OFFICE OF INFORMATION SECURITY
UNIVERSITY of WASHINGTON
Information Technology

Minimum Security Standard

Purpose

This standard describes the minimum information security controls required by University of Washington (University) Administrative Policy Statement (APS) 2.6 (Information Security Controls and Operational Practices) to protect institutional information, information systems, computerized devices, or infrastructure technology.

These controls are derived from the Center for Internet Security Critical Security Controls, Implementation Group 1, with slight modifications to be more suitable to the University environment.

Scope

Unless an exception has been granted, the controls in this standard are required for all University critical information assets and strongly recommended for all other information assets. Executive heads of University departments are responsible for ensuring that system owners/administrators establish and maintain information security controls consistent with this standard.

Exceptions require the approval of the Office of Information Security and the applicable executive head following the process managed by the University Chief Information Security Officer. For UW Medicine information assets, exception requests must follow UW Medicine IT Services procedures.

Additional Resources

APS 2.3 Information Technology, Telecommunications and Networking Projects, and Acquisitions
APS 2.5 Information Security and Privacy: Incident Reporting and Management
APS 2.6 Information Security Controls and Operational Practices
Information Security Glossary
Center for Internet Security Critical Security Controls

Security Controls

1: Inventory and control information assets

Actively manage (inventory, track, and correct) department information assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

2: Inventory and control software assets

Actively manage (inventory, track, and correct) department managed software (operating systems and applications) so that only authorized software is installed.

3: Data Protection

Establish and maintain data inventory, handling, retention, and disposal processes consistent with University data classification and retention policies.

4: Secure configuration of information assets and software
Establish and maintain the secure configuration of department information assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

5: Account management
Establish and maintain processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts and service accounts, to University information assets and software.

6: Access control management
Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for unit assets and software.

7: Continuous vulnerability management
Establish and maintain processes to continuously assess and track vulnerabilities on department information assets, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

8: Audit log management
Establish and maintain processes to collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

9: Email and web browser protections
Ensure use of only fully supported browsers and email clients to improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

10: Malware Defense
Deploy and maintain anti-malware software to prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

11: Data recovery
Establish and maintain data backup, backup protection, and backup recovery processes sufficient to restore in-scope department information assets to a pre-incident and trusted state.

12: Network infrastructure management
Ensure network infrastructure is kept up to date to prevent attackers from exploiting vulnerable network services and access points.

14: Awareness & Training
Faculty, staff, and students must complete annual role-based information security training to be security-conscious and properly skilled to reduce cybersecurity risks to the University.

15: Service Provider Management
Departments must collaborate with UW-IT and UW Procurement on significant IT purchases. Units must follow guidelines on the evaluation of IT service providers to ensure that providers are protecting University platforms and data appropriately.

16: Incident Response Management
Designate personnel to manage incident handling, establish and maintain contact information, and unit level processes to prepare, detect, and quickly respond to an attack consistent with APS 2.5 Information Security and Privacy: Incident Reporting and Management.

History

Last change: December 2023