Information Technology Services

WSU Endpoint Security Standard

Author(s): Bryan Dent

Keela Ruppenthall (initial version)

Date: 9/15/21

Washington State University

Revision History

Version No.	Date	Description	Author
1.0	06/12/2020	Initial Release	Bryan Dent Keela Ruppenthall
1.1	8/4/2021	Updated per EIS recommendations	Antony J. Opheim
1.2	8/26/2021	First round through ITSAC Infrastructure committee	Kevin Imel Antony J. Opheim
1.2	9/15/2021	Second round through ITSAC Infrastructure committee	Kevin Imel Antony J. Opheim

Contents

Standards References

NIST 800-53

- AC-2: Account Management
- AC-3: Access Enforcement
- AC-6: Least Privilege
- CA-2: Security Assessments
- CA-9: Internal System Connections
- CM-2: Baseline Configuration
- CM-3: Configuration Change Control
- CM-4: Security Impact Analysis
- CM-6: Configuration Settings

Endpoint Security

Endpoint Security Standard

Background:

Endpoints (e.g., laptops, desktops, mobile devices) are a fundamental part of the WSU information system landscape. Endpoints are an important source of connecting end users to networks and systems and are also a major source of vulnerabilities and a frequent target of attackers looking to penetrate a network. User behavior is unpredictable, clicking a potentially malicious URL or modifying endpoint settings for personal preference increases the amount of unnecessary risk and the size of WSU's threat landscape.

Endpoint security is the process of securing the various endpoints on an information system, often defined as end-user devices such as mobile devices, laptops, and desktop PCs, although hardware such as servers in a data center are also considered endpoints.

Purpose:

An information system is composed of many components that can be interconnected in a multitude of arrangements to meet a variety of business, mission, and information security needs. How these information system components are networked, configured, and managed is critical in providing adequate information security and supporting WSU's risk management process.

Scope:

This policy applies to all Institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit Institutional Data.

Standard:

1. All information systems administrators will create and maintain and endpoint inventory and determine classification for each endpoint.
2. Endpoints must be registered with the local WSU information systems administrator for each college/division or IT department. This includes endpoints owned by the university as well as granting agencies.
3. All information system administrators will maintain and manage a configuration management process that includes, at a minimum, the following:
    a. Development of a baseline configuration for all endpoints.
    b. A change management process for tracking and approving configuration changes.
    c. Configuration Monitoring to ensure compliance.
4. University personnel, including all faculty, staff, and vendors on contract to the university; may not be allowed to have administrator/root level access tied to access credentials (e.g., Network ID) used for standard day-to-day work functions.
    d. IT staff specifically assigned administrator/root functions for endpoint devices as a part of their official job role **shall** have a separate set of credentials which allow for administrator/root functions (administrator/root for servers is handled differently). There may be no commonality of naming or passwords between sets of credentials.
    e. Where applicable, exceptions for non-administrator/root level faculty/staff **may** be granted by their Area Technology Officer (ATO) for a secondary set of credentials, local to a specific endpoint only, with elevated privileges. These exceptions may never be for convenience but must be only for specific, well defined, job functions. These secondary credentials must allow elevated access to only those functions that are required for the specific job function, where possible, and may only be used only to accomplish admin/root functions as defined by the exception documentation. All password formulation and change policies apply to these secondary credentials. Where possible, MFA should be utilized to further secure these credentials. Secondary credentials may be revoked by the ATO or CISO at any time for any reason. The ATO must keep a log of all granted exceptions, will review these quarterly, and remove any which are no longer required. This log will also be made available to University Audit and CISO upon request.
    f. Software tools that allow for a temporary elevation of privileges are allowed providing that:
        i. A log is maintained for a minimum of one (1) year of all elevation requests which is made available to University Audit or the CISO upon request.
            1. Logging of the stated reason for this elevation request is highly desirable but not required
        ii. Elevation requests do not exceed a duration of one (1) hour.
        iii. Elevation requests are limited to no more than three (3) during any twenty-four (24) hour period per individual user.

4. Endpoint users may access university data, including data protected under Executive Policy #8 and other applicable university policies, state, and federal laws from university owned endpoints. In no case may this data be created on, stored, or forwarded to non-university-controlled storage except as covered by existing contract with that vendor or specifically allowed as part of assigned job duties and where it is not a violation of university policy, state, or federal law. This includes manual or automated forwarding of email, documents, etc. to storage that is not approved for university use.
    a. **Cloud Storage**: See WSU Cloud Acceptable Use Matrix for a list of approved cloud storage services https://its.wsu.edu/documents/2018/06/wsu-cloud-acceptable-use-matrix.pdf/.
    b. **Email**: Only the WSU approved email service provided via the contract with Office365 may be utilized.
5. Information system administrators must develop a patch management process that includes tracking and evidence capture of patch identification and application. For endpoints, vendor managed patching services may be used when available.
6. Information system administrators must capture security audit logs and monitor endpoints as defined in the WSU Standard for Information System Audit Logging to provide compliance, audit and investigative evidence.
7. Any WSU confidential and/or regulated data must be retained and disposed of in accordance with WSU BPPM 90.01.
8. For WSU owned endpoint devices, software installation should be limited and controlled utilizing at least one of the methods listed below.
    a. Whitelisting – All software is checked against a list approved by the university/area
        i. ITS/Information Security Services will maintain a list on the ITS website available to all university personnel, of all software that has been approved for use through the Software Review Process
    b. Checksums – All software is checked to make sure the code has not changed
    c. Certificate – Only software with signed certificates from a trusted vendor is used
    d. Path or domain – Only software within a defined and university-controlled directory or domain can be installed
    e. File extension – Software with certain file extensions cannot be installed
9. Endpoint devices must employ principle of least privilege for access to WSU data and information resources.
10. Non-mobile endpoint access shall be secured when not actively in use. They should be physically secured with a key lock and/or be locked in a secured office space.
11. Endpoint devices must encrypt all internal and directly attachable storage using an approved enterprise-class encryption solution such as BitLocker or FileVault. Portable storage devices used to store university data must also be encrypted as per above.
12. Endpoint devices must have WSU data backed up to a storage location owned and maintained by a WSU IT department to ensure ongoing access and protection against loss of critical WSU data. Microsoft OneDrive, configured to replicate My Documents and other standard folders (or equivalent), is an acceptable solution.

13. Endpoint devices must use encryption transfer protocols when transferring WSU Confidential and/or Regulated data in accordance with Executive Policy #8, Data Security Policy.
14. Backups that include WSU Confidential and/or Regulated data must be encrypted in accordance with Executive Policy #8, Data Security Policy.
15. Access points will be limited based on parameters defined in the WSU Authentication Management Standard.
16. Endpoints that do not require wireless network usage should have wireless capability disabled prior to deployment.
17. Passwords should be set to a unique value per user that must be changed immediately after first use.
18. Mobile endpoint devices must be managed as per BPPM 87.10 and 87.11.
19. Endpoint Protection Platforms (EPPs) must be used on all devices that access WSU resources and data, if available. These EPPs include:
    a. Anti-malware
        i. Anti-malware applications are part of the common secure configurations for system components. For platforms for which anti-malware software is not available, other forms of anti-malware such as rootkit detectors may be employed.
    b. Personal Firewalls
        i. Personal firewalls provide a wide range of protection for host machines including restriction on ports and services, control against malicious programs executing on the host, control of removable devices such as USB devices, and auditing and logging capability.
    c. Host-based Intrusion Detection and Prevention System (IDPS)
        i. Host-based IDPS is an application that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity. This is differentiated from network based IDPS, which is an intrusion detection and prevention system that monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify and stop suspicious activity.
20. Restrict the use of mobile code
    a. Caution should be exercised in allowing the use of "mobile code" such as ActiveX, Java, and JavaScript. An attacker can easily attach a script to a URL in a Web page or email that, when clicked, will execute malicious code within the computer's browser.
21. Any endpoint devices containing WSU Confidential and/or Regulated data that are no longer needed must be disposed of in accordance with Executive Policy #8, Data Security Policy.

Administrative:

The Office of the Chief Information Officer is responsible for the administration of, and the enforcement of compliance with this standard.

Definitions:

For further clarification on the terminology and definition of terms used within this document, please refer to the published glossary of terms associated with this document.

Exceptions:

Time-bound, localized exceptions of specific elements of this standard may be authorized by the Area Technology Officer, on a case-by-case basis. Exceptions must be document in the Areas ticketing system of record, citing the specific elements, time period, and justification.

Review Cycle:

This standard is to be reviewed every three years or on an as-needed basis due to changes to technology environments, business operations, or regulatory environments.

Appendix A: Glossary

Acronyms

Acronym	Definition
CIO	Chief Information Officer
CISO	Chief Information Security Officer
EP	Executive Policy
EPHI	Electronic Protected Health Information
EPP	Endpoint Protection Platforms
FERPA	Family Education Rights and Privacy Act
HIPAA	Health Insurance Portability and Accountability Act
IDPS	Intrusion Detection and Prevention System
ITS	Information Technology Services
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer

PCI	Payment Card Industry
PHI	Protected Health Information
URL	Uniform Resource Link
VP	Vice President
WSU	Washington State University

Terms

Term	Definition
Endpoints	Endpoints (e.g., laptops, desktops, mobile devices) are a fundamental part of any organizational system.
Anti-malware	Anti-malware software employs a wide range of signatures and detection schemes, automatically updates signatures, disallows modification by users, run scans on a frequently scheduled basis, has an auto-protect feature set to scan automatically when a user action is performed (e.g., opening or copying a file), and may provide protection from zero-day attacks.
Host-based Intrusion Detection and Prevention System (IDPS)	Host-based IDPS is an application that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity.