UNT SYSTEM
IT Shared Services

Encryption Standards

Purpose

To define the procedures by which UNT System Administration and Institutional data is encrypted.

Scope

These standards define the types of data that must be encrypted, the methods of encryption, and the compensating controls to be used in the instance that data cannot be encrypted.

Procedure

1. Encryption in Transit

Data classified as Category I is required to be encrypted while in transit. It is also recommended that data classified as Category II be transmitted securely when possible.

Examples: Encrypted Instant Messaging, SSL enabled web forms (https://), and VPN access.

2. Encryption at Rest

Sensitive data should also be encrypted while it is being stored. Using strong encryption will greatly reduce the damage incurred by a compromise and can even eliminate the chances of information disclosure. Data classified as Category I is required to be encrypted at rest, and it is also recommended that Category II data be encrypted at rest as well.

Examples: Encrypting files and folders, encrypting database tables or columns, or encrypting disks.

3. Compensating Controls

In some cases it may not be practical to utilize encryption to protect sensitive data. In these rare cases, it is required to document and implement compensating controls. Compensating controls are a combination of practices and technology that can be implemented to lessen the risk of sensitive data disclosure.

In addition to the encryption requirements, data classified as categories I or II should be protected using the following measures:

• Workstation screens should not be visible to anyone but the authorized user of secure documents.

• Workstations used to view or edit secure documents should be protected with a screen saver that requires a password to re-activate the screen after it goes into sleep mode.

• Only authorized persons may use a workstation on which secure documents are accessible.

• Follow strong password standards.

State and federal regulations may also require that some or all of the following access monitoring controls be implemented noting the following:

- who is logged into which work station; how long they are logged in
- the nature of files that are accessed
- how long a workstation is idle after an employee logs in; irregular patterns in employee logins
- a review of access logs of a computing resource to determine any potential security risks

All institutional data (categories I, II, and III) should not be stored off campus without written consent. UNT System Administration and Institution units are responsible for insuring that third party providers agree, in writing, to comply with university data protection requirements and state standards regarding encryption.

Furthermore, the use of personal accounts provided by third party vendors for use of university business or storage of confidential data is prohibited.

References

UNT System Information Security Regulation
Password Standards

Contact Information

Information Security Team
IT Shared Services
http://security.unt.edu
security@unt.edu
(940) 369-7800

Created: 6/17/2013
Updated: