Encryption Policy

Objective

The purpose of the Encryption Policy is to provide technical guidance to the University community on the use of Encryption technologies. More information regarding the specific types of information that must be encrypted can be found in the University'sWritten Information Security Program.

Applicability

Where technically feasible, the Encryption Policy applies to all faculty or staff members, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any third party service provider providing services to the University who create, use or otherwise access or interact with any University Information or University Information Resource.

Definitions

AES: Advanced Encryption Standard is cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits to protect data.

Asymmetric Key: is a form of encryption where keys come in pairs. What one key encrypts, only the other can decrypt. This is used in digital signatures and also in public-key cryptography such as PGP where you share your public key with anyone. The data is encrypted with your unshared private key and can be decrypted with your public key that you have shared. The public-key cannot encrypt any data it can only decrypt a message already encrypted with the paired private key.

Elliptical Curve Key: is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Encryption Key: a sequence of numbers used to encrypt or decrypt data.

Encryption Key Management: In Encryption it is the creation, distribution and maintenance of a secret key. It determines how secret keys are generated and made available to both parties.

Kerberos: is a secure method for authenticating a request for a service from a computer by providing an encrypted master ticket, which is created on initial user logon to a Kerberos system.

PGP: Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications. It is also used to provide disk and file encryption.

RSA: is an algorithm for public-key cryptography and is used for signing as well as encryption.

Secure Socket Layer (SSL): is a security protocol used to validate the identity of a Web site and to create an encrypted connection for sending sensitive data.

SSH: secure shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Symmetric Key: An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message (example DES).

University Information Resource: any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology..

Policy

All Encryption must meet the following minimum requirements:

- Symmetric key lengths of at least 128 bit
- Asymmetric key lengths of at least 2048
- Elliptic Curve key lengths of at least 256 bit
- AES key lengths of at least 128 bit
- RSA key lengths of at least 2048
- Web server certificates TLSv1.2 (example secure web sites HTTPS)
- SSH version 2 (example network device administration)
- Kerberos (example windows server and connecting device)
- PGP – AES 128 bit (example whole disk, file, USB, and email encryption)
- PGP – Public Keys RSA 2048 (for example digital signatures and encrypted email).

The Information Security Officer must approve all Encryption technologies used on University Information Resources. Approved Encryption will be based on publicly proven algorithms and technologies. No other Encryption technology may be used.

Digital Certificates

- Public-facing Secure Socket Layer (SSL) services must use digital certificates issued by a trusted authority approved by the Information Security Officer or Chief Information Officer.
- Non-public facing SSL services may use self-signed digital certificates when used for management purposes.

Encryption Key Management

- Encryption Key Management procedures must ensure that authorized users can access and decrypt all encrypted data and comply with data retention requirements. (see Retention Records Policy)
- Encryption keys must have at least 2 approved authorized users who can access and decrypt the applicable encrypted information.
- All Encryption keys must be treated as Confidential Information and must be stored securely. (See Data Classification Policy)

Some data is subject to encryption standards by law. To the extent that such legal requirements are different or more specific than required under this Policy, the applicable legal requirements shall be followed. For example, any use of credit cardholder data must follow PCI-DSS encryption requirements (see PCI-DSS standards https://www.pcisecuritystandards.org).

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and take other steps to ensure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	Date	Responsible University Office	Approved By
1.0	09/14/10	Provost Office	Provost Barry Brown
1.1	02/12/13	Senior VP of Finance and Administration and Treasurer Office	Senior VP Danielle Manning
1.2	11/30/21	ITS Information Security	ISO Paul Guarino