GEORGIA DEPARTMENT OF CORRECTIONS

Standard Operating Procedures

Policy Name: Program Management		
Policy Number: 105.20	**Effective Date:** 11/12/2020	**Page Number:** 1 of 8
Authority: Commissioner	**Originating Division:** Executive Division (Office of Information Technology)	**Access Listing:** Level I: All Access

I. Introduction and Summary:

This policy addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Program Management (PM) 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 Georgia Department of Corrections (GDC) risk management strategy is a key factor in establishing policy and procedures.

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, 45 C.F.R. Part 164.

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.

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.

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 GDC 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.

A. PM-1 Information Security Program Plan:

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 and disseminate an organization-wide information security program plan that:

    a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

    b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

c. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and

d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

2. Review the organization-wide information security program plan annually;

3. Update the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

4. Protect the information security program plan from unauthorized disclosure and modification.

B. PM-2 Senior Information Security Officer:

The CIO shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

C. PM-3 Information Security Resources:

The ISO, in coordination with the CIO, shall:

1. Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

2. Employ a business case to record the resources required; and

3. Ensure that information security resources are available for expenditure as planned.

D. PM-4 Plan of Action and Milestones Process:

The ISO shall:

1. Implement a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:

    a. Are developed and maintained;

    b. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

    c. Are reported in accordance with requirements.

2. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

E. PM-5 Information System Inventory:

The Manager of Technical Services, in coordination with the ISO, shall develop and maintain an inventory of its information systems.

F. PM-6 Information Security Measures of Performance:

The ISO shall: develop, monitor, and report on the results of information security measures of performance.

G. PM-7 Enterprise Architecture:

The Systems Architect (SA), in coordination with the ISO, shall develop an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

H. PM-8 Critical Infrastructure Plan:

The ISO, in coordination with the SA, shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

I. PM-9 Risk Management Strategy:

The ISO shall:

1. Develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;

2. Implement the risk management strategy consistently across the organization; and

3. Review and update the risk management strategy annually, or as required to address organizational changes.

J. PM-10 Security Authorization Process:

The ISO shall:

1. Manage (i.e., document, track, and report) the security state of organizational

information systems and the environments in which those systems operate through security authorization processes;

2. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

3. Fully integrate the security authorization processes into an organization-wide risk management program.

K. PM-11 Mission/Business Process Definition:

The ISO shall:

1. Ensure mission/business processes are defined with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

2. Determine information protection needs arising from the defined mission/business processes and revise the processes as necessary, until achievable protection needs are obtained.

L. PM-12 Insider Threat Program:

The ISO shall implement an insider threat program that includes a cross-discipline insider threat incident handling team.

M. PM-13 Information Security Workforce:

The ISO shall establish an information security workforce development and improvement program.

N. PM-14 Testing, Training, And Monitoring:

The ISO, in coordination with the Systems Architect, shall:

1. Implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:

    a. Are developed and maintained; and

    b. Continue to be executed in a timely manner;

2. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

O. PM-15 Contacts with Security Groups and Associations:

The ISO, SA, and CIO shall:

1. Establish and institutionalize contact with selected groups and associations within the security community:

    a. To facilitate ongoing security education and training for organizational personnel;

    b. To maintain currency with recommended security practices, techniques, and technologies; and

    c. To share current security-related information including threats, vulnerabilities, and incidents.

P. PM-16 Threat Awareness Program:

The ISO, in coordination with the CIO, shall implement a threat awareness program that includes a cross-organization information-sharing capability.

V. **<u>Attachments</u>:** None.

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