GEORGIA DEPARTMENT OF CORRECTIONS **Standard Operating Procedures**		
Policy Name: Asset Management		
Policy Number: 105.13	**Effective Date:** 00/00/2024	**Page Number:** 1 of 7
Authority: Commissioner	**Originating Division:** Executive Division (Office of Information Technology)	**Access Listing:** Level I: All Access

I. Introduction and Summary:

The Georgia Department of Corrections (GDC) shall use asset inventory and asset management procedures as the method by which the Agency maintains accountability of the physical computing devices and software.

II. Authority:

A. Georgia Technology Authority: Enterprise Policies, Standards, and Guidelines - PS-08- 005 Enterprise Information Security Charter;

B. Criminal Justice Information Services (CJIS) Security Policy, Version 5.9.4, 12/01/2023;

C. NIST 800-53 Rev. 5, Recommended Security Controls for Federal Information Systems and Organizations, September 2022;

D. HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, March 2013.

E. ACA Standards: 5-ACI-1F-04, 5-ACI-1F-05, 5-ACI-1F-04, 5-ACI-1F-05, 5-ACI-1F-05, 5-ACI-1F-05, 5-ACI-1F-05, 5-ACI-1F-05, 5-ACI-1F-04, 5-ACI-1F-05, 5-ACI-1F-05, 5-ACI-1F-05, 5-ACI-1F-05, and 5-ACI-1F-05.

III. Definitions: None.

IV. Statement of Policy and Applicable Procedures:

A. The Georgia Department of Corrections shall maintain perpetual and up-to-date accountability of all hardware and software (including licenses), including methods of procurement, identification, utilization, and maintenance, and shall include all staff and offender technology assets. In the case of shared resource situations among two or more entities within Georgia state government, the hosting agency shall be responsible for this accountability.

This policy is designed to align with the security controls and best practices outlined in NIST Special Publication 800-53 Revision 5 for Security and Privacy Controls for Federal Information Systems and Organizations (FISMA). By following this policy, the organization can demonstrate its commitment to robust IT asset management and information security.

This policy applies to all IT assets owned, leased, or used by the organization, including:

1. Hardware (desktops, laptops, servers, mobile devices, etc.)
2. Software (operating systems, applications, firmware, etc.)
3. Network devices (routers, switches, firewalls, etc.)
4. Peripheral devices (printers, scanners, etc.)
5. Cloud-based resources (storage, software as a service [SaaS], etc.)

All assets shall be recorded in compliance with all applicable state and agency asset management policies and Georgia law. The OA/TPOC for each department shall be responsible for conducting a quarterly audit of all assets assigned to that department.

B.

C. Asset management shall include procedures for accountability throughout the asset's lifecycle from acquisition to decommission, transfer of ownership, surplus, and/or equipment refresh/upgrades.

D. The asset management process shall be reviewed annually during the budgeting process. Any exception to the asset management process shall be approved by the Chief Information Officer (CIO) or his designee.

E. All assets shall be assigned to the appropriate department. Upon transfer of an employee to a new location, a Property Transfer Form shall be submitted to the Office of Information Technology (OIT) to update billing, upon approval of the losing entity.

F. IT Asset Management Responsibilities:

1. ***R* = *Responsible* -** Those who do the work to complete the task. There is at least one role with a participation type of *responsible*, although others can be delegated to assist in the work required.

2. ***A* = *Accountable:*** The one ultimately answers for the correct and thorough completion of the deliverable or task, the one who ensures the prerequisites of the task are met and who delegates the work to those *responsible*. There **must** be only one *accountable* specified for each task or deliverable.

3. ***C* = *Consulted:*** Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.

4. ***I* = *Informed:*** Those who are kept up to date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Roles	GDC/OIT	GETS/GTA
Tasks		
IT Asset Inventory (Non-	A	C

GETS Assets)		
IT Asset Inventory (GETS Assets)	R	A
Asset Acquisition (Non-GETS Assets)	A	I
Asset Acquisition (GETS Assets)	C	A
IT Access Control	A	R
IT Asset Use	A	C
IT Asset Disposal (Non-GETS Assets)	A	I
IT Asset Disposal (GETS Assets)	R	A

5. **GDC Senior Management:** Foster a culture of IT asset accountability and provide adequate resources for effective IT asset management.

6. **GDC OIT:** Develop and implement IT asset management procedures, maintain the IT asset inventory, and ensure compliance with this policy.

7. **Employees:** Report any changes or issues related to their assigned IT assets to the IT department promptly.

G. IT Asset Inventory:

A comprehensive and accurate inventory of all IT assets will be maintained. This inventory will include details like:

1. Asset type (hardware, software, etc.).

2. Manufacturer and model.

3. Serial number.

4. Acquisition date.

5. Assigned user or department.

6. Location.
7. Ownership status (owned, leased, etc.).

8. Security classification.

H. IT Asset Acquisition:

1. All IT asset acquisitions must be approved by the designated authority and documented within the IT asset inventory in each department.

2. Acquisitions will consider factors like organizational needs, security requirements, and budget constraints.

3. Though it is GDC's responsibility to validate inventory, it is the responsibility of the GTA vendor to enter and maintain records in the statewide CMDB.

I. IT Asset Control:

1. Access to IT assets will be granted based on the principle of least privilege, ensuring authorized users only have access to the resources they need for their job functions.

2. Strong password policies will be enforced for all IT assets.

3. Physical security measures will be implemented to safeguard IT assets from unauthorized access.

J. IT Asset Use:

1. IT assets shall be used only for authorized business purposes.

2. The installation of unauthorized software or hardware on IT assets is strictly prohibited. All software and hardware purchases must be approved by the agency CIO or their Designee.

J. IT Asset Disposal:

1. A documented process will outline the proper procedures for disposing of IT assets at the end of their useful life.
   - Decommissioning of GDC purchased assets will follow all DOAS surplus rules for all computing devices
   - Decommissioning of assets for vendor owned equipment will follow all GETS procedures for removal.
   -

2. Data sanitization will be performed on all IT assets before disposal to prevent unauthorized access to sensitive information.

K. Non-Compliance:

Failure to comply with this policy will result in disciplinary action, up to and including termination of employment.

V. <u>Attachments</u>:

<u>Attachment 1</u>- Georgia Department of Corrections Transfer Form

VI. <u>Record Retention of Forms Relevant to this Policy</u>: None.