| | |
|---|---|
| Policy Title | **Endpoint Management and Security Policy** |
| Policy Number | TBD |
| Approval Authority | Board of Regents of the University of Wisconsin System<br>UW-Madison Information Technology Committee<br>UW-Madison Vice Provost for Information Technology and Chief Information Officer |
| Policy Manager | The UW-Madison Vice Provost of Information Technology and Chief Information Officer is responsible for ensuring policy compliance and providing awareness and training associated with the tools and processes defined in the policy standards. |
| Policy Contact | IT Policy Program, Office of Cybersecurity<br>itpolicy@cio.wisc.edu<br>https://it.wisc.edu/it-community/governance/information-technology-committee-itc/it-policies/ |

## Rationale/Purpose

This policy is a fundamental requirement for protecting the confidentiality, integrity and availability of our Institutions Information and IT Resources. In carrying out its mission of teaching, research, patient care and public service, UW-Madison's faculty, other academic personnel, staff and other affiliates create, receive, transmit and collect many different types of Institutional Information. UW-Madison also maintains significant investments in IT Resources, which include information technology (IT) infrastructure, computing systems, network systems and industrial control systems.

The purpose of this policy is to provide guidance to all members of the campus community in order to ensure that all computers and electronic devices accessing campus resources using electronic means are managed, available, set up reliably to do the expected work, and secured at the appropriate level. Associated Endpoint Management and Security Policy standards/procedures will provide guidance to achieve an adequate level of security to protect the university against unintended access, exposure, modification, or removal of University-owned data by unauthorized individuals and reduce the risk of security breaches that could compromise the integrity of university infrastructure.

Complying with this policy enables faculty and staff to support divisional, departmental, and unit operations relating to teaching and learning, research, outreach, and administration. This policy will help units align with regulatory requirements, legal and contract requirements, and other UW-Madison and UW System Policies.

## Scope

This policy applies to any device, virtual or physical, that connects to the UW System managed network and/or is used to access, manage, process, or store UW System data.

## Policy

1. All devices accessing campus resources must be intentionally managed to reduce risk, safeguard proper and efficient operation of and appropriate access to the intended resource. Applicable standards are outlined in the standards document.
    a. Standards for a particular device should be determined based on the use of the device and the sensitivity/risk of data accessed from a device.
    b. Risk Executives are responsible for reviewing exposure risk for any given endpoint; they are encouraged to work with the Office of Cybersecurity to assist with risk assessments.

2. The UW-Madison Chief Information Officer and Vice-Provost of Information Technology, working with key stakeholders and representatives across campus, is responsible for the collaborative development and maintenance of the standards in support of this policy, and for providing the common tools, processes, and support.

3. Divisions, departments, and units are responsible for creating, documenting, and maintaining implementation and standards for managing endpoints that are specific to the risk and operations of their respective mission.

4. The inability to comply with this policy may require the Risk Executive for the school, college, or division to accept that risk or direct actions to mitigate the risk.

## Related UW-Madison Policies

Cybersecurity Risk Management Policy
https://policy.wisc.edu/library/UW-503

IT Incident Reporting and Response Policy
https://policy.wisc.edu/library/UW-509

IT Asset Inventory Policy
In Development

Vulnerability Scanning Policy
https://policy.wisc.edu/library/UW-518

60.10 Endpoint Security Policy (HIPAA)
https://helpdesk.medicine.wisc.edu/hc/en-us/articles/360037031113-60-10-Endpoint-Security-Policy

## Related UW-Madison Documents

Continuous Diagnostic Matrix (CDM) Expectations Matrix
In Development

## External References including University of Wisconsin System Administration (UWSA) Related Policies

UWSA 1000 Information Security: General Terms and Definitions
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/general-terms-and-definitions-2/

UWSA 1042 Threat and Vulnerability Management Policy and Standards
In Development

UWSA 1036 Endpoint Protection Policy and Standards (TBA)

UWSA 1038 Network Protection Policy and Standards (TBA)

## Policy Administration

The policy will be reviewed for changes approximately one year after the adoption of the policy by the policy governing bodies and then on an on-going, three-year cycle by the UW-Madison IT Policy Analysis Team.

| | |
|---|---|
| Effective Date | |
| Policy History | Issuance Dates:<br>Revised Dates:<br>Reviewed Dates:<br>End Date: |
| Next Review Date | |