ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

STATEWIDE Policy

	NUMBER 107-004-010	**SUPERSEDES** Policy #107-004-010 September 8, 2008
	EFFECTIVE DATE	**PAGE NUMBER** Pages 1 of 2
	REVIEWED DATE	
Division **Enterprise Information Services (State CIO)**	**REFERENCE** ORS 174.112, 276A.230, 276A.233, 276A.236 Oregon Accounting Manual 10.50.00.PO, 10.50.00.PR, 15.55.00, 15.60.10 Statewide Procedure 107-004-010_PR National Institute of Standards and Technology Special Publication 800-53 (Rev5)	
Policy Owner Cyber Security Services		
SUBJECT Information Technology Asset Inventory and Management (Software)	**APPROVED SIGNATURE**	

PURPOSE

This policy establishes methods and timeframes that state agencies must use to manage, collect, and report information technology (IT) software asset information.

Agencies will establish procedures to track the acquisition, deployment, management, and disposition of all IT software assets under their control. Agencies will collect and report information about IT software assets and planned IT investment (lifecycle) to Enterprise Information Services (EIS).

APPLICABILITY

This policy applies to all state agencies as defined in ORS 174.112, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and board are excluded:

- Secretary of State
- State Treasurer
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice
- Oregon State Lottery
- State Board of Higher Education or any public university listed in ORS 352.002

DEFINITIONS

End of support (EoS) / end of life (EoL) means products that are no longer supported or maintained by the vendor, meaning the vendor has stopped providing updates, patches and technical support for the product.

Extended service support means a paid, time-limited mechanism that delivers a narrower set of vendor-issued updates after official EoS.

Third-party or vendor extended security updates (ESU) programs means continued maintenance for customer-entitled version included security patches and operational support after vendor maintenance ends.

Software means computer programs and associated data that may be dynamically written or modified during the device's execution (e.g., application code, libraries) and includes on-premise software installed on agency hardware and software as a services (SaaS) accessed via network. Software is categorized as system software or application software. Examples of system software include operating system, device drivers and language processors. Examples of application software include general purpose software, customized software and utility software.

GENERAL INFORMATION

Asset Inventory Management

Agencies must identify an Agency IT Asset Management Coordinator.

Agencies must create and maintain a continuous IT Software Asset Inventory to submit annually by December 31 which includes:

- Assigning a unique asset identifying number to all capital and non-capital IT software assets. If an asset identifying number is not assigned, EIS will assign a unique identifier when the asset is added to the enterprise asset management tool.
- Annually inventorying all capital and non-capital IT assets at all agency locations, including IT assets assigned to employees, contractors, and volunteers. Inventory may be conducted through a combination of automated discovery tools, manual verification of license entitlements and vendor portal audits.
- Investigating and documenting:
    - discrepancies between the documented inventory and undocumented, discovered software assets
    - discrepancies between documented inventory and missing software assets.

Refer to the Information Technology Asset Inventory and Management (Software) procedure (107-004-110_PR) for mandatory data elements for the IT Software Asset Inventory.

Asset Lifecycle Management

Agencies must create and maintain, asset lifecycle replacement plan(s) to ensure continued security supportability, and compliance with operational and cybersecurity standards.

Lifecycle plans should not override or supersede any vendor-declared sunset dates or end-of-support (EOS) milestones. (For assistance in identifying software EOS dates, refer to Center for Internet Security End-of-

Support Software Report List https://www.cisecurity.org/insights/blog/end-of-support-software-report-list.) Lifecycle plans that override or supersede any vendor-declared sunset dates or EOS milestones must document extended service support or third-party or vendor extended security updates programs that mitigate EOS risks.

Agencies must submit asset lifecycle replacement plans annually with their asset inventory.

Software License Management

Agencies must have in place and maintain software licensing agreements for all software in their inventory.

Agencies must actively manage their software licensing agreements.