GEORGIA DEPARTMENT OF CORRECTIONS **Standard Operating Procedures**		
Policy Name: Maintenance		
Policy Number: 105.28	**Effective Date:** 11/12/2020	**Page Number:** 1 of 3
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 Maintenance (MA) 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.

A. 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.

B. 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.

A. MA-1 System Maintenance Policy and Procedures:

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

1. Develop, document, and disseminate:

   a. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

2. Review and update the current:

a. System maintenance policy annually; and

b. System maintenance procedures annually.

B. MA-2 Controlled Maintenance:

The System Architect (SA) shall:

1. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; and

2. Explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

V. Attachments: None.

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