Encryption Procedure

Information Assurance Procedure (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 Procedure
Information Assurance Procedure (v1.0)

Purpose:
Information assurance procedures 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, procedures can define the control standards the organization will follow to meet those requirements.

Specifically an encryption procedure 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 procedure 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 procedure must be properly approved and documented in accordance with the organization’s information assurance exception procedure.

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. All data assets classified as “Public – Non-sensitive” or “Private – Non-Sensitive” as defined by the organization’s Data Classification Policy do not need to be encrypted whether at rest on a system or in transit between systems.

2. All data assets classified as “Private – Sensitive” or “Private – Highly Sensitive” as defined by the organization’s Data Classification Policy must adhere to the appropriate encryption controls as defined in 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.

3. If the organization determines with the help of their legal counsel that they are exporting encryption products classified under Category 5, Part 2, of the US Department of Commerce’s Bureau of Industry and Security’s Export Administration Regulations, then it will file an encryption registration and comply with all legal requirements regarding the exportation of such a product.

4. 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.

5. 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.

6. 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.

7. Examples of acceptable symmetric cryptographic algorithms that the 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
   g. International Data Encryption Algorithm (IDEA)

8. Examples of acceptable asymmetric cryptographic algorithms that the 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
   e. Elliptic Curve Cryptography (ECC)
9. The organization will maintain documented standards for cryptographic key management for all classes of systems utilizing such keys which include documentation on the standard 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

10. Exceptions to this procedure 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 procedure, the organization will train all workforce members on their responsibilities that align with this procedure. 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 procedures 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 procedure shall notify the appropriate business owners of the deficiencies that exist.

Sanctions:
Any workforce member discovered violating this procedure 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 procedures. 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.