OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	**Information Technology Lifecycle**	**ISD_610_04**
Supersedes:	None	
Applicability:	All state employees (their agents), volunteers, vendors and contractors, including those affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives.	
Reference:	ISD_620_01 Information Asset Classification ASD 250_02 Asset Tracking ASD Procedure FS-022 'Asset Tracking Procedure' IRM 107-004-010 Information Technology Asset Inventory & Management	
Effective Date:	**March1, 2020**	**Approved:**

I. PURPOSE

State policy requires all state-owned Information Technology (IT) assets to be managed throughout the asset's lifecycle (acquisition through disposal). This policy establishes the lifecycle and administrative expectations for IT assets at ODFW.

II. DEFINITIONS

A. **Agency:** General term that refers to the Oregon Department of Fish and Wildlife (ODFW) and employees

B. **Asset Classification:** A systematic arrangement into groups or categories according to a set of established criteria. In this case, to categorize agency risk per policy ISD_620_01 'Information Asset Classification'.

C. **Asset Inventory:** The process of discovering, verifying, and documenting information about an organization's assets (through manual and/or automated means).

D. **Enterprise:** Incorporating all aspects of an organization, employing a solution that is comprehensive or an undertaking that is especially difficult, complicated, or risky.

E. **Information Technology (IT) Asset:** Any data, application, computer, peripheral, portable computing device, or other technology used to store, transport, modify, display, or report

information that has value to the organization regardless of its physical form or characteristics.

F. **Lifecycle:** The series of stages through which an asset will be subject to during its lifetime including, but not limited to, acquisition, deployment, support, and disposal. These stages will often include a process of budget management and asset tracking.

G. **Software / Software Application:** Computer code installed on a user's computer or accessible via the internet (cloud) for the purpose of performing specific functions directly for an end user or another application.

H. **Virtual:** Not physically existing but made to appear so by software and other technology.

III. POLICY

A. Establishment of Lifecycle and Standards

The Information Systems Division (ISD) will establish and periodically update technology standards including serviceable lifecycle expectations for common technology used by the agency. This includes lifecycle standards for IT hardware, software, and other technology devices or systems (physical or virtual) that are connected directly to or otherwise interface to the agency's computer network infrastructure (physically or wirelessly), or when functioning as a standalone state.

A listing of asset lifecycles, standards, and other specific information can be found on the ISD Inside page.

B. Lifecycle Determining Factors

Lifecycles are established as a result of multiple factors that contribute to the security, sustainability, compatibility, and operational efficiency of an IT asset. Together these factors represent the total operational business risk to the agency and determine the lifecycle requirements including maximum length of service.

C. Asset Stewardship

Throughout the lifecycle of an IT asset, agency employees are responsible for protecting and controlling IT assets assigned to them regardless if it is in their direct possession, on loan, or otherwise temporarily assigned elsewhere. No part of a state IT asset is, or may become, the private property of any individual. The state owns all legal rights to control, transfer, or use all or any part or product of its systems.

At no time during the lifecycle (procurement through disposal) will an agency IT asset (or IT assets in the stewardship of the agency) be assigned, loaned, borrowed, or otherwise used for personal use. IT assets on loan from another organization, or procured with external funding, must be disposed in accordance to the agreement.

IT assets awarded, gifted, or acquired as proof of concept will become the property of State of Oregon and are not for personal use. Prior to operation they must be certified by ISD to meet operational standards and recorded within the agency's physical asset inventory system (as applicable).

D. **Physical Asset System of Record**

The agency's physical asset inventory system managed by the Administrative Services Division (ASD) is the official record of inventory for all ODFW assets. Any IT asset records maintained by ISD are for the purposes of supporting operational needs including deployment, product maintenance, technical support, and lifecycle management.

E. **Asset Inventory Data Collection and Disclosure**

Automatic data collection and reporting of IT assets is utilized to improve operational efficiencies throughout the lifecycle and is intended to enhance technical support objectives such as license compliance, policy compliance, trend reporting, security patch management and other business specific uses. Data collected either physically or electronically may be used to supplement the record keeping of the agency's official asset inventory records system or other systems. In addition, IT asset inventory records may be disclosed to meet audits or other official requests as applicable by law.

F. **Procurement of IT Assets**

Product standards and additional documentation are provided on the 'How To Buy IT Items' tab of the ISD Inside page https://inside.dfw.state.or.us/isd/buying_equipment.asp). Accompanying agency policies and procedures for the procurement of goods are located on the ASD Inside pages.

IT assets are processed through ISD to complete the ordering, initial setup, asset tagging, and deployment to the end user. For efficiencies, ISD may designate certain items for direct purchase (e.g. keyboards, mice, cables) or direct ship (e.g. heavy, bulky), and complete the setup remotely or with the assistance of the local office employees, such as unpacking, setup, or asset tagging.

G. **Lifecycle Planning and Approach**

The IT asset lifecycle provides a proactive and predictive approach to planning budgets and maintaining operational efficiencies by establishing the recommended and maximum expectations before replacement of an IT asset is required.

It is highly recommended to plan and synchronize the replacement of all IT assets with their end of life to avoid loss of services or funding complications. Many IT asset lifecycles aligned with biennial schedules, replacements often occur every 2nd or 3rd biennium budget cycle. For instance, planning the replacement of 1/3 of computers each biennium distributes the expense of computer operations evenly and yet maintains full compliance of lifecycle policy. In addition, lifecycle planning prevents unexpected and sometime untimely replacement of assets.

CAUTION: Some providers, especially smaller organizations or those operating in very specialized markets, may stop support of their products abruptly and without notice. To the extent possible, avoid selecting products from companies with narrow offerings and limited support base that may result in a shorter than expected lifecycle. This is true for any specialty purpose hardware and software. Therefore, it is advised to fully research options prior to any procurement.

H. Hardware Lifecycle Standards

The lifecycle for any technology hardware is determined by the expected useful life considering the overall cost of operation and business efficiencies including increasing failure rates, interoperability issues (system to system), declining vendor support, high operating costs, security vulnerabilities, and other significant factors that place business operations at risk.

The hardware lifecycle is considered a security risk, regardless of age, when the product no longer has main stream support, has exceeded extended support, security patches are no longer made available, or is not compatible with other systems or software.

I. Software Lifecycle Standards

The lifecycle for any software applications is determined by the expected useful life considering the overall cost of operation and business efficiencies including increasing instability, interoperability issues (system to system), declining vendor support, high operating costs, licensing compliance, security vulnerabilities, and other significant factors that place business operations at risk.

The software lifecycle is considered a security risk when, regardless of age, the product has exceeded extended support, security patches are no longer made available, or is not compatible with currently implemented operating systems. In addition, the software lifecycle may be considered expired if the Dynamic Link Libraries (DLL) are outdated and/or recognized industry security professionals have identified the software as a moderate or higher business risk.

Lifecycles for commercially available enterprise software are often posted on the internet months or years in advance of end of support or end of life. Significant pre-planning may be required to update or replace in advance of the deadline to avoid a business disruption.

At no time shall a software application remain in service that is unable to meet legal compliance, poses a security risk to business operations, or otherwise unable to meet the minimum qualifications of software lifecycle standards.

J. Data Lifecycle Standards

Data lifecycle retention and destruction is managed by both agency and statewide retention policy and rules. It is an expectation that all employees will follow these schedules for the proper retention and timely destruction of documents or data as required.

K. Disposal

All computing, data storage, networking, communication, and some peripherals retain sensitive data despite deletion or formatting. Disposal requires special handling to maintain information security and prevent unwanted disclosure of information. This includes, but not limited to, the following devices:

- Desktop computers
- Laptop Computers
- Tablets
- Smart phones
- Hard drives (fixed and portable)
- USB keys (thumb drives)

- CD/DVD
- Recording tape
- Network switches and routers
- Copy machines equipped with hard drives (all Ricoh)
- Fax machines equipped with hard drives

To ensure data is irrecoverable, follow established agency procedures or contact ISD to destroy and dispose of these devices by means of physical, electromagnetic, and/or other destructive methods.

CAUTION: Any assets containing (or once contained) agency data with classifications of Level 3 'Restricted' or Level 4 'Critical' are considered high risk and must be disposed with special handling. Contact ISD for specific handling instructions prior to transporting or completing the disposal processing.

Peripherals and components that do not retain data can be disposed directly including, but not limited to the following items:

- Keyboards
- Monitors
- Mice (and other pointing devices)
- Cables

Note: DAS policy may require items of value to be sent to DAS Surplus. See https://www.oregon.gov/DAS/surplus/Pages/Index.aspx for more information.

To maintain accurate service and inventory records, all disposed IT assets must be recorded on the agency's physical asset inventory and provided to ISD.

L. Early Lifecycle Termination

When operational conditions significantly increase the business risk to the agency, it may be necessary to declare an early lifecycle termination. This could result from a lack of security updates, repetitive failures, inconsistent or unreliable data collection, or when use is no longer in compliance with Terms of Condition (TOC) or End User License Agreement (EULA).

Managers may also decide to replace an IT asset earlier than established in order to meet new or changing business demands. The existing asset must have sufficient remaining lifecycle to be repurposed or otherwise must be disposed. See section 'Reassignment of Assets (Trickle Down)' for additional information.

M. Reassignment of Assets (Trickle Down)

Reassignment of IT assets is allowed when the asset has at least 75% of the lifecycle remaining and only when there is significant overall business value to the agency. The total cost of ownership (TCO) value of the IT asset is generally the lowest with the fewest number of reconfigurations. This takes in factors such as setup, user familiarity, re-licensing, asset tracking, down time, and tech support time.

To maintain accurate service and inventory records, all transfer requests for IT assets must be recorded on the agency's physical asset inventory and provided to ISD.

N. **Donations of IT Assets (Receive or Issue)**

Donations of any IT assets to the agency are subject to the same policy, practices, and standards established for the procurement and lifecycle management as if originally purchased by ODFW. Pre-authorization by ASD (asset controls) and ISD (security, legal, and administrative controls) must be obtained in writing and include a written agreement specifying the terms of the donation.

Donations must fully comply with all state and agency policies, and procedures applicable to the item. This includes, but not limited to, any necessary documentation to describe the action, updating asset records, data destruction, and removal of any non-transferable licenses or support conditions.

Any license must be explicitly transferable and documentation provided, otherwise must be fully removed and repurchased in compliance with all license agreements for the intended purpose.

O. **Loaning of IT Assets (Receive or Issue)**

Approval to receive or issue loaned IT assets must be obtained in advance by ASD (asset controls) and ISD (security, legal, and administrative controls), and include a written agreement specifying the terms of the loan agreement including a liability clause and/or disclosure stating the liability if lost, stolen, compromised, or devalued. Loaning of IT assets will be for agency business purposes only.

Loaned IT assets (hardware or software) are subject to the same policy, practices, and standards established for the lifecycle management of the asset and must comply with the established IT standards, or qualified exception, to maintain the security of the agency's network or integrity of its data.

Software assets must remain in full compliance with all End User License Agreements (EULA) and Terms of Conditions (TOC).

Assets returning to ODFW must be recertified by ISD including reconfiguration and scanning for malicious code prior to returning to any service within the agency.

Assets on loan are intended for use with Level 1 'Published' information only. Approval by the data owner is required for use with Level 2 'Limited' data. The director's office and ISD must approve any use of assets with access to Level 3 'Restricted' or Level 4 'Critical' data.

P. **Asset and Lifecycle Exception Process**

Any action that deviates from the standards established for IT asset or lifecycle management must be approved in advance and documented by ISD as an exception. Request for exceptions should be made in writing to the ISD division administrator or deputy.

IV. POLICY GROUP

This policy is part of a suite of Information Technology policies that collectively sets the expectations and use of computing devices and related technology, and falls under the principle policy ISD_610_01 Acceptable Use of State Information Assets.