GEORGIA DEPARTMENT OF CORRECTIONS **Standard Operating Procedures**		
Policy Name: Incident Response		
Policy Number: 105.27	**Effective Date:** 10/14/2022	**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:

This SOP addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the Incident Response (IR) 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 Department of Corrections 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 Department of Corrections 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 5.9 CJISD-ITSDOC-08140-5.9, 06/01/2020.

C. NIST 800-53 Rev. 5, Recommended Security Controls for Federal Information Systems and Organizations, September 2020; and

D. HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Parts 160 and 164, March 2013.

III. Definitions:

Cybersecurity Incident - An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

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.

IR-01: INCIDENT RESPONSE

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

1. Develop, document, and disseminate:

a. An incident response policy that addresses purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance; and

b. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

2. Review and update the current:

a. Incident response policy annually; and

b. Incident response procedures annually.

IR-02: INCIDENT RESPONSE TRAINING

A. The ISO, shall:

1. Provide incident response training to information system users consistent with assigned roles and responsibilities:

a. Within thirty (30) days of assuming an incident response role or responsibility.

b. When required by information system changes; and

c. Annually thereafter.

IR-02(1): INCIDENT RESPONSE TRAINING | SIMULATED EVENTS

A. The Infrastructure Lead and ISO, shall:

1. Incorporate simulated events into incident response training to facilitate effective response by personnel in crises.

IR-02(2): INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

A. The Infrastructure Lead and ISO, shall:

1. Employ automated mechanisms to provide more thorough and realistic incident response training.

IR-03: INCIDENT RESPONSE TESTING

A. The Infrastructure Lead and ISO, shall:

1. Test the incident response capability for the information system annually to determine the incident response effectiveness and document the results.

IR-03(1): INCIDENT RESPONSE TESTING

A. The ISO, shall:

1. Coordinate incident response testing with organizational elements responsible for related plans.

IR-04: INCIDENT HANDLING

A. The ISO shall:

1. Implement an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery.

2. Coordinate incident handling activities with contingency planning activities; and

3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

IR-05: INCIDENT REPORTING

A. Users shall:

1. All potential Cybersecurity Incidents either from an internal or an external source should be reported to GDC_InfoSec@gdc.ga.gov.

B. The ISO shall:

1. Ensure an incident response report is completed and provided to the CIO.

2. The incident is reported and tracked in GETS ServiceNow portal.

IR-06: INCIDENT RESPONSE ASSISTANCE

A. The ISO shall:

1. Provide an incident response resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IR-07: INCIDENT RESPONSE PLAN

A. The ISO shall:

1. Develop an incident response plan that:

   a. Documents the definition of a Cybersecurity Incident.

   b. Documents Cybersecurity Incident classification and severity for Cybersecurity Incidents.

   c. Documents how incidents are tracked.

d. Documents its Cybersecurity Incident Response Team (CIRT) roles and responsibilities.

e. Documents its Incident Handling Team (IHT) roles and responsibilities.

f. Documents applicable contact information for those listed in the cyber incident response plan (CIRP).

g. Documents its notification and communication capabilities in its CIRP. This should include details on how to communicate to law enforcement and/or customers.

h. Defines GDC's cybersecurity response capabilities.

i. Defines GDC's incident escalation tactics.

j. Includes lessons learned from incidents as appropriate.

k. Provides metrics for measuring the incident response capability within the organization.

l. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

m. Is reviewed and approved by the CIO.

2. Distribute copies of the incident response plan to incident response personnel.

3. Review the incident response plan annually.

4. Update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

5. Communicate incident response plan changes to incident response personnel; and

6. Protect the incident response plan from unauthorized disclosure and modification.

V. Attachments: None.

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