GEORGIA DEPARTMENT OF CORRECTIONS **Standard Operating Procedures**		
Policy Name: Information Security		
Policy Number: 105.02	**Effective Date:** 1/11/2021	**Page Number:** 1 of 11
Authority: Commissioner	**Originating Division:** Executive Division (Office of Information Technology)	**Access Listing:** Level I: All Access

I. Introduction and Summary:

A. The Georgia Department of Correction (GDC) shall maintain a strong information security position through the application of security controls, data ownership responsibilities, and maintenance of the security infrastructure. This policy articulates requirements that assist in defining a framework that establishes a secure environment. This framework provides the overarching structure for safeguarding information technology assets, and ensuring the confidentiality, integrity and availability of sensitive data.

B. The GDC has the responsibility to have controls in place and in effect that provide reasonable assurance that security objectives are adequately addressed. The Information Security Officer (ISO) has the responsibility to exercise due diligence in the adoption of this framework. The GDC must achieve compliance with the overall information security goals of the Agency including compliance with laws, regulations, policies, and standards to which agency technology resources and data are subject.

C. This policy applies to:

1. All GDC data, systems, activities, and assets owned, leased, controlled, or used by GDC, its agents, contractors, or other business partners on behalf of GDC;

2. All GDC employees, contractors, sub-contractors, and their respective facilities supporting GDC business operations, wherever GDC data is stored or processed, including any third party contracted by GDC to handle, process, transmit, store, or dispose of GDC data;

3. All business partners that access GDC information technology assets or shared environments; and

4. All third parties in any aspect of the process of providing goods and services to the agency. These include, but are not limited to, electronic data collection, storage, processing, disposal, dissemination, and maintenance.

D. Violations:

1. Any user of GDC information technology assets found to have violated any policy, standard, or procedure 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.

E. Other GDC divisions are encouraged to adopt security requirements in accordance with the GDC Information Security Policy at a minimum, or 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-08- 005 Enterprise Information Security Charter;

B. Criminal Justice Information Services (CJIS) Security Policy, Version 5.5 CJISD-ITS- DOC-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;

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

E. ACA Standards: 2-CO-1F-06, 5-ACI-1F-02 (ref. 4-4100), and 5-ACI-1F-03 (ref.

4-4102).

III. <u>Definitions</u>: None.

IV. <u>Statement of Policy and Applicable Procedures</u>:

A. The GDC shall implement policies, associated procedures and controls that protect the agency's information assets from all internal and external threats, whether deliberate or accidental. All sensitive or confidential data, whether contained in paper, physical, or media format will be protected throughout collection, storage, retrieval, access, use, and transmission processes. In addition to the guiding principles of information security (confidentiality, integrity, and availability), the agency must review the overall implementation of security controls against all applicable laws, regulations, policies, standards, and associated risks.

1. Information Security Management Program: The GDC shall implement an Information Security Program (ISP) that represents the policies and controls implemented within the organization. The ISP shall provide both management and users with a detailed understanding of the goals, approach, and implemented controls for securing the organization's information assets, including, but not limited to, sensitive information, and must address the ISP lifecycle including risk assessment, risk treatment, selection and implementation of security controls, and ongoing evaluation and maintenance.

2. Risk Assessment: The GDC shall identify, quantify, and prioritize risks against operational and control objectives, and design, implement, and exercise controls that provide reasonable assurance that objectives will be met, and that risk will be managed to an acceptable level.

    a. Risk assessments shall include at a minimum:

        i. Identification of risk factors: Evaluation of risk by considering the

potential threats to the information and to information technology assets, including:

1) Loss of data or systems due to accident or malicious intent;

2) Loss of availability, such as data or systems being unavailable for an unacceptable length of time; and

3) Unknown changes to the data or systems rendering the information no longer reliable.

ii. Identification of threat**:** Evaluation of impact and likelihood of potential threat, including:

1) Cost if each threat actually occurred. Costs shall be interpreted broadly to include money, resources, time, and loss of reputation among other factors; and

2) Evaluation of the probability of each threat occurring.

3. Risk Treatment: The Department of Corrections shall monitor and evaluate the specific controls that must be implemented to meet the stated security objectives. This process must identify which security controls shall be or are implemented and identify and justify which security controls are not deemed necessary or applicable.

4. Statement of Applicability: The Statement of Applicability shall list the Agency's information security control objectives, controls and adopted policies that are relevant and applicable to the agency's Information Security

Program. The Agency shall maintain a statement of applicability for all data

and information technology assets. Specific information security objectives and controls, including document sources and details, shall be defined within the Statement of Applicability document.

5. Security Policy, Policy Adoption and Documentation Review: The GDC shall adopt and document a comprehensive information security program consisting of a granular set of policies based on an evaluation of business drivers.

    a. The GDC shall review the ISP annually at a minimum. The purpose of the review is to ensure the continued suitability, adequacy and effectiveness of the policies. The ISP may require review on a more frequent basis, particularly if significant changes occur within the Agency that may have an impact on the effectiveness of the policy. Divisions should inform the Office of Information Technology (OIT) of any policy related changes that are necessary but conflict with current agency security policies.

    b. Changes to the components of the ISP shall be subject to appropriate review and approval and shall be adequately documented.

6. Organization of Information Security: The GDC shall maintain the security of the agency's data and information processing facilities that are accessed, processed, communicated to, or managed by employees and contractors (staff) and third parties by:

    a. Documenting the specific responsibilities of staff and third parties; and

    b. Ensuring that all applicable contractual agreements incorporate and support the security-based requirements.

7. Asset Management: The GDC shall achieve and maintain appropriate protection of data and information technology assets by assigning the

responsibility to implement controls for achieving:

a. Inventory of information technology related assets;

b. Data classification;

c. Appropriate tagging and data handling per classification; and

d. Acceptable use via implementation and enforcement of an Acceptable Use Policy.

8. Human Resources Security: The GDC shall ensure that employees, contractors, and third-party users understand their security responsibilities and have the requisite skills and knowledge required for effectively executing their assigned roles. In order to reduce the risk of unauthorized access, use or modification of data or information technology assets (theft, fraud, or misuse of facilities), these security responsibilities shall include, but are not limited to:

   a. Risk assessment to determine applicable level of employee screening prior to and upon change in responsibility during employment;

   b. Security awareness and training during employment;

   c. Disablement of access rights to data systems after an extended period of inactivity;

   d. Return of agency issued equipment and/or devices upon termination or change of employment; and

   e. Removal of access rights upon termination of employment.

9. Physical and Environmental Security: The GDC shall secure against unauthorized physical access or damage to, or interference with, the agency's premises and information technology assets, including data, by implementing:

    a. Workforce security;

    b. Facility access controls of information technology assets;

    c. Equipment security;

    d. Least privilege;

    e. Visitor control; and

    f. Secure disposal or reuse of equipment.

10. Communications and Operations Management: The GDC shall implement procedures for managing system activities associated with access to data and information systems, modes of communication, and information processing by implementing:

    a. Controls for securing removable media;

    b. Data backup procedures;

    c. Data collection and secure disposal of data;

    d. Monitoring of system use;

    e. Audit logging;

f. Protection of log information, including administrator and operator logs;

g. Fault logging;

h. Antivirus;

i. Network controls;

j. Clock synchronization; and

k. Network management controls.

11. Access Control: The GDC shall protect applications, data, and information technology assets and infrastructure against improper or unauthorized access that could result in compromise of confidentiality, integrity or availability of data or information technology assets. Access control rules shall take into account the existing agency policies for information dissemination and authorization.

12. Information Systems Acquisition Development and Maintenance: The GDC shall ensure that information security is an integral component of information technology assets from the onset of the project or acquisition through implementation:

    a. Application and system security;

    b. Configuration management;

    c. Change control procedures;

    d. Encryption and key management; and

e. Software maintenance including, but not limited to, upgrades, antivirus, patching and malware detection response systems.

13. Information Security Incident Management: The GDC shall implement management controls that result in a consistent and effective approach for addressing incidents including:

    a. Incident reporting procedures;

    b. Staff roles and responsibilities for incident response and management;

    c. Incident investigation procedures;

    d. Incident remediation and closure procedures; and

    e. Post-incident review and action planning procedures that focus on preventing future reoccurrences.

14. Business Continuity Management: The GDC shall document, implement and annually test plans, including the testing of all appropriate security provisions, to minimize impact to systems or processes from the effects of major failures of information technology assets or disasters via adoption of a:

    a. Disaster recovery plan; and

    b. Continuity of operations plan.

15. Compliance**:** The GDC shall implement the security requirements of this policy in addition to any state or federal law, regulatory, and/or contractual obligations to which agency data or information technology assets are subject, including but not limited to:

a. Security and privacy of personal information;

b. Patent, copyright, and trade secret protection;

c. Documented plans for all audit requirements and activities for information systems and assets, as appropriate;

d. Results of self-audits conducted at a minimum of annually; and

e. Compliance with security policies and standards.

16. Roles and Responsibilities: The roles and responsibilities associated with implementation of, and compliance with, this policy are as follows:

    a. Information Security Officer (ISO) and Chief Information Officer (CIO): The ISO and CIO are responsible for exercising due diligence in adoption of this framework to meet the obligations of the Department of Corrections by ensuring that adequate security controls are in place and in effect to promote reasonable assurance of security control objectives that safeguard the information assets including, but not limited to, sensitive data.

        i. Ensure that all information systems and applications developed conform to this and all related agency information technology policies, standards, and procedures. Non-conforming information systems or applications shall not be deployed unless the purchasing entity and their contractor have jointly applied for and received approval in writing from the ISO or designee for a specified variance.

        ii. Provide communication, training and enforcement that support the security goals of the agency.

iii. Provide proper third-party oversight as applicable for any information systems and applications.

iv. Review and sign all agency security programs, plans, self-audits, and reports.

v. The CIO shall be responsible for ensuring compliance with all applicable laws, regulations, and contractual obligations.

vi. The CIO shall be responsible for signing off on the agency's acceptable risk level for meeting information security objectives.

b. Information Security Officer (ISO):

i. Ensure that the goals and requirements of the Information Security Program are implemented and met.

ii. Maintain all required documentation as specified in information technology policies, standards, and procedures.

iii. Conduct self-audits at a minimum annually, documenting reasonable assurance that compliance with information technology policies, standards, and procedures has been achieved.

iv. Coordinate the GDC's compliance with the requirements of applicable executive orders, federal and state laws and regulations, OIT security standards and policies, and security-related contractual requirements.

v. Recommend revisions and updates to this policy and related standards.

vi. Manage the variance process and provide recommendations to the

Chief Information Officer (CIO) for approval.

vii. Develop security policies, standards, and guidelines.

viii. Act in a consultative capacity to the Office of Information Technology (OIT) and the agency.

c. Office of Information Technology (OIT):

i. Establish, adopt, and implement agency-wide policies and standards as determined by the Information Security Officer in support of the agency's information security goals including:

1) Continuous testing and monitoring of the environment;

2) Providing ongoing education and outreach; and

3) Consult with agency divisions and the Georgia Technology Authority (GTA) on the planning and deployment of IT assets.

d. Third Parties:

i. Ensure that all information systems and applications developed by or for the GDC or operating within the agency network conform to this and other applicable information technology policies, standards, and procedures. Non-conforming information systems or applications shall not be deployed unless the purchasing entity and their contractor have jointly applied for and received approval in writing from the ISO or designee for a specified variance.

V. Attachments: None.

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