

Encryption

Table of Contents

- [Getting Started](#) | [Overview](#) | [Resources](#) | [Standards](#)
- [Cryptographic Controls](#)



Getting Started

In order to implement encryption effectively throughout an institution of higher education, start by developing a strategy that incorporates risk management, compliance requirements, data protection, policies, and standards.

1. **Develop** requirements. The following Guide chapters can help.
 - a. Chapter 8, [Asset Management](#), discusses the need to identify and categorize/classify all your information assets. Understanding/knowing where confidential information resides (ex. SSNs, PII) is a critical component in establishing an encryption strategy.
 - b. Chapter 9, [Access Control](#), addresses the need to ensure authorized access to information resources. Confidential information needs to be protected throughout its lifecycle (access, process, transmit, store).
 - c. Chapter 18, [Compliance](#), provides information in relation to various legal and information security requirements that stipulate the need to protect specific types of information. These types of requirements (ex. PCI DSS, HIPAA) discuss the need to encrypt specific types of data (cardholder data, electronic protected health information)
 - d. The [Risk Management](#) chapter emphasizes the importance of analyzing risks to information. Risk treatment activities may include deploying encryption solutions to protect confidential information.
 - e. Chapter 5, [Information Security Policies](#), stresses that policies provide the direction institutional leadership wants to take in regards to information security goals and objectives. In order to develop an institutional strategy for encryption that will be widely supported and adopted, it's necessary to gain support of institutional leadership.
2. **Seek** to protect data at rest and in motion using Full Disk Encryption (FDE) solutions and transport layer encryption protocols.
3. **Ensure** that your encryption keys are sufficiently strong and well protected using professional and open-source vetted encryption products.
4. **Use** encryption algorithms that are up-to-date and strong. AES 256-bit encryption is the gold standard for FDE. TLS 1.2 is the current gold standard for transport layer security.
5. **Provide** a means for institutional staff to process confidential data while it is encrypted. Ensure secure data transfer environments in internal and external communication channels.
6. **Protect** encryption keys by using long, complex passwords with proper access rights to the keys. Maintain audit logs of access to encryption keys.
7. **Develop** a key management process that automates the process of verifying identity and access rights. Active Directory ensures only active institutional users can access and authenticate secure resources.

Note: Encryption is often a computationally intensive process and may degrade performance of IT applications or infrastructure if not implemented in an optimal way. Be sure to calculate performance requirements of enterprise services and end users before implementing encryption methods. Develop an implementation strategy, gather requirements, complete test plans, deploy following best practices of products, and effectively manage ongoing encryption solutions.

[Top of page](#)

Chapter Summary

This chapter provides a top level overview of cryptography and addresses policy on the use of cryptography, key management, symmetric key cryptography, public key cryptography, encryption standards, as well as various cryptographic libraries.

Overview

In the context of information security, cryptography covers a broad range of topics for securing data. Encryption is the conversion of "cleartext" into "ciphertext". The reverse process, "ciphertext" to "cleartext", is referred to as decryption. Applied properly, cryptographic controls provide considerable protection for the confidentiality of data and, when coupled with other related methods, extend integrity and authenticity safeguards for data, both at rest and in transit.

Both encryption and decryption rely upon secure use of a "key." Authorized parties use keys to view and modify ciphertext data and help secure against unauthorized access. While encryption methods themselves are often strong, insecure handling or generation of encryption keys are common vulnerabilities. It is always important to remember that the security of a cryptographic implementation is no stronger than the security of the keys. For this reason, key management standards and procedures should also be carefully considered when implementing cryptographic systems.

Encryption is a foundational defense against many different risk scenarios ranging from communications eavesdropping to data breach and theft to access control of critical data. As such, institutions should develop policies and standards to help define the appropriate secure use of encryption and related key management methods. Decide where will you store encryption keys securely. For enterprise institutions, key management quickly becomes complex and difficult to manage and central key storage is likely the best option. Dictate strong access and auditing policies for this storage so only authorized individuals can access keys. Ensure a limited amount of trusted administrators (but no fewer than two) can access this location so that only one person does not hold the keys. For critical encryption keys, consider escrowing them in a physically secure location in the event of database failure and backup failure.

Trusted Platform Modules (TPM) used for storing encryption keys is one example of a secure key management technique on client machines.

It is important to note that encryption is another layer in the security framework of an institution. Encryption is not a quick fix for all security risks facing organizations. Data is decrypted on servers and stored in memory while being processed. Data can be stolen by an unauthorized person on your server or network. Encryption is added for defense in depth. Learn more by visiting the [Encryption 101](#) toolkit.

[Top of page](#)

Cryptographic Controls

Objective: Describe considerations for an encryption policy ensuring the protection of information confidentiality, integrity, and authenticity (CIA).

When considering cryptographic controls it is often helpful to first consider your institution's data. This data exists in one of three states: at rest, in transit, or undergoing processing (see *graphic below*). Data are particularly vulnerable to unauthorized access when in transit or at rest. Portable computers (storing data at rest) are a common target for physical theft, while attackers may intercept data in transit over a network through man-in-the-middle attacks or packet capturing and analysis. Unauthorized access may also occur while data processes, but here security systems may rely on the processing application to control and report on such access attempts. When used appropriately, encryption is a powerful tool to prevent unauthorized access to data.

Data States

[blocked URL](#)

Data States and Encryption Methods

Data States	Examples	Relevant Encryption Methods
Data In Use /Processing	Credit card use, W-2 processing, research data	Data is decrypted to be used; data masking of particularly sensitive data should be considered.
Data At Rest	Fileserver storage, desktop files, external media	Full Disk Encryption, Container Based Encryption
Data In Motion	SFTP, HTTPS, SMTPS	TLS (SSL is deprecated); IPsec

It is important for an organization to categorize information and conduct risk assessments to understand which data requires the most protection. Not all files need to be encrypted. Specific types of data require higher degrees of security like HIPAA, FERPA, and PCI data. Understanding which members of your organization use this sensitive data will maximize the efficiency and effectiveness of implementing an encryption policy. Some organizations require all mobile devices use encryption, while other organizations require only select members use encryption. Your organization must determine the scope and scale of the encryption policy to ensure meeting security requirements.

Full disk encryption (FDE) mitigates the risk of data-at-rest exposure, but the security is effective only when the computer is off and encryption keys are secure. FDE may be most effective when used on laptops that, when stolen or lost, are often powered off. See [Introduction to Full Disk Encryption \(FDE\)](#) for an overview of FDE.

Protection of data in motion is accomplished with multiple encryption methods. Virtual private networks (VPN) encrypt and tunnel traffic at the network level across the internet from site-to-site. Another method of protection used relies upon transport layer security (TLS) which encrypts communications between internet applications and web-browser transmissions. Data protected with TLS is encrypted and sent across the unsecure internet. Unlike a VPN that creates an encrypted tunnel to protect data, TLS encrypts the traffic itself and sends directly across unprotected internet space.

Encryption is an important part of an organization's security apparatus, however it is not the panacea to all security issues. It is one piece of the proverbial puzzle to securing your data. Encryption is useful for both enterprise and personal appliances. The biggest differences between enterprise and personal implementations are enterprise solutions allow auditing and tracking of encrypted devices, remote wiping capabilities, and key management. Personal device encryption is usually just as strong as enterprise level, but depends on the implementation practices.

Most enterprise solutions recommend pre-boot authentication before unlocking an encrypted device using full disk encryption for maximum protection. Pre-boot authentication means using a pin, password, or security token to authorize the unlocking of the encrypted drive which then loads the operating system. Encryption keys are not released to memory until pre-boot authentication completes. Personal devices may not require pre-boot authentication for ease of use or the administrator may implement TPM key storage and deployment without pre-boot. The lack of pre-boot authentication leaves a device susceptible to side channel attacks, meaning an attacker focuses on defeating encryption through stealing encryption keys from memory or other methods rather than breaking the algorithm used to generate the ciphertext.

Each organization must calculate the level of risk of losing data and then implement the solution based on this assessment. Some organizations will decide not to use pre-boot authentication based upon this assessment. It is important to consider the impact of encryption solutions on the business or organization to have proper acceptance of your encryption policy. Some organizations allow greater flexibility with user requests while others mandate policies. It is up to your organization to educate the users on the risks of data loss and find a balance between maximum ease of use and total security while meeting the mandated requirements of data protection in your organization.

Useful Resources

- [GA Tech Encryption Standard](#)

[Top of page](#)

Cryptographic Standards

There are many standards in cryptography that are used for various issues and solutions. The most common standards are listed here.

AES | Advanced Encryption Standard (Symmetric Cryptography) is used in file and full disk encryption.

PKI | Public Key Infrastructure (Asymmetric Cryptography) is a system for creating, storing, and distributing digital certificates issued from certificate authorities. PKI is used in [public key cryptography](#) which allows entities to securely communicate on an insecure public network.

Public Key Cryptography | ECDH | KEY EXCHANGE (Asymmetric Cryptography) is used during insecure public transmission of encryption keys for transmitting data through encrypted channels over public networks.

OpenPGP | Pretty Good Privacy (Hybrid Cryptography) is used for email encryption, instant message encryption, session key exchange, and other uses. OpenPGP uses both symmetric and asymmetric cryptography.

Cryptographic Hash Functions are used for identity verification with digital signatures, file integrity verification, and fingerprinting of messages for authentication. SHA-256 and SHA-512 are examples of a cryptographic hash function.

References:

- [Suite B Cryptography](#) and [The Case for Elliptic Curve Cryptography](#) (NSA)
- [Elliptic Curve Cryptography](#) (Certicom)
- [Guide to Elliptic Curve Cryptography](#) (Hankerson, Menezes, Vanstone)
- [NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography](#)
- [FIPS Pub 180-4: Secure Hash Standard \(SHS\)](#)
- [Cryptographic Hash Function](#) (Wikipedia)
- [PGP: A Hybrid Solution](#) (SANS Institute)

Cryptographic Libraries

Software developers and vendors usually write cryptographic libraries for various platforms. OpenSSL, the open source secure socket layer library is arguable one of the most popular, as well as most widely used cryptographic library. OpenSSL is used as the default cryptographic library for *NIX systems, including all Linux variants, all BSD variants and in Mac. Microsoft Operating Systems use the Microsoft Cryptographic Provider, which is also the foundation for .NET cryptography. Other common cryptographic libraries include the Java Cryptographic Library and Wei Dai C++ Crypto library.

References:

- [Crypto++ Library 5.6.2](#)
- [Microsoft Developer Network: System.Security.Cryptography Namespace](#)
- [The Cryptography API, or How to Keep a Secret](#)
- [PHP Manual: Cryptography Extensions](#)
- [Java Cryptography Architecture \(JCA\) Reference Guide](#)
- [Introducing Conceal: Efficient Storage Encryption for Android](#)
- [Mac Developer Library: Cryptographic Services Guide](#)
- [The Legion of the Bouncy Castle](#)

[Top of page](#)

Resources

EDUCAUSE Resources

- [Encryption 101](#)
- [Encryption, EDUCAUSE Resource page](#)
- [Introduction to Full Disk Encryption \(FDE\)](#)

Initiatives, Collaborations, & Other Resources

- [Stanford Whole Disk Encryption](#) - Stanford University
- [Microsoft BitLocker](#)
- [Apple File Vault](#)
- [PGP Whole Disk Encryption at Indiana University](#)
- [eSecurity Planet Buyers guide to Full Disk Encryption](#)



[Top of page](#)


Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
-----	------	-------	---------	------------------------------	----------------

27002:2013 Information Security Management Chapter 10: Cryptography ISO/IEC 9796-2:2010 ISO/IEC 9797-1:2011 ISO/IEC 9798-2:2008 ISO/IEC 11770-1:2010 ISO/IEC 14888-1:2008 ISO/IEC 18033-1:2005	800-111 800-56A FIPS 180-4	DS5.8 APO11.02 APO11.05 BAI03.03 DSS01.01 DSS01.02 DSS01.04 DSS01.05 DSS05.01 DSS05.02 DSS05.03 DSS05.06 DSS06.05	Req 3 Req 4	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	45 CFR 164.312(e)(1) 45 CFR 164.312(a)(1)
---	---	--	------------------------------	---	--

[Top of page](#)

 Questions or comments?  [Contact us.](#)

 *Except where otherwise noted, this work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](#) (CC BY-NC-SA 4.0).*