



Software Asset & Service Provider Management Standard (CIS CSC 2 & 15)

Introduction

The inventory and control of software assets and service provider management are critical functions for managing risk within Weber State University's (WSU) IT environment. This standard is a foundation for preventing cyber-attacks, ensuring only authorized software is installed and utilized, and managing third-party service providers to protect the university's data and operational integrity.

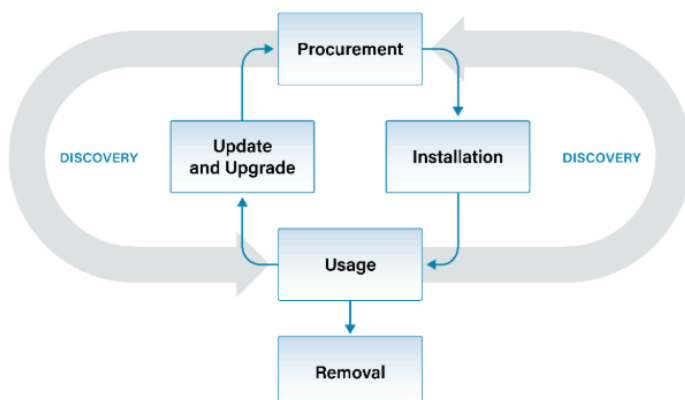
Purpose

This Software Asset & Service Provider Management Standard establishes a comprehensive framework for identifying, tracking, maintaining, and securely decommissioning software and service providers within WSU. This ensures that only authorized and supported software is used and that service providers adhere to the university's security and compliance requirements.

Responsibility

- IT Security Office: Responsible for overseeing all software asset management functions, maintaining the inventory of service providers, conducting assessments, and ensuring compliance with this standard.
- IT Software Licensing and Contract Management Director: Responsible for maintaining (software and vendor) inventories, informing users of their responsibilities, writing RFPs for needed product solutions, managing contracts and software purchases handled by IT, and decommissioning applications and service providers upon retirement.
- Employees: Responsible for adhering to [WSU PPM 10-2, Acceptable Use Policy of University Information Technology Resources](#) and ensuring no unauthorized software is installed or used.
- Legal Counsel: Responsible for incorporating necessary security clauses in contracts with service providers and overseeing provider compliance.

Software Asset Management Lifecycle



Procurement

To protect valuable resources and personal information, the university has put in place a [Software Risk Assessment form](#) for users to request an online cloud service review or a software application review. This software risk assessment will be used to evaluate all software requests and software applications requiring a security and/or legal review. Once the software has been fully approved, the ISO office is responsible for updating the approved software catalog.

Installation

1. All software installations on enterprise assets must be recorded in the authorized software inventory ([see procedures](#)).
2. Controls:
 - a. Only IT Division-approved software may be installed.
 - b. All software must be obtained exclusively from approved IT Division sources.

Usage

- Guidelines: Adhere to [WSU PPM 10-2. Acceptable Use Policy of University Information Technology Resources](#) for all software applications.
- Compliance: Ensure that software usage aligns with business purposes and does not introduce unnecessary security risks.

Discovery

1. Monitoring:
 - a. Utilize automated software inventory tools to monitor and discover installed software continuously.
 - b. Compare discovered software against the authorized inventory.
2. Review:
 - a. The IT Division is responsible for auditing the software asset inventory annually to ensure completeness and accuracy.
 - b. Reconciliation of Inventories
 - i. Cross-check the software inventory against:
 1. Actual deployments (discovery tools, endpoint agents).
 2. Purchase/license records.
 3. Authorized software lists (whitelists).
 - c. Validation of Authorization Status
 - i. Confirm each installed software title is approved and authorized.
 - d. If applicable, check for license compliance
 - i. Verify that the number of deployed instances matches the licenses held.
 - ii. Address over-licensing or non-compliance risks.
 - e. Review of Usage Data (Optional but Recommended)
 - i. Check how frequently software is used.
 - ii. Decommission or reassign licenses for underused or redundant software.
 - f. Document Findings
 - i. Findings (e.g., unauthorized software, exceptions, outdated software).
 - ii. Actions taken (e.g., removal, patching, licensing remediation).
 - iii. Responsible parties and due dates for remediations.
 - g. Reporting and Metrics
 - i. Provide reports to management or security teams on:
 1. Software asset posture.
 2. Compliance levels.
 3. Remediation progress.

3. Action:
 - a. Document Findings
 - i. Findings (e.g., unauthorized software, exceptions, outdated software).
 - ii. Actions taken (e.g., removal, patching, licensing remediation).
 - iii. Responsible parties and due dates for remediations.
 - b. Reporting and Metrics
 - i. Provide reports to management or security teams on:
 1. Software asset posture.
 2. Compliance levels.
 3. Remediation progress.
 - c. Update the allowed software catalog

Removal

1. Remove or remediate unauthorized software instances.
2. Upon retirement of services, the IT Division must decommission applications and service providers, ensuring the secure disposal of enterprise data.
3. Security:
 - a. Remove retired software from the network or isolate affected assets to protect against residual data risks.
 - b. Maintain copies of user data as needed.
 - c. Ensure that any retired software does not store data in other servers or cloud infrastructure not owned by WSU.

Service Provider Management Process

Figure 1. Service Provider Management Process



Identify Service Providers

1. Inventory: Maintain a comprehensive list of all service providers, including:
 - a. Name of Service Provider
 - b. Business Unit Leveraging the Platform
 - c. Service Provider Classifications
 - d. Point of Contact at Service Provider
 - e. Point of Contact within the Enterprise Managing the Service Provider Relationship
2. Review: Update the inventory annually or upon significant changes to the enterprise or service provider's operations.


Establish Requirements

1. Development: Define security obligations, performance metrics, availability requirements, reporting standards, and shared responsibility models for all service providers.
2. Classification: Categorize providers based on risk, sensitivity of handled data, and business criticality.

Classify Service Providers

Purpose of Classifying Service Providers is to identify high-risk vendors who require stricter security controls and

monitoring, streamline oversight and contract management based on risk, ensure compliance with regulations (GDPR, HIPAA, GLBA, etc.) by knowing who processes sensitive data.

1. Criteria: Assess service providers based on:
 - a. Data Sensitivity
 - b. Data Volume
 - c. Availability Requirements
 - d. Applicable Regulations
 - e. Inherent Risk or Mitigated Risk
 - f. Geographical Location
 - g. Supply Chain Dependencies
2. Documentation: Ensure each service provider has an assigned classification based on the type of data they are handling and that classifications are integrated into this standard.
 - a.  3.7 - Data Classification Framework.docx

Assess Service Providers

1. Evaluation:
 - a. Utilize standardized assessment reports (e.g., SOC 2, PCI Attestation of Compliance, HECVAT) and customized questionnaires.
 - b. Conduct assessments during onboarding, annually at a minimum, upon contract renewal, and when significant changes occur.
2. Frequency: Assessments must occur annually or with new and renewed contracts.

Onboard Service Providers

1. Integration: Ensure seamless integration of service providers into the existing technology stack, adhering to established security requirements and compliance standards.

Monitor Service Providers

1. Continuous Oversight:
 - a. Monitor compliance with contractual agreements and security frameworks.
 - b. Perform vulnerability monitoring and review service provider release notes.
 - c. Monitor for third and fourth-party relationships.
 - d. Track changes in security posture and incident response capabilities.
2. Reporting: Document and address any deviations or incidents promptly.

Decommission Service Providers

1. Procedure: Securely remove all enterprise data from service provider systems, deactivate user and service accounts, terminate data flows, and ensure the secure disposal of data upon contract termination.
2. Verification: Ensure all decommissioning actions comply with this standard.

Service Provider Inventory Management

- Establish and Maintain an Inventory of Service Providers
 - Maintain an up-to-date inventory of all with whom your organization shares data or services, including classifications on the sensitivity of data shared, the criticality of the service provided, and the enterprise contracts ([see procedures](#)).

Note: The following appendices correspond to each CIS CSC Standard:

[Appendix A](#)
[Appendix B](#)

Revision History
Creation Date: March 12, 2025
Amended: N/A