Use of Cryptographic Controls Standard

I. STANDARD STATEMENT

This standard operates under University Policy 117 Information Security.
and the associated
establish requirements for the use of encryption techniques to protect sensitive data both at rest and in transit. This standard defines the controls and related procedures for the various areas where encryption and other cryptographic techniques are employed.

II. SCOPE AND APPLICATION OF THE STANDARD

Cryptographic controls can be used to achieve different information security objectives, e.g.:

Confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted

Integrity/authenticity: using digital signature certificates or message authentication codes to verify authenticity or integrity of stored or transmitted sensitive or critical information

Non-repudiation: using cryptographic techniques to provide evidence of the occurrence of an event or action

Authentication: using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities and resources

III. DEFINITIONS

Cryptography: a method of storing and transmitting data in a form that only those for whom it is intended can read and process it

SSL certificates are a common example that have identifying data about a server on the Internet as well as the owning authority's public encryption key.

Digital Signature Certificate: a type of digital certificate that proves that the sender of a message or owner of a document is authentic, and the integrity of the message or document is intact. A digital signature certificate uses asymmetric cryptography and is not a scanned version of someone's handwritten signature or a computer-generated handwritten signature (a.k.a. an electronic signature).

SSH Keys: A public/private key pair used for authenticating to SSH servers and establishing a secure network connection.

IV. USE OF CRYPTOGRAPHIC CONTROLS STANDARD

- Approved encryption methods for data at rest
  - The _____ require that the storage of sensitive data in some locations be encrypted. Refer to the for specific requirements.
  - Refer to the _____ for approved encryption methods.

Encryption methods for data in motion

- The _____ require the transfer of sensitive data through a secure channel. A secure channel is an encrypted network connection.
- Various methods of encryption are available and generally built-in to the application. The user should be aware of the data connection being used to transmit sensitive data and if encryption is enabled for that connection.
- Encryption is required for:

  The transport of sensitive files (secure FTP, SCP, or VPN usage to encrypt sensitive data for network file access of unencrypted files).

  Access to sensitive data via a web site, web application or mobile app. Encryption is required for accessing sensitive data from anything with a web interface, including mobile devices (i.e.,

send data from database or a RESTful web service call to retrieve or send data from a cloud application).

Privileged access to network or server equipment for system management purposes.

Encryption of Email

- The _____ require that when emailing some sensitive data it must be encrypted.
- Refer to the _____ document for instructions on encrypting Email.

Use of digital signature certificates

- Digital signature certificates are a way to guarantee the authenticity and integrity of an Email message or document.
- Digital signature certificates are not used for encrypting data.
- Digital signature certificates can be a form of electronic signature or e-signature. Refer to

Legal advice should be sought to ensure compliance before encrypted information or cryptographic controls are moved across jurisdictional borders.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002:2022, Clause 8 Technological Controls)