	DEPARTMENT OF CORRECTIONS **Information Systems**	
Title:	**Information Technology Asset Management**	**DOC Policy: 60.3.1**
Effective:	**9/13/23**	**Supersedes: 8/5/22**
Applicability:	**All functional units**	
Directives Cross-Reference: **DOC Policy 30.1.7 Donations** **DOC Policy 30.2.1 Fixed Assets** **DOC Policy 60.1.1 Acceptable Use of Oregon Department of Corrections Information Technology** **DAS Policy 107-004-010 IT Asset Inventory and Management** **DAS Policy 107-004-100 Transporting Information Assets** **DAS Policy 107-011-050 PR Sustainable Acquisition and Disposal of Electronic Equipment (e-waste/recovery)**		
Attachments: **IT Services Remote Device Agreement**		

I. PURPOSE

The purpose of this policy is to establish the policy and procedure for the information technology (IT) asset management program for the Department of Corrections (DOC) to manage, collect, and report IT assets from acquisition to disposition.

II. DEFINITIONS

A. Asset: A tangible or intangible item of value to stakeholders including all present and future forms of capital and non-capital computer hardware, software, telecommunications, and related items used for agency data management and office automation. The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include, but are not limited to, business or mission concerns.

B. Capital Asset: All tangible and intangible property with an estimated lifespan of one year or greater (including ancillary charges) and an initial value of more than $5,000.

C. Computing Device: A device that can perform substantial computations, including numerous arithmetic operations and logic operations without human intervention. A computing device can consist of a standalone unit or several interconnected units. It

can also be a device that provides a specific set of functions, such as a phone or a personal organizer, or more general functions such as a laptop or desktop computer.

D. Embedded System: A computer system that is designed to perform a dedicated function, either as an independent system or as a part of a larger system.

E. E-waste: Obsolete or non-working electronic equipment and associated electronics that potentially store sensitive or confidential data or are required to be environmentally disposed of timely and accurately.

F. Excess IT Asset: Any IT asset that is not being used for 120 days or more.

G. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of the preceding sentence, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

H. Information Technology Asset Manager (ITAM): The individual responsible for the collection, management, and reporting of information related to the agency's IT asset inventory, and the central point of contact with the Department of Administrative Services (DAS) in matters relating to IT asset inventory and management.

I. Information Technology Services (ITS): The unit that is responsible for providing technical or operational technology services in support of the agency's mission.

J. IT Standard: Minimum criteria established by ITS to ensure that all hardware and software is sustainable and does not impair the availability, reliability, and security of agency and state assets.

K. Mobile Device: A portable computing device that has a small-form factor such that it can easily be carried by a single individual, is designed to operate without a physical connection, possesses local, non-removable or removable data storage, and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations.

L. Non-capital Asset: All tangible and intangible property with an estimated lifespan of one year or greater (including ancillary charges) and initial value of less than $5,000.

M. PC Lifecycle: The series of stages in form and functional activity through which a personal computer (PC) passes during its lifetime.

N. Physical Inventory: The verification of the existence and location of an asset by physical or electronic means.

O. Plug and Play: IT assets that install and work automatically without additional configuration or adjustment.

P. Property Tag: A tag affixed to IT assets for identification and tracking.

Q. Remote Device: Any IT asset that is not physically located at a DOC managed worksite.

R. Risk: A measure of the extent to which an entity or individual is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

III. POLICY

Information Technology Services (ITS) is responsible for developing and maintaining the department's IT asset management program in support of DOC Policy 30.2.1 Fixed Assets. All employees, volunteers, contractors, and other DOC IT asset users are expected to follow the provisions of this policy for the acquisition, management, deployment, and disposition of DOC IT assets. Anyone who violates or otherwise abuses the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

A. General Information

The agency's Chief Information Officer (CIO) or designee shall appoint an ITAM responsible for developing ITAM programs and procedures that track and manage IT assets under their control through:

1. Acquisition

2. Management

3. Deployment

4. Disposition

B. Acquisition

1. IT assets shall be reviewed by the ITAM Coordinator or their designee prior to purchase, contract, donation, or installation. See also DOC policy 30.1.7 Donations. Review shall consist of:

    a. Evaluation of risk to DOC;

    b. Conformity and consistency with IT standards;

    c. Adherence to DOC and state policy as well as state and federal legislation, regulations, and standards; and

    d. Efficient and cost-effective method(s) for support, management, upgrades, migrations, and future technology changes.

2. Any IT assets acquired, purchased, or developed by a DOC employee, contractor, or volunteer shall be deemed DOC property.

3. The ITAM or their designee shall establish a PC lifecycle replacement plan for computers that consists of:

    a. Development of a budget and PC lifecycle replacement plan which is submitted to the Budget Office each biennium. This budget and plan exclude embedded systems and special purpose PCs used in heating, ventilation, and air conditioning (HVAC), security, fire alarm, or other embedded systems and special purpose PCs;

    b. Maintenance of a PC lifecycle that is a maximum of five years; and

    c. Management of a central PC lifecycle replacement budget established for ITS.

4. Any computer that falls outside of the PC lifecycle replacement plan shall be budgeted by the requesting unit.

5. All new IT assets shall be delivered to a DOC managed site.

C. Management

IT assets are controlled by ITS to comply with state and department policies, as well as applicable licensing and copyright laws, regardless of acquisition. This includes, but is not limited to, configuration, protection, and IT asset tracking.

1. IT assets are assigned to a position and not individual staff.

2. Excess IT assets shall be returned to ITS for re-deployment or e-waste.

3. Computing devices shall be connected to the network minimally every 30 days to be updated to reduce risk to the department.

4. The ITAM or designee shall ensure that a physical inventory is conducted on IT assets at least annually and reported to other state agencies upon request.

5. Any IT asset that is discovered as missing must be reported to the Information Security Officer (ISO) immediately.

6. All computer licenses shall be tracked centrally by ITS.

7. Excluding position-assigned mobile and remote device(s), IT assets shall only be transported by ITS unless prior approval has been provided by the CIO or ITAM or their designee. See also DAS policy 107-004-100 PR Transporting Information Assets.

8. ITS shall affix a property tag on all capital and non-capital IT assets that are required to be tracked or IT assets that are deemed as high-theft or high-risk. See also DAS policy 107-004-010 IT Asset Inventory and Management.

9. Any IT asset that is at risk, unapproved, unlicensed, or is not DOC property shall not be connected, or installed on any DOC IT asset and will be immediately removed from all DOC IT assets if discovered. See also DOC policy 60.1.1 Acceptable Use of Oregon Department of Corrections Information Technology.

10. The responsible manager and remote user must sign the IT Services Remote Device agreement (DOC policy 60.3.1 - Attachment A), acknowledging that they are responsible for remote device(s).

11. All systems that are no longer assigned to or in use by an employee, contractor, or volunteer, shall be immediately returned to ITS.

D. Deployment

Installation of all hardware and software shall be conducted by ITS. Exceptions to this policy are DOC purchased and approved IT assets that are plug and play. (Ex. Approved mice, keyboards, and webcams; approved self-provisioned applications that are published to the computer or user.)

1. ITS shall delete all data and applications from excess IT assets prior to redeployment.

2. ITS shall deploy monitoring systems that control, manage, inventory, and protect IT assets.

E. Disposition

All excess IT assets shall be the responsibility of ITS to re-deploy or process as e-waste, excluding embedded systems and special purpose PCs used in HVAC, security, fire alarm, or other embedded systems and special purpose PCs. IT assets that have exceeded their lifecycle or cannot be economically repaired shall be processed as e-waste in accordance with DOC policy and state guidelines regarding electronic e-waste. See also DAS policy 107-011-050 Sustainable Acquisition and Disposal of Electronic Equipment (e-waste/recovery).

F. Exceptions

Any exceptions to this policy must be submitted in writing to the ITS CIO or designee for approval. All approved exceptions shall be recorded and annually reviewed.

IV. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: ____signature on file_____
Julie Vaughn, Rules Coordinator

Approved: ____signature on file_____
Heidi Steward, Acting Director

IT Services Remote Device Agreement

Date:

This agreement must be completed, signed, and submitted to the DOC ServiceDesk prior to any device being utilized outside of a DOC managed worksite.

PLEASE READ THIS FORM CAREFULLY BEFORE SIGNING. All parties acknowledge they are subject to and have read the policies below, have an active DOC account (required) with a current UAF (User Authorization form) on file with IT Services, and agree to:

1. Utilize issued remote devices for department business only;
2. Maintain reasonable physical control over all hardware;
3. Report lost or stolen remote devices immediately to their Manager and ITS Security;
4. Not install or connect any non-approved device(s) or software that is not deemed DOC property;
5. Power on, login, and connect remote device to a secure network for at least one day, at a minimum of every 30 days for system updates. If system updates cannot be completed, the device shall be brought into a DOC managed worksite and connected to the DOC network to complete;
6. Resubmit a new form to the DOC Service Desk to transfer remote device or if any other changes occur;
7. Contact the DOC Service Desk when the remote device is no longer utilized; and
8. Read and adhere to Chapter 60 Information Systems Policies

Division Information

Division: Unit: Location:

Remote Device Information

6-digit Asset Tag Number: Desktop: Laptop:

Physical Location

Home

Business Business Name:

Other Other Description:

If the device will not be in the State of Oregon, enter the state or country:

Authorization

By signing this Agreement, you acknowledge that you will follow the guidelines above, have read the Chapter 60 policies, and are responsible for this remote device.

User Printed Name	Phone	Signature

Managers Printed Name	Phone	Signature

Submit Form

Terms of this agreement may be subject to change at any time, including but not limited to a State of Emergency