GEORGIA DEPARTMENT OF CORRECTIONS **Standard Operating Procedures**		
Policy Name: Audit and Accountability		
Policy Number: 105.22	**Effective Date:** 1/8/2021	**Page Number:** 1 of 4
Authority: Commissioner	**Originating Division:** Executive Division (Office of Information Technology)	**Access Listing:** Level I: All Access

I. Introduction and Summary:

This SOP addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Audit and Accountability (AU) family of controls as documented in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

This policy and related procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. The Department of Corrections risk management strategy is a key factor in establishing policy and procedures.

Scope:

This policy and related procedures apply to all GDC employees, contractors, and all other users of GDC information and information systems that support GDC operations and assets.

This policy and related procedures are applicable to all GDC information and information systems used, managed, or operated on behalf of GDC by a contractor or another organization.

Violations:

A violation of any policy, standard, or procedure contained herein may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Other Department of Corrections divisions may adopt security requirements in accordance with this policy at a minimum or, if necessary, a more stringent division specific policy in compliance with division and business-related directives, laws, and regulations.

II. Authority:

A. Georgia Technology Authority: Enterprise Policies, Standards, and Guidelines – PS-08005 Enterprise Information Security Charter;

B. Criminal Justice Information Services (CJIS) Security Policy, Version 5.5 CJISD-ITSDOC-08140-5.5, 06/01/2016;

C. NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013, January 2012; and

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

III. Definitions: None

IV. Statement of Policy and Applicable Procedures:

Note: Procedures specific to information technology may be confidential and are securely stored elsewhere, available only to authorized individuals.

AU-1 AUDIT AND ACCOUNTABILITY

The Information Security Officer (ISO), under direction of the Chief Information Officer (CIO) and in coordination with the Office of Information Technology (OIT), shall:

a. Develop, document, and disseminate:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Review and update the current:

1. Audit and accountability policy annually; and

2. Audit and accountability procedures annually.

AU-2 AUDIT EVENTS

The Systems Architect (SA) shall:

a. Determine which events the information system is capable of auditing;

b. Coordinate the security audit function to enhance support and help guide the selection of auditable events;

c. Provide a rationale for why the auditable events are deemed to be adequate to support after the fact investigations of security incidents; and

d. Determine which events are to be audited within the information system along with the frequency of auditing for each identified event.

A-2(1) AUDIT EVENTS | REVIEWS AND UPDATES

The System Owner (SO) shall review and update the audited events weekly.

AU-3 CONTENT OF AUDIT RECORDS

The SA shall ensure that the information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

AU-3(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

The SA shall ensure that the information system generates audit records containing all additional information required by the agency.

AU-3(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

The SA shall ensure provision of centralized management and configuration of the content to be captured in audit records.

AU-4 AUDIT STORAGE CAPACITY

The SA shall ensure the allocation of audit record storage capacity sufficient to meet all agency storage requirements.

AU-5 AUDIT RECORD RETENTION

The SA shall ensure that audit records are retained consistent with the records retention policy to provide support for after the fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

V. Attachments: None.

VI. Record Retention of Forms Relevant to this Policy: None.