewing of confidential data by individuals who are not authorized to view the data. Unlocked workstations may not be left
unattended. Portable workstations must be reasonably secured at all times, and extra care must be taken to prevent loss or theft of the device. Lost or stolen workstations should be reported to the Department of Public Safety (DPS). Lost or stolen workstations with access to University information systems or containing data for which the University must maintain confidentiality must be reported to OIT Information Security Office as soon as practicable, by e-mail at security@siu.edu.

(i) Operating system inactivity lockouts.

Workstations used to access, store, transmit, or receive data must have a reasonable and appropriate operating system inactivity lockout feature enabled (see table below). Configuration and use of workstation locking mechanisms, including workstation screen saver activations and session idle timeouts, are determined by the University CIO, or designee, in consultation with the affected college or department, and are based on a risk analysis. By default, all clinical workstations should require user authentication before deactivating an operating system screen saver. Any configuration and use of workstation automatic login and logoff feature should be determined by the University CIO, or designee, based on a risk analysis, in consultation with the affected department.

<table>
<thead>
<tr>
<th>LOCKOUT SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Minutes</td>
<td>The default operating system idle timeout for all clinical workstations and any other workstations processing ePHI information.</td>
</tr>
<tr>
<td>15 Minutes</td>
<td>The default operating system idle timeout for all other workstations, excluding labs as noted below.</td>
</tr>
<tr>
<td>20 Minutes</td>
<td>The default operating system idle timeout for labs and workstations in public areas. Instructor workstations in classrooms (i.e., lecture halls) are currently exempt.</td>
</tr>
</tbody>
</table>

(j) Network security.
All workstations which access, store, transmit or receive data must be configured with a basic host firewall or a reasonable substitute as determined by the University CIO, or designee.

(k) Logging; consent to audit.

All workstations which access, store, transmit or receive confidential data (e.g., ePHI, PCI, etc.) must have vendor default application, and security logging enabled with a retention period of at least one year, and such workstations must be made available to the University administration for investigation, inspection, and audit upon request.

(l) Disposal.

Disposal of University workstations must comply with all University workstation disposal and decommissioning policies and standards. When disposing of a device, or transferring the device to another campus unit, the owner and/or LAN Admin must erase or remove all SIUC information from the device using University approved software. Upon request, OIT will assist in this effort.

(m) Loss, theft, damage.

SIUC is not responsible for damage, loss, or theft of workstations not owned by the University. Lost or stolen workstations should be reported to the Department of Public Safety (DPS). Lost or stolen workstations with access to University information systems or containing data for which the University must maintain confidentiality must be reported to OIT Information Security Office, security@siu.edu, within five days.

(n) Local administrator access.

University information technology must have the ability to gain local administrator access to all workstations regardless of operating system, and regardless of the ownership of the workstation. By default, users are not granted administrator access to workstations except as necessary. Users with a business need for elevated access to a specific workstation may submit an OIT help desk request to be granted the appropriate level of access.
(o) Data backup.

Users are responsible for maintaining accurate and secure backups of any data stored locally on workstations. Care should be taken to ensure that backups are encrypted. The University does not back up individual workstations and is not responsible for the loss of data stored on workstations. OIT recommends that all locally stored data be synched/kept on University approved systems (i.e., OneDrive) so that secure backups may be made without user action.

Supported Hardware and Software

(a) Supported hardware.

All workstation hardware, to be purchased with University funds, for University business, must follow approved University procedure. Exceptions may apply and must be approved by the University CIO, or designee. If a department purchases hardware from a vendor other than those recommended by OIT, the equipment may not be provided access to the University network.

(b) Supported software.

All workstation software, to be purchased with University funds, for University business, must follow approved University procedure. All software residing on SIUC workstations must have some level of support (i.e., vendor) and vulnerabilities patched. Vulnerable software must be removed, or will require compensating security controls as approved by the University CIO, or designee. The following categories of software are indicative of the types of supported software.

i. Operating systems. Supported, current and updated operating systems include current vendor-supported versions of Microsoft Windows, Apple Mac OS and enterprise Linux distributions (specifically RHEL and CentOS). Except in cases where paid vendor support is available, other operating systems are supported on a best effort basis.
ii. Enterprise applications. Requests for a new enterprise or clinical applications are reviewed via the procurement process. A list of currently supported enterprise applications is maintained by OIT.

iii. Licensed software. OIT keeps institutional licensing for a broad range of academic, business, clinical, and research related software. Software with limited licensing quantities or licensing purchased within departments may be restricted to functional areas, departments or individuals.

Unacceptable Use

The following activities are prohibited:

(a) Destruction, alteration, damage, or unauthorized modification of workstation hardware without prior approval by OIT.

(b) Circumvention of workstation security controls, including:
    i. Disabling anti-virus or other security software;
    ii. Disabling or circumventing workstation encryption software;
    iii. Disabling or modifying workstation idle timeouts and lockouts;
    iv. Placing BIOS passwords on workstations without prior approval from the University CIO, or designee.

(c) Circumvention of network security controls, including:
    i. Internet protocol ("IP") or MAC address manual assignment without prior review and approval by the University CIO, or designee.
    ii. Circumventing network firewalls, proxy servers, and intrusion prevention workstations.
    iii. Unauthorized monitoring of the University network.

(e) Use of a workstation for illegal activity, including unauthorized "hacking," "cracking" or intrusion of any workstation, system, or network.
(f) Storage, processing, transmission, receipt, or access to information for which the University must maintain confidentiality on a device or workstation in violation of the requirements of this policy.

**ROLES AND RESPONSIBILITIES**

All SIU personnel including, but not necessarily limited to, students, faculty, staff, retirees, outsourced contractual workers, guests, volunteers, temporary extra help, student workers, graduate assistants, undergraduate assistants, and vendors are required to abide with the requirements and standards established within this Workstation Standard.

**DEFINITIONS**

Departmental IT Staff – Refers to decentralized IT staff in colleges, departments, and units across campus with the responsibility of supporting technology and the use of technology by end users within that given area. Typically, this responsibility includes administration of end user workstations as well as departmental file servers.

Level 4 -- Highly Restricted Data – Refer to the University Data Classification Standard.

Local Area Network (LAN) Administrator – See Departmental IT Staff.

Workstation – Workstation is defined as any electronic computing technology asset (i.e., device) with associated equipment, peripherals or storage media, regardless of ownership or control, such as a Microsoft Windows or Apple Mac OS-based desktop, laptop, or tablet computer. A particular mobile device such as a tablet, e-reader, smartphone, or any other such equipment used for University business or to access, store, or transmit University data is considered a workstation for the purposes of this standard. Any device that utilizes the University’s network, and does not otherwise fall into the aforementioned definitions, is also considered a workstation. Workstations may be owned, acquired, or controlled by the University, whether leased, purchased, donated, or provided to the University. Devices owned by an individual, or by a third party (such as home PCs and personally owned tablets or smartphones) are considered workstations for the purposes of this standard as well. All other devices not specifically referenced by the aforementioned definitions, but access the University’s network, fall under the definition of workstation for the purposes of this standard.
COMPLIANCE AND AUDIT

In the case of a security event or alleged breach, the University has the authority to investigate and identify any data involving workstations, and to the extent possible, fulfill the University's obligations to mitigate the effects of the incident. Use of the University network constitutes consent to provide access to a device in this regard, including making the equipment available to audit and investigation by University personnel.

Violations of this standard may result in suspension or loss of the violator’s use privileges, concerning institutional data and University-owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal and equitable remedies may apply.

REFERENCES

ISP-007 Data Classification Standard

AUTHORITY


REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Revision Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Standard was approved by CIO.</td>
<td>08/03/2018</td>
<td>Director of Information Security</td>
</tr>
</tbody>
</table>