Encryption Policy

Information Assurance Policy (v1.0)

These materials are considered to be sensitive and confidential materials and may not be used for any purpose other than the organization’s own internal use. This material may not otherwise be shared, used, reproduced, or disseminated outside of the organization in any way without prior written permission.
Encryption Policy
Information Assurance Policy (v1.0)

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 the organization will follow to meet those requirements.

Specifically an encryption policy is necessary to define how and when encryption will be used in an organization, as well as what encryption standards are acceptable in an organization. This will help to ensure that the organization’s sensitive confidential data remains confidential and protected from unauthorized disclosure.

Scope:
This information assurance policy applies to each of the organization’s workforce members who have contact or potentially may have contact with the organization’s data. This includes, but is not limited to employees, contractors, vendors, service providers, volunteers, or any others who have or may come into contact with the organization’s data, whether in a paid or unpaid capacity. Exceptions to this policy must be properly approved and documented in accordance with the organization’s information assurance exception policy.

Standards
References
NIST 800 Series:
NIST SP 800-21
NIST SP 800-29
NIST SP 800-57
NIST SP 800-111
NIST SP 800-130 – 133

NIST 800-53:
IA-7, MP-4, MP-5, SC-8, SC-9, SC_11, SC-12, SC-13, & SC-28

20 Critical Controls:
3.8, 8.4, 10.6, 12.5, 17.1, & 17.7

COBIT:
Not Applicable

ISO 27000 Series:
27002 – 10.8 & 10.9
27002 – 12.3

Australian DSD Top 35:
Controls #29 & #30

IIA GTAGs:
Not Applicable

PCI DSS:
2.3, 3.2, 3.4, 3.5, 3.6, 4.1, & 6.5

HIPAA / HITECH:
HIPAA 164.310(d)(1)
HIPAA 164.312(a)(1)
HIPAA 164.312(e)(1)
HITECH 170.202
HITECH 170.205
HITECH 170.210

Other Standards:
All current FIPS Publications (especially FIPS 140-1 & 140-2)
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 the 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 the organization’s Business Application Security Policy, Data Backup & Archiving Policy, Database Security Policy, Mobile Device Policy, Network Security & Monitoring Policy, Removable Media Policy, Server 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 the organization’s Data Classification Policy and protected using controls defined at that classification level.

6. The organization will maintain documented procedures for supported cryptographic algorithms, by data classification level, which include documentation of:
   a. Acceptable cryptographic key lengths
   b. Acceptable cryptographic algorithms

7. The 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
   h. Auditing and logging cryptographic key management

8. Exceptions to this policy shall be managed and maintained by following the processes outlined by the organization’s Change Management Policy and Control Exception Policy.
Assurance:
In order to ensure continued compliance with this policy, the 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 the organization as well as continued education events on a regular basis in accordance with the organization’s standards for training and education.

In addition, the organization shall implement an ongoing audit program. This audit program will adhere to the 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 or employment or breach of contract with the organization. For employees, this disciplinary measure shall be administered by the organization’s human resources department in accordance with all human resources policies. For other workforce members this disciplinary measure may result in breach of contract or service level with the organization and therefore appropriate sanctions will be applied as per the agreed upon contractual terms by the purchasing representative or business process owner.

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