



---

## PURPOSE

*The purpose of this document is to outline the procedures and guidelines to be used for school board/authority employees who maintain and/or transfer personal and confidential information using electronic means. This guideline is provided to assure the confidentiality and integrity of personal information should data encryption be used as an information protection control. This document is intended to provide guidance in understanding encryption technologies. It applies to all devices, physical or virtual where board data is stored. School boards/authorities may use this guideline in the development of policies or procedures for the use of data encryption within their school board/authority.*

---

## Definition

Encryption is a secure process for keeping personal and confidential information private. It is a process by which bits of data are mathematically jumbled using a password key. The encryption process makes the data unreadable unless or until decrypted.

## Background

Data encryption can be an effective information protection control when managing staff or student personal data. School board/authority employees 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.

## Encryption Applicability

**Transmission:** Any data classified as personal and private and having a required need for confidentiality and/or integrity should be transmitted via encrypted communication to ensure that it does not traverse the network or web in clear text.

Applications of encryption for data transmission include, but are not limited to, the following:

- **File Transfers** - Encryption transfers can be achieved via the use of an encrypted transmission protocol or network service (e.g., WinSCP, SFTP, etc.) or by transferring a file that has been encrypted prior to the transmission.
- **Email** - Confidential content transmitted in email messages should be encrypted prior to the transmission, presented via a secure web application, or encrypted in a secure message format given that email is exposed to the possibility of unauthorized access at a number of points throughout the delivery process.
- **Interactive Sessions** - Encryption of private data, including login passwords, transmitted during remote login sessions (e.g., Telnet and remote control software for PCs) should be provided through the use of secure applications or protocols.



- **Web-Based Applications** - Encryption of private data communicated between a user's browser and a web-based application should be provided through the use of secure protocols (e.g., HTTPS, TLS/SSL, etc.). The display of data should be limited to only what is required by the user's authorized use of the application.
- **Network Printer Communications** - Encryption of private data that is output to a printer connected to a network can be provided through the use of secure printing applications (e.g., JetDirect) or protocols (e.g., IPP) to prevent unauthorized network interception.
- **Remote File Services** - Encryption of private data transmitted by remote files services should be provided through the use of encrypted transmission protocols (e.g., IPSec, ISAKMP/IKE, SSL/TLS) to prevent unauthorized interception.
- **Database Access** - Encryption of private data transmitted between an application server and a database can be implemented to prevent unauthorized interception. Such encryption capabilities are generally provided as part of, or an option to, the database server software.
- **Application-to-Application Communications** - Encryption of private data transmitted between cooperating applications should be provided through the use of commonly available encrypted protocols (e.g., SOAP with HTTPS) to prevent unauthorized interception.
- **Virtual Private Network (VPN)** - A VPN connection offers an additional option to protecting private 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.

**Storage:** Any data classified as personal and private and having a required need for confidentiality and/or integrity should be stored encrypted in systems and/or databases and/or portable media.

Applications of encryption for data storage include, but are not limited to, the following:

- **Whole Disk Encryption** - Encryption of private data stored on portable computing devices (e.g., PDAs, tablet PCs, laptops, and smart phones), as well as storage media, (e.g., CDs, DVDs, and USB drives) should be provided through the use of a whole disk encryption tool or one that can at least be configured to encrypt all personal data.
- **File Encryption** - Encryption of private data should 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, or USB drives.)
- **Database Storage** - Encryption of private data contained in a database server should 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.
  - Staff who hold data 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 should also be implemented for database servers processing private data.
  - Staff who hold data 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).
- **Backup and Archiving** - Encryption of private data contained in backups and/or archive copies should be provided to prevent unauthorized access.



**Additional Mitigating Factors:** A combination of business practices and technology can reduce the risk of unauthorized data exposure, thereby reducing the specific need to implement data encryption.

Examples of such mitigating factors include, but are not limited to, the following:

- Firewall Restricting Capabilities
- Detailed Audit Logging
- Detailed Process Logging
- Intrusion Detection Capabilities
- Intrusion Prevention Capabilities
- Integrity Checking Capabilities
- Separation of Personal and Confidential Duties
- Physical Security Capabilities

## Encryption Services

Symmetric algorithms should be used for encrypting private information. Symmetric encryption is cryptography in which the same key is used to both encrypt and decrypt the data. It requires a separate secure channel to exchange keys. The following are symmetric algorithms:

- AES (128-, 192-, or 256-bit)
- RC6 (256-bit)
- Blowfish (128- or 448-bit)
- Triple DES (112- or 168-bit)
- RC4-128
- IDEA-128
- CAST-128
- RC5 (128-bit only)
- SAFER (128-bit)

**Asymmetric algorithms** should be used for public key encryption of private data. Asymmetric encryption is cryptography in which a pair of keys is used to encrypt and decrypt a message. The sender of the message encrypts the message with the recipient's public key. The recipient then decrypts the message with his/her private key. The following are public key asymmetric algorithms:

- RSA (minimum 1024-bit)
- ECC (minimum 384-bit)



**Digital Signatures** should be used to associate a user or entity with a respective public key. A public key is the publicly available key of a signature key pair that is used to validate a digital signature and/or to encrypt confidential information. For digital signature purposes when private information is involved, the following encryption services should be used:

- RSA (minimum 1024-bit) with SHA-1
- DSA (minimum 1024-bit) with SHA-1
- ECDSA (minimum 384-bit) with SHA-1

**Digital Certificates** should apply recognized standards (e.g., X.509v3) and should, at least:

- Identify the issuing certificate authority - the certificate authority should be one authorized by records management or strictly designated for internal board usage;
- Identify the individual (subscriber) who is the subject or entity designee named or identified in a certificate issued to that individual and possesses a private key, which corresponds to the public key listed in the certificate;
- Provide the subscriber's public key ;
- Identify its operational period;
- Be digitally signed by the issuing certificate authority.

## Encryption Key Management

1. Encryption keys used to protect personal data should also be considered personal data.
2. Professional key management is critical to prevent unauthorized disclosure of personal data or irretrievable loss of important data. A centralized school board/authority key management infrastructure should be made available to all school board/authority staff to ensure appropriate controls are applied. The school board/authority data managed by all key management infrastructures should be considered both personal and mission-critical.
3. All school board/authority key management infrastructures should create and implement an encryption key management plan to address the requirements of these encryption guidelines, other school board/authority policies, and applicable education and/or privacy law.
  - The encryption key management plan should ensure that data can be decrypted when access to data is necessary. Backup or other strategies (e.g., recovery agents, etc.) should 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 should address handling the compromise or suspected compromise of encryption keys. The plan should address what actions should 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 should also address the destruction or revocation of encryption keys that are no longer in use (e.g., the user has left the school board/authority) or that are not associated with a key management program.



4. All symmetric encryption keys used on systems associated with personal data should be randomly generated according to industry standards. Acceptable standards include, but are not limited to, the following:
  - FIPS 186-2
  - ANSI X9.31
  - ANSI X9.62
  - ANSI X9.82
5. Where symmetric encryption is used to protect personal data:
  - Master keys (keys used to derive other symmetric keys) should be changed at least once per year.
  - Key-encrypting keys (keys used to encrypt other keys using symmetric key algorithms) should be changed at least twice per year.
  - Data-encrypting keys (keys used with symmetric key algorithms to apply confidentiality protection to information) should be changed once per session or every 24 hours.
6. When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate is defined by the encryption key management plan of the issuing certificate authority.
7. Encryption keys should 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 should 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 personal data.
8. Encryption keys are confidential information, and access should be strictly limited to those who have a need to know. The owner(s) of data protected via encryption services should explicitly assign responsibility for the encryption key management that should be used to protect this data. If keys are transmitted over communication lines, they should 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.
9. Encryption keys that are compromised (e.g., lost or stolen) should be reported immediately to the school board/authority office, the key manager, and the information owner of the data being protected. The key should be revoked or destroyed and a new key generated. Key re-assignments should require re-encryption of the data.

## Certificate Authorities

1. Encryption keys that are generated by a certificate authority (CA) and used to control access to the CA server or used by the CA to perform functions should be stored on Hardware Security Modules (HSM).
2. All HSMs used within the school board/authority should adhere to recognized standards (e.g., FIPS 140-3).
3. School board/authority CAs must be designed such that all CA administrator functions are accounted for in detail. Ideally, no single administrator should obtain full access to the CA encryption keys (e.g., access measures should involve separation of duties, dual control, etc.)
4. School board/authority CAs within the school board/authority should adhere to an encryption key management plan.



## References

University of Texas – *UT Austin Data Encryption Guidelines*  
<http://www.utexas.edu/its/policies/opsmanual/encrypt-guide.php>

UT-Austin: [IT Security Operations Manual](#)

UT-Austin: [Data Classification Standard](#)

UT-Austin: [Minimum Security Standards for Systems](#)

UT-Austin: [Minimum Security Standards for Data Stewardship](#)

NIST Special Publication 800-57:

[Recommendation for Key Management, Part 1](#) and [Recommendation for Key Management, Part 2](#)

Portions adapted from *University of Pittsburgh: Security Guidelines for Encryption*

([http://technology.pitt.edu/documentation/Security\\_Guidelines/Encryption\\_Guideline-vs-2.0.pdf](http://technology.pitt.edu/documentation/Security_Guidelines/Encryption_Guideline-vs-2.0.pdf)), with permission from the University of Pittsburgh, Pittsburgh, Pennsylvania 15260-3332

Portions adapted from *Encryption at the University of California: Overview and Recommendations*

(<http://www.ucop.edu/irc/itsec/uc/EncryptionGuidelinesFinal.html>), with permission from the University of California Office of the President, Oakland, California 94607-5200.

McMaster University - Campus Technology Liaison glossary: [www.mcmaster.ca/ctl/glossary.htm](http://www.mcmaster.ca/ctl/glossary.htm)