Augusta University
Policy Library

Encryption Policy
Policy Manager: Chief Information Officer

1.0 POLICY STATEMENT
Augusta University is committed to protecting the confidentiality, integrity, and availability of organizational data in support of its academic, research, clinical, and administrative missions. Encryption is a critical safeguard used to protect organizational data from unauthorized access, disclosure, alteration, or loss.

This policy mandates the use of strong, industry-standard encryption to protect the organization's data across all systems and services. This policy outlines when encryption must be used and the approved mechanisms to apply encryption that align with recognized information security frameworks. Encryption shall be implemented in accordance with applicable federal and state laws, regulatory requirements, contractual obligations, and recognized security standards.

This policy adheres to or exceeds the standards found in the *University System of Georgia (USG) IT Handbook*.

2.0 AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☐ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☐ Other:

3.0 DEFINITIONS
Refer to the *Cybersecurity Charter, Appendix B* for all applicable definitions. This can be found online in the Augusta University Policy Library..

Encryption: Encryption is the process of converting plaintext data into unreadable ciphertext through cryptographic techniques, ensuring data confidentiality and security during transmission or storage. It relies on encryption algorithms and keys. Symmetric encryption employs a single secret key for both encryption and decryption. AES (Advanced Encryption Standard) is a prominent symmetric algorithm, with variations of 128, 192, or 256 bits, securing data efficiently. Asymmetric Encryption, also known as public-key encryption, is used with key pairs, public (shared openly) and private (kept secret). RSA and ECC (Elliptic Curve Cryptography) are examples. RSA handles secure communication, digital signatures, and key exchange. ECC offers strong security with shorter key lengths, useful for resource-constrained systems. These encryption methods underpin secure communication, data protection, and privacy across various digital platforms and applications.

Hashing: One-way cryptographic process that transforms data of any size into a fixed-length, unique output, called a hash or digest, using a mathematical algorithm, designed so the original data cannot be reconstructed from the hash.

Keys: A string of bits used by a cryptographic algorithm to transform data, such as encrypting plaintext into ciphertext or decrypting ciphertext back into readable form.

Secrets: Sensitive pieces of authentication or authorization data that provide access to systems, applications, services, or encrypted information. They must always remain confidential because anyone who obtains a secret can impersonate a user, service, or system. Secrets typically include passwords, API keys, tokens, private keys, certificates, cryptographic keys, connection strings, and other credentials used to verify identity or establish trust between systems.

4.0 SCOPE

This policy applies to all organizationally managed and owned technologies accessing organizational data, including but not limited to, information systems, applications, databases, networks, and cloud environments. Organizational data consists of any data requiring protection, to include but not limited to, AU proprietary data and data classifications as identified in the *Data Management and Classification Policy*.

5.0 ROLES AND RESPONSIBILITIES

5.1 All workforce members:

- 5.1.1 Must use encryption technology in accordance with this policy.
- 5.1.2 Report any suspected violations or non-compliance with this policy to AU Cyber Defense or 72CYBER@augusta.edu.

5.2 The Division of Information Technology (IT):

- 5.2.1 Identify and establish the encryption standards for the organization.
- 5.2.2 Ensure all organizational technology is securely configured and managed per the standards outlined in this policy.
- 5.2.3 Implement and conduct continuous monitoring for misconfigurations or misalignment to the standards outlined in this policy.

5.3 Vendors/Contractors:

- 5.3.1 Ensure any associated technologies accessing organizational resources or data adhere to or exceed the standards outlined in this policy.
- 5.3.2 Must provide attestation documentation demonstrating adherence to the standards outlined in this policy.

6.0 REQUIREMENTS

6.1 Encryption Requirements

- 6.1.1 Data-at-rest stored on servers, endpoints, mobile devices, removeable media, and cloud storage must be encrypted in accordance with industry standards, compliance requirements, and organizationally defined configuration standards. This includes the current standards for symmetric encryption, asymmetric encryption, and hashing.
- 6.1.2 Data-in-transit transmitted over internal or external networks must use secure cryptographic protocols in accordance with current industry standards, compliance requirements, and organizationally defined configuration standards. This includes any form of data transmission where data moves from one technology to another, network-level encryption, and communication between web applications.

6.1.3 Unencrypted, insecure, or unsupported protocols and algorithms, such as file transfer protocol (FTP), telnet, hypertext transfer protocol (HTTP), and simple mail transfer protocol (SMTP) without transport layer security (TLS), are prohibited unless encapsulated within an approved secure tunneling mechanism.

6.1.4 Passwords must be hashed in accordance with current industry standards. Secrets must be encrypted at-rest.

6.2 Key Management Requirements

6.2.1 Keys must be generated using mechanisms in accordance with current industry standards.

6.2.2 Keys must never be stored in plaintext and must be managed in accordance with current industry standards.

6.2.3 Keys must be stored in secure hardware or software vaults such as hardware security modules (HSMs), cloud key management solutions (i.e. Azure Key Vault), and/or encrypted key vaults with strict access controls.

6.2.4 Keys must be rotated in accordance with current industry standards, organizational standards, or immediately upon a suspected compromise.

6.2.5 Session keys must be managed in accordance with current industry standards or organizational standards enforcing secure configurations.

6.2.6 Access to keys must be based on the individual's role and provisioned appropriately. All key access must be logged and monitored, where such mechanisms are supported.

6.3 Implementation Requirements

6.3.1 Application development must follow secure coding practices in accordance with current industry standards. Encryption must be integrated into software development pipelines with automated security testing.

6.3.2 Cloud providers and cloud solutions must support encryption at-rest and in-transit by default.

6.3.3 Encryption controls must be reviewed at least annually.

6.3.4 Automated technology must be utilized to continuously monitor for misconfigurations to encryption. Logs related to encryption events must be retained according to the data retention requirements within the organization.

6.3.5 In the event of a suspected encryption failure or key compromise, incident response procedures in accordance with the *Cybersecurity Incident Response Plan Policy* must be implemented, with organizationally defined activities to address the affected keys and systems.

6.3.6 All vendors and third-party entities handling organizational data are contractually required to maintain encryption practices that align with the standards outlined in this policy.

7.0 COMPLIANCE

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request approval for an exception through the AU Cyber Defense Governance, Risk and Compliance (GRC) Exception to Policy (ETP) process as referenced in Service Now in *Knowledge Base Article Computer Standard Configuration*

Exception Request KB2300201. All approved exceptions shall have a defined expiration date and be reviewed periodically for continued necessity.

Failure to adhere to the conditions outlined in an approved exception to policy may result in revocation of the exception or further sanctions.

Failure to adhere to this policy may result in disciplinary action up to and including termination of employment.

8.0 REFERENCES & SUPPORTING DOCUMENTS

Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules
NIST Cybersecurity Framework (CSF)
NIST Special Publication (SP) 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-77, Guide to IPsec Virtual Private Networks (VPNs)
NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
NIST SP 800-113, Guide to SSL VPNs
NIST SP 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations

University System of Georgia (USG) Information Technology (IT) Handbook
Service Now Knowledge Base Article, KB2300201

9.0 RELATED POLICIES

Cybersecurity Charter Policy
Data Management and Classification Policy
Cybersecurity Incident Response Plan Policy

All AU Policies can be found online at the Augusta University Policy Library.

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/25/2026

President, Augusta University Date: 7/8/2026