AuditScripts

Encryption Security Policy

Version 2.3

EDITED BY KELLI K. TARALA

SECURITY enclave

Encryption Security Policy

Information Assurance Policy (v2.3)

Purpose:

Information assurance policies are created to set universal standards for organizations to facilitate data protection. They also align business goals and strategies with appropriate methods for technically or operationally protecting data. As business owners determine their requirements for protecting data, policies can define the control standards this organization will follow to meet those requirements.

Scope:

This information assurance policy applies to each of this organization's workforce members who have contact or potentially may have contact with this organization's data, applications, and computing resources. Workforce members include, but are not limited to, employees, contractors, vendors, service providers, volunteers, or any others who have or may come into contact with this organization's data, whether in a paid or unpaid capacity. Exceptions to this policy must be properly approved and documented in accordance with this organization's information assurance Control Exception Policy.

Standards References

CIS Critical Controls (v6.1):
10, 11, 13, 14, 15

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-21, 22
NIST SP 800-25, 29
NIST SP 800-32, 57, 111
NIST SP 800-130–133

NIST 800-53 (rev4):
IA-7, MP-4, MP-5, SC-8, SC-9, SC-11, SC-12, SC-13, SC-28

COBIT 5:
APO13, DSS05

ISO 27002:2013:
10.8, 10.9, 12.3

NIST Cybersecurity Framework (v1.0):
Not Applicable

IIA GTAGs:
Not Applicable

PCI DSS (v3.2):
2, 3, 4, 6, 7

HIPAA / HITECH:
164.308(a)(1), 164.308(a)(5), 164.312(a)(1), 164.312(c)(1), 164.312(e)(1)

GDPR:
Not Applicable

Statements:

1. The use of encryption to protect a data asset will be the result of a data classification decision made by the asset's data owners. The requirement to use or not use encryption will be based on the classification level assigned to a data asset. The classification level assigned to a data asset will be based on this organization's Data Classification Policy.
2. Based on the classification level assigned to a data asset, data at rest shall be encrypted in accordance with this organization's Business Applications Security Policy, Data Backup and Archiving Policy, Logging and Monitoring Policy, Mobile Device and Acceptable Use Policy, Network Security Policy, Remote Access Policy, Removable Media Policy, Server Security Policy, Wireless Security Policy, or Workstation Security Policy.
3. Based on the classification level assigned to a data asset, data in transit shall be encrypted in accordance with this organization's Business Applications Security Policy, Data Backup and Archiving Policy, Logging and Monitoring Policy, Mobile Device and Acceptable Use Policy, Network Security Policy, Remote Access Policy, Removable Media Policy, Server Security Policy, Wireless Security Policy, or Workstation Security Policy.
4. The exporting or international use of encryption systems shall be in compliance with all United States federal laws (especially the US Department of Commerce's Bureau of Industry and Security's Export Administration Regulations) or appropriate international laws.
5. Cryptographic private or shared keys, cryptographic secrets, or authentication secrets or hashes will be classified at the highest classification level as outlined by this organization's Data Classification Policy and protected using controls defined at that classification level.
6. This organization will maintain documented procedures for supported cryptographic algorithms, by data classification level, which include documentation of: (a) Acceptable cryptographic key lengths, and (b) Acceptable cryptographic algorithms.
7. All data assets utilizing symmetric encryption algorithms shall only do so utilizing cryptographic keys of 112 bits or longer. Larger key spaces, however, are recommended for longer term security.
8. All data assets utilizing asymmetric encryption algorithms shall only do so utilizing cryptographic keys of 2048 bits or longer. Larger key spaces, however, are recommended for longer term security.
9. Proprietary encryption algorithms are not to be utilized on production systems. Only those cryptographic algorithms that have undergone and passed public examination shall be acceptable for use.
10. Examples of acceptable symmetric cryptographic algorithms that this organization may decide to use for productions include the following: (a) Advanced Encryption Standard (AES), (b) Blowfish, (c) Triple DES, (d) Serpent, (e) Twofish, (f) RC6, and (g) International Data Encryption Algorithm (IDEA).
11. Examples of acceptable asymmetric cryptographic algorithms that this organization may decide to use for productions include the following: (a) Diffie–Hellman (DH); (b) Rivest, Shamir, and Adleman (RSA); (c) Digital Signature Standard (DSS); (d) ElGamal; and (e) Elliptic Curve Cryptography (ECC).
12. This organization will maintain documented procedures for cryptographic key management which include documentation on the processes of: (a) Generating cryptographic keys; (b) Distributing cryptographic keys; (c) Escrowing cryptographic keys; (d) Enabling authorized users to access stored cryptographic keys; (e) Changing and updating cryptographic keys; (f) Revoking cryptographic keys; (g) Archiving cryptographic keys; and (h) Auditing and logging cryptographic key management.
13. All developers and system administrators shall be properly trained and educated on the use and security of the encryption systems they administer in accordance with this organization's Training, Education, and Awareness Policy.

14. Exceptions to this policy shall be managed and maintained by following the processes outlined by this organization's Configuration Management and Change Management Policy and Control Exception Policy.

Assurance:

In order to ensure continued compliance with this policy, this organization will train all workforce members on their responsibilities that align with this policy. This training will consist of an initial education upon affiliating with this organization as well as continued education events on a regular basis in accordance with this organization's standards for training and education.

In addition, this organization shall implement an ongoing audit program. This audit program will adhere to this organization's policies and standards for auditing which shall reflect industry standards, practices, and ethics in this area. All levels of workforce members shall engage in this assurance effort, and they will not be limited to a formal internal audit group. Any workforce member who notices non-compliance with this policy shall notify the appropriate business owners of the deficiencies that exist.

Sanctions:

Any workforce member discovered violating this policy may be subject to disciplinary measures, up to and possibly including termination of employment or breach of contract with this organization. For employees, this disciplinary measure shall be administered by this organization's Human Resources Department in accordance with all human resource policies. For other workforce members, this disciplinary measure may result in a breach of contract or service level with this organization and therefore appropriate sanctions will be applied as per the agreed upon contractual terms by the purchasing representative or business process owner.

Administrative:

The Chief Executive Officer of this organization has the responsibility for the overall administration of this policy. Establishment of the administrative procedures for the compliance with Corporate Policies is the responsibility of the officers and the managers of this organization and its business units.

Definitions:

For further clarification on the terminology and definition of terms used within this document, please refer to this organization's published glossary of terms associated with this document.

Revision History:

Title and Version Number:	Encryption Security Policy
Status and publication date:	In draft
Last Formal Review:	
Superseded Documents:	All local policies
Related Documents:	Business Applications Security Policy Configuration Management and Change Management Policy Control Exception Policy Data Backup and Archiving Policy Data Classification Policy Logging and Monitoring Policy Mobile Device and Acceptable Use Policy Network Security Policy Remote Access Policy Removable Media Policy Server Security Policy Training, Education, and Awareness Policy Wireless Security Policy Workstation Security Policy

Signature:

Prepared By:	Approved By: