ISO Information Security Office

The University of Texas at El Paso

Data Encryption Guidelines

Contents

Introduction

The most reliable way to protect the University's sensitive data is to avoid handling sensitive University data. Sensitive University data should be retained or handled only when required. Sensitive data is information maintained by the University that requires special precautions to protect it from unauthorized modification or deletion. Sensitive data may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. The controlling factor for sensitive data is that of integrity. Encryption can be an effective information protection control when it is necessary to possess sensitive University data.

IT Owners and IT Custodians should understand that data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorization; that data encryption should be used in conjunction with those other controls; and that data encryption implementations should be proportional to the protection needs of the data.

Purpose

This guideline[1] serves as a supplement to the UTEP Information Resources Use and Security Policy, which was drafted in response to Texas Administrative Code 202 and UT System UTS-165. Adherence to these guidelines will better assure the confidentiality and integrity of the University's sensitive information should data encryption be used as an information protection control.

The purpose of these guidelines is to provide guidance in understanding encryption and the encryption key management required for maintaining the confidentiality and integrity of the University's sensitive data, should data encryption be used as an information protection control.

Scope

These guidelines apply to all devices, physical or virtual, where University data is classified as Confidential, Controlled, or Published (see UTEP's Standard 9: Data Classification).

Roles and Responsibilities

1. Encryption Applicability
    a. Transmission: In order to protect the confidentiality and integrity of the University's sensitive information; any data classified as Confidential data, and having a required need for confidentiality and/or integrity, shall be transmitted via encrypted communication to ensure that is does not traverse the network in clear text. It is further recommended, but not required, that data classified as Controlled be transmitted via encrypted communications when possible. Refer to UTEP's Standard 9: Data Classification for further clarification on the classification of University data. Applications of encryption for data transmission include, but are not limited to, those identified in **APPENDIX-A**.
    b. Storage: In order to protect the confidentiality and integrity of the University's sensitive data; any data classified as Confidential data, and having a required need for confidentiality and/or integrity, shall be stored encrypted in systems and/or databases and/or portable

---

[1] Adapted from the "Data Encryption Guidelines" (https://security.utexas.edu/policies/encryption), with permission from ITS, The University of Texas at Austin, Austin, Texas 78712-1110

computer devices/media. Controlled or Published data classifications do not require such encrypted storage. See the University Data Classification Guidelines for further clarification on data classification. Applications of encryption for data storage include, but are not limited to, those identified in **APPENDIX-B**.

   c. A combination of business practices and technology can act as mitigating factors and could significantly reduce the risk of unauthorized data exposure, thereby offsetting the specific need to implement data encryption. Examples of such mitigating factors include, but are not limited to, those identified in **APPENDIX-C.**

2. Encryption Services
   a. The symmetric algorithms referenced in **APPENDIX-D** shall be used for encrypting Confidential information.
   b. The algorithms referenced in **APPENDIX-E** shall be used for public key asymmetric encryption of Confidential information.
   c. The encryption services referenced in **APPENDIX-F** shall be used for digital signature purposes when Confidential information is involved.
   d. Digital signatures shall be used to associate a user or entity with a respective public key.
   e. Digital certificates shall apply recognized standards (e.g., X.509v3) and shall at least:
      - Identify the issuing certificate authority (aka CA); the certificate authority shall be one authorized by DIR or strictly designated for internal UTEP usage
      - Identify its subscriber
      - Provide the subscriber's public key
      - Identify its operational period
      - Be digitally signed by the issuing certificate authority
3. Encryption Key Management
   a. Encryption keys used to protect Confidential data shall also be considered Confidential data.
   b. Professional key management is critical to prevent unauthorized disclosure of Confidential data or irretrievable loss of important data. A centralized campus key management infrastructure shall be made available to all university users to ensure appropriate controls are applied. The university data managed by all key management infrastructures shall be considered both Confidential and mission critical.
   c. All University key management infrastructures shall create and implement an encryption key management plan to address the requirements of these encryption guidelines, other University and UT System regulations, and applicable State and Federal law. UTEP CISO shall approve such plans.
      - The encryption key management plan shall ensure data can be decrypted when access to data is necessary. Backup or other strategies (e.g., key escrow, recovery agents, etc.) shall be implemented to enable decryption; thereby ensuring data can be recovered in the event of loss or unavailability of encryption keys.
      - The encryption key management plan shall address handling the compromise or suspected compromise of encryption keys. The plan shall address what actions shall be taken in the event of a compromise (e.g., with system software and hardware, private keys, or encrypted data).
      - The encryption key management plan shall also address the destruction or revocation of encryption keys that are no longer in use (e.g., the user has left the University) or that are no longer associated with a key management program.

d. All symmetric encryption keys used on systems associated with Confidential data shall be randomly generated according to industry standards. Acceptable standards include, but are not limited to, those referenced in **APPENDIX-G**.
e. Where symmetric encryption is used to protect Confidential data:
   - Master keys shall be changed at least once per year.
   - Key encrypting keys shall be changed at a minimum of twice per year.
   - Data encrypting keys shall be changed once per session or every 24 hours.
f. When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate are defined by the encryption key management plan of the issuing certificate authority.
g. Encryption keys shall be stored within an encrypted key store or an otherwise encrypted form using approved algorithms; or the keys may be stored on a security token (e.g., a smart card). The encryption keys shall never leave the device if stored on a security token.
   - This requirement does not pertain to keys (e.g. SSH host keys) or protocols (e.g. encryption used by backup technologies) that are providing layers of encryption transport in addition to the strong encryption that has already been applied to Confidential data.
h. Encryption keys are Confidential information, and access shall be strictly limited to those who have a need-to-know. The owner(s) of data protected via encryption services shall explicitly assign responsibility for the encryption key management that should be used to protect this data. If keys are transmitted over communication lines, they shall be sent in encrypted form. The exchange of keys should employ encryption using a stronger algorithm than is used to encrypt data protected by the keys.
i. Encryption keys that are compromised (e.g., lost or stolen) shall be reported immediately to the Information Security Office (security@utep.edu), the key manager, and the information owner of the data being protected. The key shall be revoked or destroyed and a new key generated. Key re-assignments shall require re-encryption of the data.

4. Certificate Authorities
   a. Encryption keys that are generated by a University production certificate authority (CA) and used to control access to the CA server or used by the CA to perform functions shall be stored on Hardware Security Modules (HSM).
   b. All HSMs used within the University shall adhere to recognized standards (e.g., FIPS 140-3, etc.).
   c. University CAs must be designed such that all CA administrator functions are accounted for in detail. Ideally, no single administrator shall obtain full access to the CA encryption keys (e.g., separation of duties, dual control, etc.)
   d. University CAs within the University must adhere to a respective encryption key management plan and create a documented Certificate Practice Statement (CPS).

5. Legal Requirements
   The encryption systems used by the University must comply with applicable laws and regulations. Any export or import of encryption products (e.g., source code, software, or technology) must comply with the applicable laws and regulations of the countries involved, including those countries represented by foreign nationals affiliated with the University. The United States Department of Commerce provides additional guidance specific to such encryption export controls, http://www.bis.doc.gov/index.php/policy-guidance/encryption.

Roles and Responsibilities

1. Information Security Office Responsibilities
   a. Development and maintenance of the University Data Encryption Guidelines.
   b. Assess the secure installation and maintenance of all equipment supporting encryption controls at the University.
   c. Assess the performance and security monitoring for all elements of the encryption control processes.
   d. Assess all related key management processes.
   e. The Information Security Office, acting on behalf of the University, reserves the right to refuse any encryption request that may compromise the security of the University's networks or sensitive data.

2. Key Manager Responsibilities
   a. Adherence to the University Data Encryption Guidelines and related policies established by the University (see also Standard 11: Safeguarding Data).
   b. Ensure secure installation and maintenance of all respective equipment supporting encryption controls.
   c. Ensure performance and security monitoring for all respective elements of the encryption control process.
   d. Ensure all related key management processes can be accounted for in detail and, if possible, that no single key management supporting staff member can individually obtain full access to master keys or CA encryption keys (e.g., separation of duties, dual control, etc.).
   e. Undergo a background check and complete the UTEP Acceptable Use of Information Resources and Security Policy Agreement.

3. User Responsibilities
   - All users shall adhere to the University's Data Encryption Guidelines and related policies established by the University.
   - All users shall be familiar with the UTEP Minimum Security Standards for Data Stewardship.
   - All users shall acknowledge a key escrow agreement, which will identify the required escrow of the subscriber's private key. This requirement will be established for the benefit of the user, the University, and to comply with state and federal law.
   - All users must manage the storage and transmission of data files in a manner which safeguards and protects the confidentiality, integrity, and availability of such files.
   - Questions about the classification of a specific piece of data should be addressed to the local supervisor or respective IT Owner. Questions about these guidelines should be addressed to the Information Security Office.

References

UTEP Information Resources Use and Security Policy
Standard 9: Data Classification
Minimum Security Standards for Systems
Minimum Security Standards for Data Stewardship
NIST Special Publication 800-57:
Recommendation for Key Management, Part 1: General (Revision 4) and
Recommendation for Key Management, Part 2: Best Practices for Key Management Organization

Sources

Appendices

APPENDIX A: Application of Encryption for Data Transmission

1. File Transfers
   Encryption of Confidential file transfers can be achieved via the use of an encrypted transmission protocol or network service (e.g., SCP, SFTP, etc.) or by transferring any Confidential file that has been encrypted prior to the transmission.

2. E-mail
   All content transmitted via e-mail messages shall be encrypted prior to the transmission, presented via a secure web application, or encrypted in a secure message format, given e-mail is exposed to the possibility of unauthorized access at a number of points throughout the delivery process.

3. Interactive Sessions
   Encryption of Confidential data, including login passwords, transmitted during remote login sessions (e.g., Telnet, PeopleSoft and remote control software for PCs) shall be provided through the use of secure applications or protocols. Domain level authentication should be enabled for Remote Desktop protocol on Windows systems).

4. Web-Based Applications
   Encryption of Confidential data communicated between a user's browser and a web-based application shall be provided through the use of secure protocols (e.g., HTTPS via TLS, etc.) The display of Confidential data shall be limited to only what is required by the user's authorized use of the application.

5. Network Printer Communications
   Encryption of Confidential data that is output to a printer connected to a network shall be provided through the use of secure printing applications (e.g., JetDirect) or protocols (e.g., IPP) to prevent unauthorized network interception.

6. Remote File Services
   Encryption of Confidential data transmitted by remote files services shall be provided through the use of encrypted transmission protocols (e.g., IPSec, ISAKMP/IKE, TLS, SFTP/FTPS) to prevent unauthorized interception.

7. Database Access
   Encryption of Confidential data transmitted between an application server and a database shall be implemented to prevent unauthorized interception. Such encryption capabilities are generally provided as part of, or an option to, the database server software.

8. Application-to-Application Communications
   Encryption of Confidential data transmitted between cooperating applications shall be provided through the use of commonly available encrypted protocols (e.g., SOAP with HTTPS) to prevent unauthorized interception.

9. Virtual Private Network (VPN)
   A VPN connection offers an additional option to protecting Confidential data transmitted via the network when other alternatives are not feasible. The use of VPNs should be carefully considered so that all security and networking issues are understood. Telecommunications Infrastructure (aka Networking) staff should be consulted prior to any VPN implementations.

APPENDIX B: Applications of Encryption for Data Storage

1. Whole Disk Encryption
   Encryption of Confidential data stored on portable computing devices (e.g., PDAs, tablet PCs, laptops, and smart phones), as well as storage media, (e.g., CDs, DVDs, External Hard Drives, and USB drives) shall be provided through the use of a whole disk encryption tool or one that can at least be configured to encrypt all Confidential data.

2. File Encryption
   Encryption of Confidential data shall be provided to facilitate the secure transport of individual files over a network without transmission encryption or to off-line storage devices (e.g., CDs, DVDs, External Hard Drives, or USB drives.)

3. Database Storage
   Encryption of Confidential data contained in a database server shall be provided through the use of whole disk encryption or through features native to the database server software. Encryption capabilities native to database server software may allow for encryption of specific tables or columns of a database and may also be required to segregate access rights among multiple applications that utilize a single database server.

   a. IT Owners and IT Custodians should understand that database server encryption does not imply that data in the database server is encrypted when transmitted over a network. In general, the database server decrypts data before it is transmitted, therefore encryption for data transmission shall also be implemented for database servers processing Confidential data.
   b. IT Owners and IT Custodians should consider a number of factors when making decisions on database server encryption (e.g., data classification, need for confidentiality, number of associated applications, system administration, performance, cost, and backup requirements).

4. Backup and Archiving
   Encryption of Confidential data contained in backups and/or archives copies shall be provided to prevent unauthorized access.

APPENDIX C: Examples of Potential Mitigating Factors
- Firewall Restricting Capabilities
- Detailed Audit Logging
- Detailed Process Logging
- Intrusion Detection Capabilities
- Intrusion Prevention Capabilities
- Integrity Checking Capabilities
- Separation of Sensitive Duties
- Physical Security Capabilities

APPENDIX D: Symmetric Algorithms
- AES (128, 192, or 256 bit)
- RC6 (256 bit)
- Serpent (128, 192 or 256 bit)
- Twofish (128, 192, 256 bit)

APPENDIX E: Public Key Asymmetric Algorithms
- RSA (minimum 1024 bit)
- ECC (minimum 384 bit)

APPENDIX F: Digital Signature Algorithms
- RSA (minimum 1024 bit) with SHA-2
- DSA (minimum 1024 bit) with SHA-2
- ECDSA (minimum 384 bit) with SHA-2

APPENDIX G: Industry Standards for Symmetric Key Generation
- FIPS 186-2
- ANSI X9.31
- ANSI X9.62
- ANSI X9.82

Revision History
Created: October 4, 2007
Revised: March 22, 2016
Revised: March 16, 2018
Revised: June 14, 2018

Approved: June 14, 2018 by Gerard D. Cochrane Jr., Chief Information Security Officer