GEORGIA DEPARTMENT OF CORRECTIONS **Standard Operating Procedures**		
Policy Name: Telecommunications		
Policy Number: 105.04	**Effective Date:** 00/00/2024	**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 Telecommunications planning and management as documented in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, 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 (GDC) risk management strategy is a key factor in establishing policy and procedures.

A. Scope:

The scope of this policy includes all telecommunications assets governed by the Georgia Department of Corrections. All personnel and service providers who have access to or utilize information assets of the Agency, including data at rest, in transit or in process shall be subject to these requirements. This Policy applies to all information assets operated by the Agency; all information assets provided by the Agency through contracts, subject to the provisions and restrictions of the contracts; and all authenticated users of Georgia Correctional Industries information assets. This includes, but is not limited to:

1. Company issued mobile phones, tablets, and laptops;
2. Voice Over Internet Protocol (VOIP) systems;
3. Email and messaging platforms;
4. Fax Machines;
5. Video Conferencing Systems; and
6. Public Switch Telephone Networks (PTSN).

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 5.9.4, 12/01/2023;

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

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. TC-1 Telecommunications Control 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 telecommunications control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    b. Procedures to facilitate the implementation of the telecommunications control policy and associated controls;

2. Review and update the current:

    a. Telecommunications control policy annually; and

    b. Telecommunications control procedures annually.

B. TC-2 Data Security.

The System Owner (SO) shall:

1. Ensure sensitive data at rest and in transit is secure for all GDC personnel, contractors, and offenders.

2. Implement appropriate data classification procedures to identify and safeguard sensitive data.

3. Dispose of electronic media containing telecommunications securely.

C. TC-3 Network Security.

The System Architect (SA) shall:

1. Keep all telecommunications software and firmware updated with the latest security patches.

2. Segment the network to isolate critical systems and data from external sources.

3. Segment the network to isolate managed offenders from unapproved/unrestricted network access.

4. Utilize firewalls and intrusion detection and prevention systems to monitor and protect telecommunications network from unauthorized access and malicious activity.

D. TC-4 Physical Security:

The System Owner shall:

1. Secure physical access to telecommunication equipment and infrastructure to prevent unauthorized access and tampering of GDC information systems.

2. Configure and provide updates to telecommunications equipment and user devices to ensure latest security updates.

V. **Attachments:** None.

VI. **Record Retention of Forms Relevant to this Policy:** None.
Any records??????Even electronic subject to this SOP.