# Computer Security Protections Overview

## Required: Level II (moderate) and Level III (high) sensitivity data
## Recommended: Level I (low) sensitivity data

Digital systems/ devices utilized in research, academic, or administrative applications that house, handle, create, or process ***sensitive institutional data*** are required to implement the security protections described in University of Iowa Information Security Policies, as *briefly* summarized below. See the guidelines, tools, resources, and policy documents following this checklist for more detailed information.

**PHYSICAL SECURITY:**

□ Devices must be kept in an access controlled and monitored location, connected to a backup (UPS) power source if availability is critical.
□ Sensitive hardcopy and electronic media removed from the system/device must be secured during transportation and disposal. Printed: Use cover sheets on reports & shred them before disposal; Media: Use locked containers, encrypt portable storage devices, laptops, and tablets, and encrypt data before sending outside the University.
□ DOD-level erase/wipe digital media before disposal or reassignment. Destroy if unable to wipe.
□ Three versions of data backups (incremental, differential, or full) are required, each of which should each be kept for a *minimum* of 30 days. In addition, one fully-recoverable version of all critical data must be stored in a secure off-site location. The restore process must be documented.

**LOGICAL ACCESS:**

□ Individual accounts must be defined for every user of the system/device, preferably using the University HawkID. (Shared service accounts and guest/anonymous accounts must be justified, and should typically be avoided.)
□ Integrate the system with University HawkID authentication to automatically manage user accounts and passwords. Use local strong password practices if Hawk ID authentication is not possible: set complex 15+ character passwords on all *privileged accounts* consisting of a combination of alpha, numeric, and/or special characters, and change passwords every 180 days.
□ Employ the “least privilege” principle by granting system/ device users the minimum necessary authorization level to sensitive information stored on the system in order to do their work.
□ Perform a quarterly review of all accounts and authorizations on the system/device, deactivate invalid/terminated users, and remove unnecessary access rights.
□ Employ 20 minute maximum inactivity timeouts on devices which are used to access sensitive data. (Screen savers with passwords may be used as an alternative.)
□ Configure the system to record login activity, and accesses to sensitive data files. Keep system logs on a separate log/archive server for a minimum of 90 days**.**

**COMMUNICATION SECURITY:**

□ Secure (encrypted end-to-end) communications are required when transmitting sensitive data over the Internet. For example, use HTTPS for web, secure shell (SSH) for terminal sessions, secure FTP (SFTP) for file transfers. Use SSL or IPSEC to secure other un-encrypted legacy

communication protocols.

□ Employ operating system facilities to restrict communications to a defined/limited set of IP addresses and communications ports using an appropriately configured firewall program. (Other facilities such as IPSEC, IP tables, TCP Wrappers, or TCP/IP filters can also be used to restrict communications.)

□ All eligible computers, including those connecting to the system, must have current anti-virus software. (Both the current version installed, and virus signatures updated daily.)

□ All campus client devices connecting to the system are required to be configured to install updates automatically, have a firewall installed and appropriately configured, and regular anti-virus scans to be assured virus and spyware free. Successful patch installation should be verified using a university workstation management service. System Center Configuration Manager (SCCM) for Windows or Casper Suite for Macs are available at no cost.

□ Devices connecting to the system from off-campus are recommended to install updates automatically, have a firewall enabled, and run regular anti-virus scans to be assured virus and spyware free. Successful patch installation should also be verified.

□ The UI Wireless Network Service ("eduroam") should be used for wireless connections. Note that wireless is not allowed for credit card processing transactions without prior approval from the Information Security and Policy Office.

**SYSTEM ADMINISTRATION:**

□ At least two people (system administrators) need access to and knowledge of the system to ensure data integrity, continuity of operations, and change management procedures are followed. Logs must be reviewed regularly, and all changes to the system must be documented.

□ All *unnecessary* services, communications ports, and system-level accounts must be disabled. Document the services (programs) running on the system and the communication ports left open, for future reference.

□ Keep the operating system and all installed applications up to date with service patches, by reviewing, testing, and installing them at least monthly. If for any reason patches cannot be applied, the vendor must be consulted for compensating protections, which must be approved by the Information Security and Policy Office.

□ Implement a Host-Based Intrusion Detection/Prevention System such as Tripwire or OSSEC to monitor the system (i.e., log analysis, file integrity checking, rootkit detection, time-based alerting, and active monitoring).

□ Utilize full disk encryption to protect data stored locally on mobile devices (laptop, tablet, externally attached storage devices, etc.)

□ Register the system in the Uiowa System Registry so that the system can be regularly scanned and monitored for potential security problems.

□ *Immediately* report all suspicious activity and/or security incidents to the Information Security and Policy Office.

For more information, contact the Information Security and Policy Office:
It-security@uiowa.edu (319) 335-6332 http://itsecurity.uiowa.edu

# Computer Security Protections Overview

## Required: Level II (moderate) and Level III (high) sensitivity data
## Recommended: Level I (low) sensitivity data

### University of Iowa Information Technology Policy:

Security Framework: http://itsecurity.uiowa.edu/policy/policy-information-security-framework.shtml
Institutional Data: http://itsecurity.uiowa.edu/policy/policy-InstitutionalDataAccess.shtml
Backup and Recovery: http://itsecurity.uiowa.edu/policy/policy-backup-recovery.shtml
Acceptable Use: http://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources
Network Citizenship: http://itsecurity.uiowa.edu/policy/NetworkCitizenship.shtml
Social Security Numbers: http://opsmanual.uiowa.edu/community-policies/social-security-numbers
Computer Disposal: http://itsecurity.uiowa.edu/policy/ComputerEquipmentDisposal.shtml

### UI Guidelines, Tools, & Other Resources:

Guidelines for Classifying Data: http://itsecurity.uiowa.edu/bestprac/InstData-Classification.shtm
Information Security Program: http://itsecurity.uiowa.edu/resources/infosec-plan.shtml
Defense in Depth: http://itsecurity.uiowa.edu/bestprac/Defense-in-Depth.shtml
Secure Removal of Data: http://itsecurity.uiowa.edu/bestprac/SecureRemovalofData.shtml
ITS Help Desk Protect Your Computer: http://its.uiowa.edu/security
HIPAA Compliance Resources: http://itsecurity.uiowa.edu/hipaa/
Server SSL Certificates Service: http://itsecurity.uiowa.edu/services/servercerts.shtml
Network Security Scan Service: http://itsecurity.uiowa.edu/scan/networkscan-form.shtml
Uiowa System Registry (USR): https://apps.its.uiowa.edu/systemreg/beans/serverlist.action

### All Operating Systems:

CIS Benchmark Tools and System Hardening Guides: http://www.cisecurity.org/

### Windows:

Microsoft Baseline Security Analyzer Tool: http://technet.microsoft.com/en-us/security/cc184924.aspx
Microsoft Security Resources: http://www.microsoft.com/about/twc/en/us/security.aspx
Microsoft Windows Server 2012 and 2012 R2 Guide:
https://technet.microsoft.com/en-us/library/Hh831360.aspx
Microsoft Windows 2008 Security Guide:
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17606
Microsoft Windows 8.1 Security Guide:
http://technet.microsoft.com/en-us/windows/aa905062
Microsoft Windows 7 Security Guide:
https://technet.microsoft.com/en-us/windows/jj667547

### Unix:

UI Linux Security Best Practices & References: http://itsecurity.uiowa.edu/bestprac/linux.shtml
UI ITS Helpdesk Linux Info: http://its.uiowa.edu/linux
Redhat Network Sattelite Server: http://its.uiowa.edu/redhat-network

### Macintosh:

UI ITS Helpdesk Mac OS X Info: http://its.uiowa.edu/macos/
UI Casper Suite management system: http://its.uiowa.edu/casper