# Computer & Server Security Standards

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

## PURPOSE

The purpose of this document is to establish standards for the base configuration and ongoing support of Washtenaw Community College computers and servers. Effective implementation of this standard will minimize security incidents involving College resources.

## SCOPE

This standard applies to all hardware or virtual-based servers and computers, defined as any workstation, desktop or laptops, that are:

- Owned or managed by Washtenaw Community College; or
- Personally owned by employees or contractors; and
    - Connected to Washtenaw Community College networks, resources, or services; and
    - Used to conduct College business; or
    - Storing Washtenaw Community College data

This policy is divided into sections (procedures) covering (a) All Computers, (b) All College-Owned Computers, and (c) Servers. All in scope computers, regardless of whether privately- or college-owned, should be configured to the Baseline Standard. All College-owned computers will additionally conform to the College-Owned Computer standard. All servers will conform to all server-specific standards listed.

## ROLES & RESPONSIBILITIES

**Information Security Office:** Responsible to ensure compliance with this policy as a component of the College's information security program.

Advises Server Administrators on best practices to secure servers. Conducts periodic vulnerability assessments.

**Security Incident Response Team:** Responsible to provide security incident management in response to reported incidents.

**System Owners and Administrators:** Ensures that all existing and new computers and servers are configured to support these standards, or that an alternate plan for risk management is provided. Requests vulnerability assessments for new servers and mitigates identified vulnerabilities.

## REQUIREMENTS & PRACTICES

### Baseline Standard for All Computers

The owner of a personal computer may use it at his or her discretion; however, once that computer is connected to the Washtenaw Community College Network (see *College Network* definition), resources, or services and used for the purpose of conducting College business or used to store, process or transfer College data, it is subject to applicable laws and regulations and to College policies. The following are the minimum baseline requirements for all computing systems and devices, regardless of ownership, within the scope of this policy:

- **Systems and applications that are unable to meet the requirements of this section should be immediately brought to the attention of the Information Security Office**
- No individually- or privately-owned systems may be used to store, process or transfer any *Confidential* data as defined with the *Data Classification Policy*. All systems storing, processing or transferring *Confidential* data must be college-owned and adhere to more stringent system and data protection standards (see also *Mobile Device Policy*).
- No system running an unsupported operating system or applications should be connected to the Washtenaw Community College Network or allowed to store any sensitive data as defined with the *Data Classification Policy*
- All systems must use a vendor-supported operating system that currently receives vendor security updates and technical support

- Ensure that all relevant operating systems and application security patches are installed within thirty (30) days of release
- All systems should make use of anti-virus software with up-to-date virus definitions and ensure that anti-virus applications selected are capable of detecting, removing and protecting against other forms of malicious software, including spyware and adware
- System or local firewalls should be enabled to filter inbound traffic to the host with implicit "deny all" policy
- Users must lock their computer or logout when unattended to prevent unauthorized access
- Remove, disable or change password of all default, unused or unneeded accounts
- Ensure that all accounts are in compliance with password requirements in the *Password Complexity & Protection Policy*

**All College-owned Computers**

This standard applies to all computers, including workstations, desktops, laptops or tablets (not including servers) procured, operated or contracted by the College. The following are the minimum requirements established for this group of computers within the scope of this policy:

- **Systems and applications that are unable to meet the requirements of this section should be immediately brought to the attention of the Information Security Office**
- All systems must use a vendor-supported operating system that currently receives vendor security updates and technical support
- Disable all unneeded and insecure services and applications
- Restrict unauthorized physical access by using automated account logout or password-protected screen-saver lock-out after 15-minutes of inactivity
- Users should not be administrators of the local machine
- The use of generic, shared or service accounts should be avoided wherever possible and practical in favor of individual authenticated system access

- System or personal firewalls must not be alterable by users
- The use of applications or services that provide direct remote access to the system is not permitted, e.g. Remote Desktop, VNC, LogMeIn, etc. Remote access to systems connected to Washtenaw Community College networks should be via college-provided VPN services only (see *Remote Access Policy*).
- Users and systems should only use secure and encrypted communications or networks (e.g. VPN) to access, work with or transfer sensitive data. Wireless networks will not be utilized without appropriate authentication, encryption and secured communications.
- The system will not function as a server, e.g. will not provide file shares, web, ftp or peer-to-peer applications
- The system must be affixed with a Washtenaw Community College asset tag or inventory barcode
- The configuration, imaging, deployment and ongoing maintenance of all systems should make use of tools which assist in assuring that consistent configurations are maintained across like systems, e.g. WSUS, SCCM, Ghost, Deepfreeze, AD group policy, etc.
- Systems storing or used to work with sensitive data as defined within the *Data Classification Policy* should do so in accordance with the *Physical & Environmental Security Policy*
- Users working with sensitive data will ensure monitors are positioned in such a way so that it restricts the viewing of to anyone but the authorized user
- All systems should, where feasible and reasonable, institute a login banner that displays the following content:

  "This computer and network are provided for use by authorized members of the Washtenaw Community College community. Any use constitutes acknowledgment that the user has read and understands all applicable Washtenaw Community College policies. All other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer or a network may not be private. Sensitive communications should be encrypted or communicated via an alternative method."

- All computers and media shall be sanitized prior to reuse or destroyed prior to disposal in accordance with established guidelines

**Server Configuration Standard**

The security standards included in the procedures that follow apply to Servers within the scope of this policy (see *Servers* definition). Servers can be involved in the storage, processing or transmission of sensitive data, thus special care must be taken to protect data the confidentiality, integrity and availability of both data and operations involving these systems.

The following standard is provided for installation, setup and configuration of servers:

- **Systems and applications that are unable to meet the requirements of this section should be immediately brought to the attention of the Information Security Office**
- Prior to setup and configuration of any server, configuration and security best practices specific to the operating system being utilized should be reviewed. See the *Further Information* below.
- Systems may not be opened for production or testing access until they have had the latest operating system and application updates applied, anti-viral software installed and activated (where applicable), firewall enabled, and strong passwords enabled on all accounts
- Prior to deployment, conduct a vulnerability assessment in conjunction with the Information Security Office to identify any security vulnerabilities. Remediate or mitigate vulnerabilities.
- Operational groups, including all college departments operating systems meeting the definition of *Server*, must maintain an inventory of all servers within their scope of responsibility. Inventory can either be maintained independently by departments or appropriate information provided centrally to ITS. At a minimum, the following information is required to positively identify the point of contact:
    - Server administrator contact(s) and location, and a backup contact
    - Operating system version and service pack level
    - Device make & model

- Physical vs. Virtual (and hypervisor(s) in use)
- Hardware support status, e.g. warranty dates, end-of-life announcements
- Hostname(s) & IP address(es), including external/internal, e.g. NAT
- Server role, functions and applications, if applicable

- Server inventories must be kept up-to-date on a semi-annual basis
- Ensure that all servers are located in suitably protected and maintained environments as defined within the *Physical & Environmental Security Policy*

**Server Operating Systems & Applications**

- All systems must use a vendor-supported operating system that currently receives vendor security updates and technical support
- No system running an unsupported operating system or applications should be connected to the Washtenaw Community College Network or allowed to store any sensitive data as defined with the *Data Classification Policy*
- Only one primary function should be implemented per server (e.g. web servers, database servers, and DNS should be implemented on separate servers). Core services (DHCP, DNS, NTP) may be housed on the same server. If you are unsure of the number of functions on your server, contact the Information Security Office.
- All servers should be provisioned utilizing configuration management tools and standardized templates to ensure consistency of operating system and application environments across like systems, e.g. WSUS, SCCM, Ansible, Puppet, Chef, virtual server templates, etc.
- Ensure that all system components and application software have the latest vendor-supplied security patches installed

**Server Anti-virus**

- Deploy anti-virus software, where applicable, with up-to-date virus definitions on all systems and ensure that anti-virus applications

selected are capable of detecting, removing and protecting against other forms of malicious software, including spyware and adware

- Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs

**Server Accounts & Access**

- Remove, disable or change password of all default accounts
- Disable all guest accounts
- Identify all users with a unique user name with at least one authentication method (e.g. password, token device and/or biometrics)
- Ensure that all accounts are in compliance with password requirements in the *Password Complexity & Protection Policy*
- All accounts should be created following the principle of least privilege, meaning the minimal level of rights needed to perform the requirements. Additional access should be granted only on an as-needed basis.
- All local and domain accounts with privileges above normal user level should ensure use of strong passwords
- Disable all unneeded and insecure services and applications
- Restrict unauthorized physical access by using automated account logout or password-protected screen-saver lock-out after 15-minutes of inactivity
- Password "lockout" features should be enabled on any systems where it is available and reasonable to implement. Users should be locked out of systems after six (6) unsuccessful attempts within a thirty (30) minute period of time. Access should be denied for thirty (30) minutes or until reset by authorized staff.
- Where practical, all servers shall institute a login banner that displays the following content:

  "This computer and network are provided for use by authorized members of the Washtenaw Community College community. Any use constitutes acknowledgment that the user has read and understands all applicable Washtenaw Community College policies.

All other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer or a network may not be private. Sensitive communications should be encrypted or communicated via an alternative method."

- Limit system, application and data access only to authorized users and, where possible, encrypt all stored sensitive data. See the *Data Classification Policy* for further information on Washtenaw Community College's data classification levels and requirements.

**Server Networks**

- Use an appliance-based firewall or enable host-based firewall to block non-allowed traffic
- Build a firewall and/or VPN configuration that restricts connections between publicly accessible systems and any system component storing sensitive data, including any connections from wireless networks
- Ensure that servers are appropriately located or isolated on networks, e.g. DMZ, public, private, and are only publicly or widely reachable when appropriate to satisfy application or functional requirements
- Prohibit direct public access between external networks and any system component that stores sensitive data (e.g. databases, logs, trace files)
- Disable insecure remote access protocols, and use only secure remote-access protocols such as SSH, SFTP, SCP, RDP with strong encryption, and VPN
- Encrypt all non-console administrative access. Make use of secure, encrypted technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.
- Clock must be automatically synchronized via NTP to a recognized time server
- Do not enable open, non-authenticated, file sharing
- Ensure that remote access is provided in accordance with the *Remote Access Policy*

- Avoid trust relationships between systems, as these may present a security risk. Do not make use of a trust relationship when some other method of communication exists sufficient to fulfill requirements. If establishing a trust relationship between systems or services is unavoidable, ensure that passwords are periodically changed or contact the Information Security Office if you are unaware of alternatives. See *Password Complexity & Protection Policy.*

**Server Backups**

- System, application and data backups will be taken regularly (e.g. daily, weekly, monthly) per schedule determined cooperatively with data owners and functional business leads. This schedule should be based on a number of factors including data sensitivity, criticality, time and ability to recover and resume operations, and compliance and legal requirements.
- A media inventory will be maintained by backup administrators
- All external media will be encrypted
- All external media will be appropriately labeled, including content summary and date
- All media containing sensitive data will be accurately tracked, e.g. location
- All media containing sensitive data will be transported securely, e.g. secure courier
- All media stored either on- or off-site shall be physically secure
- All media will be retained in accordance with established data retention guidelines
- All media shall be erased prior to reuse or destroyed in accordance with established guidelines

**Server Monitoring & Logging**

- All servers should be continually monitored via software tools for essential operations, including:
    - System reachability and availability
    - Memory, CPU and network bandwidth utilization

- Amount of free space on attached drives
- Critical application availability

- Automated alerting (e.g. text message or email) of system administrators will take place should monitored operations of production or mission critical servers fall outside of established parameters or thresholds
- Server logging will be enabled to identify and track account activity, e.g. login/logout, and potential breach or security incidents
- All servers should be directed to transmit or store logging on a centrally established log, syslog or Security Information and Event Management (SIEM) server, if one exists
- All security-related events on servers must, where possible, be logged and audit trails saved, including:
  - Account login/logout
  - Actions taken by privileged users, e.g. administrator, root
  - Use of privileges, e.g. sudo, User Account Control (UAC)
  - Access to audit or accounting records
  - Activation and deactivation of privileged functions
  - Modification of identification or authentication mechanisms
  - Access to or manipulation of sensitive stored College data, e.g. database access

  Logged event data should include:
  - User identification
  - Type of event
  - Date and time
  - Success and failure indication
  - Origination of the event
  - Identity or name of affected sensitive stored College data
  - Network addresses and protocols

- All security logs must be reviewed, or aggregated and then reviewed, daily
- All security logs will be kept online for a minimum of one (1) month
- All security-related events of clear or suspicious significance will be promptly reported to the Information Security Office

**Server Ongoing Maintenance**

- Establish a process to identify newly discovered security vulnerabilities (e.g. subscribe to alert services freely available on the Internet)
- All relevant operating system and application security patches should be installed within thirty (30) days of release
- Operating systems should not be older than one minor release or service pack from the current release
- Establish a review cycle for event and alert logs
- Established a process for approval, acceptable use and removal of system privileges
- Audit the use of all privileged accounts, e.g. administrator or root, where possible. This auditing should include the functions or commands performed, e.g. sudo, UAC, etc. performed by these accounts.
- Immediately revoke access for any users who have left the College
- Remove or expire unneeded, inactive user accounts at least every ninety (90) days
- Establish and follow change control procedures for all system and software configuration changes
- Ensure that servers and associated applications are maintained utilizing configuration and change management tools to ensure consistency of operating system and application environments across like systems, e.g. WSUS, SCCM, Ansible, Puppet, Chef, etc.
- Adopt procedures to help ensure that individuals occupying positions of responsibility within organizations (including third-party service

providers) are trustworthy and meet established security criteria for those positions

- Adopt procedures to help ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers
- Report security incidents involving the potential breach of server access to the Security Incident Response Team
- Establish, maintain, and effectively implement plans for emergency response, backup operations and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations
- Ensure that vendor recommended best practices, support and maintenance guidance are followed
- Ensure that server hardware and software applications supporting functions identified as essential to operation of business related operations are suitably protected under vendor maintenance agreement

**Server Audits**

- Vulnerability scans will be performed on all servers monthly by the Information Security Office
- Authorized Information Security Office members will perform compliance audits annually. These audits will include compliance assurance checks, e.g. PCI-DSS, GLBA, etc., as well as review of configuration and operations against established College policy, standards and guidelines.

## Further Information

The following websites offer more information on compliance, configuration and security best practices:

- Center for Internet Security (CIS) – *www.cisecurity.org*
    - Information available includes a compilation of security configuration actions and settings to "harden" various operating systems

- Microsoft Windows Security Baselines – *docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines*
    - Available tools include the Microsoft Security Baseline Analyzer
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) – *csrc.nist.gov*
- Payment Card Industry Data Security Standards (PCI-DSS) – *www.pcisecuritystandards.org/document_library*
- United States Server Emergency Readiness Team (US-CERT) – *www.us-cert.gov*

## COMPLIANCE

This policy is a component of Washtenaw Community College information security program that is intended to comply with the PCI-DSS, FERPA, HEOA, GLBA, HIPAA and other regulations.

## EXCEPTIONS

In the event a device or software cannot support this policy compensating controls will be documented and used to mitigate the risk of a breach by a compromised passphrase/password.

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

## VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Washtenaw Community College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

## DEFINITIONS

**CIA Triad:** Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

> **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
>
> **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
>
> **Availability**: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

**College Network:** The Washtenaw Community College Network is defined as all computer and data communications infrastructure, including the core or backbone network, all local area networks, and all equipment either connected to those networks (independent of ownership) or registered to any domain owned by the College.

**Computer:** Computers are defined as computing devices, e.g. workstation, desktop or laptop systems, smart phones, tablets, etc., typically intended for individual or personal use.

**Data:** Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

**Data Owner:** Data Owners are College officials having direct operational-level responsibility for the management of one or more types of data.

**Network Address Translation (NAT):** A method of remapping one IP address space into another by modifying network address information in IP header of packets while they are in transit across a traffic routing device. Also, a technique that hides an entire IP address space, usually consisting of

private IP addresses, behind a single IP address in another, usually public address space.

**File Transfer Protocol (FTP):** A network protocol used to exchange and manipulate files over a TCP computer network, such as the Internet.

**Remote Desktop Protocol (RDP):** A multi-channel protocol that allows a user to connect to a networked computer.

**Secure Copy Protocol (SCP):** Application for secure transfer of computer files between two remote hosts using the Secure Shell (SSH) protocol.

**Secure File Transfer Protocol (SFTP):** SFTP, or secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network.

**Secure Shell (SSH):** Secure Shell is an application utilized to log into another computer over a network using authentication and strong encryption.

**Service Account:** A system account that is required by applications as part of normal function or operation. Note that service accounts are not typically utilized for interactive login.

**Server:** A computer which is either physically connected, or virtually connected in the case of hypervisor environments, to the Washtenaw Community College Network or residing or hosted externally for the purpose of sharing or distributing its information resources, including applications or data, in support of a Washtenaw Community College business- or academic-related function.

**Security Information and Event Management (SIEM):** Software products and services that provide real-time analysis of security alerts generated by applications and network hardware.

**User:** Any Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

**Virtual Private Network (VPN):** An application that provides a secure connection to another network over the Internet.

## REFERENCES

*Data Classification Policy*

*Mobile Device Policy*

*Password Complexity & Protection Policy*

*Physical & Environmental Security Policy*

*Remote Access Policy*

*Request for Policy Exception*

## REVISION HISTORY

| Version | Description | Revision Date | Review Date | Approver |
|---|---|---|---|---|
| 1.0 | Initial version | 12/10/2018 | - | WJO |