Encryption Standard

Rev 1.3

Type of Standard: Administrative
Effective Date: November 2016
Last Revised: November 2016

Standard Owner: Georgia Tech Cyber Security
Standard Contact: Blake Penn, Information Security Standard and Compliance Manager, blake.penn@security.gatech.edu

1. Executive Summary

This document is in direct support of the Georgia Institute of Technology Data Access Policy. The standard sets forth the requirements for encrypting Sensitive Data and Highly Sensitive Data as defined in the Data Access Policy. By implementing an encryption standard, Georgia Tech can provide for the protection of sensitive data by preserving the confidentiality, integrity, and authenticity of the data. In addition, this document is meant to provide a standardized solution that can be applied across all units.

2. Scope

This Institute-wide standard applies to all hardware, media and/or software that store, process, or transmit Sensitive or Highly Sensitive Data.

3. Definitions

Cryptography	This is the practice or study of hiding information. That is, devising a way to encrypt information.
Key Management	The management of cryptographic keys including dealing with the generation, exchange, storage, use, and replacement of keys.

4. Standard

The following statement applies to all Georgia Tech account holders and users of Georgia Tech IT (Information Technology) resources including but not limited to students, applicants, faculty, affiliates, staff and contractors.

Sensitive and Highly Sensitive data must be protected both during storage and transmission with NIST Special Publication 800-175B (NIST SP 800-175B) compliant cryptography and must adhere to the key management practices in that standard.

5. Recommended Technology for Storage of Sensitive or Highly Sensitive Data.

Platform	Technology
Microsoft Windows	BitLocker
Apple Macintosh	FileVault2
Linux	dm-crypt/LUKS

6. Recommended Technology for Transmission of Sensitive or Highly Sensitive Data.

Technology
HTTPS
Secure Shell (SSH)
Internet Protocol Security (IPsec)

7. Related Information

Resource	Link
Georgia Tech Data Access Policy	http://www.policylibrary.gatech.edu/information-technology/data-access
Georgia Tech Data Protection Safeguards	https://security.gatech.edu/sites/default/files/data-protection-safeguards-rev2.0-20140314.pdf
NIST SP 800-175B	http://dx.doi.org/10.6028/NIST.SP.800-175B

8. Revision History

Revision Number	Author	Description
1.0	Richard Biever	Initial Draft
1.1	Richard Biever	Review/Changes from ITAC
1.2	Jimmy Lummis	Initial Release
1.3	Blake Penn	Update to follow NISP SP 800-175B