	Georgia Technology Authority	
Title:	**Use of Cryptography**	
PSG Number:	**PS-08-024**	
Effective Date:	03/20/2008	**Review Date:** 12/01/2023
Synopsis:	Establishes the requirement to use cryptographic controls on State information systems as necessary	

PURPOSE

Cryptography is a discipline that embodies principles, means and methods for providing several security services: confidentiality, data integrity, authentication and non-repudiation.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(21) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Charter*

TERMS AND DEFINITIONS

Cryptography - a branch of applied mathematics concerned with encrypting and decrypting data such that the sender's identity (authentication and non-repudiation), data confidentiality or integrity can be assured.

- **Encryption** is the process of converting ordinary information (plaintext) into unintelligible character strings (i.e., *ciphertext*).
- **Decryption** is the reverse, moving from unintelligible ciphertext to plaintext.
- A **cipher** (or *cypher*) is a pair of algorithms that perform this encryption and the reversing decryption.

Non-Repudiation - a service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party.
Authentication - a process that establishes the origin of information or determines an entity's identity.

POLICY

Agencies shall use cryptographic controls where the confidentiality, authenticity, non-repudiation or integrity of data is categorized as MODERATE or higher or when the risk of compromise or exposure is higher than acceptable or when required by policy, law, or regulation, and other compensating controls are insufficient to meet the required security levels.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Cryptographic Controls (SS-08-040)

REFERENCES

NIST SP 800-12 An Introduction to Information Security (nist.gov)

NIST SP 800-175A Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and PoliciesCrypto key management

NIST SP 800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

NIST Cryptographic Key Management | CSRC (nist.gov)

FIPS 140-2 Security Requirements for Cryptographic Modules *FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov)*