9/6/22, 7:19 PM Information Security Policy and Standards: Data Encryption: Information Technology - Northwestern University

**INFORMATION TECHNOLOGY**

**Information Security Policy and Standards: Data Encryption Purpose:**

This document provides the University community with the information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure Legally/Contractually Restricted Information (Sensitive Data) (refer to Northwestern University – Data Access Policy (/dataaccess.html) ).

The focus is on providing a range of tools for the most common systems that are likely to be deployed in the University environments which store, transmit or process Sensitive Data.

When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

**Audience:**

All Faculty and Staff All contractors, vendors and any others (including 3rd parties) entrusted with University Sensitive Data **Policy Statement:**

Schools, departments and business functions are required to employ University-approved encryption solutions to preserve the confidentiality and integrity of, and control accessibility to, University data classified as "Legally/Contractually Restricted" where this data is processed, stored or transmitted.

**Policy/Procedures:**

**Encryption Products (Appendix D)**

The value of the data that requires protection and the system storing the data need to be considered carefully. Physical security refers to being able to control access to the system’s storage media. All encryption methods detailed in these guidelines are applicable to desktop and mobile systems.

A defense in depth approach is recommended when evaluating and deploying encryption products. In an ideal situation, full disk and/or boot disk encryption would be combined with file/folder encryption in order to provide two “layers” of encryption to protect data in the event the first layer is compromised. This typically involves a combination of boot/full disk encryption and file/folder encryption.

Commercial operating systems such as Windows Vista and Mac OS X provide integrated encryption solutions at no additional cost. Northwestern IT Information Security Office recommends the use of integrated encryption solutions in combination with preferred third party products detailed in the following scenarios.

a. **Boot Disk Encryption**

Scenario:

Mobile systems such as laptops are highly susceptible to theft and frequently contain valuable data. Boot disk encryption requires the key in order to start the operating system and access the storage media. In this scenario the operating system is removed as a vector for attack in the event of physical compromise. Boot disk encryption is typically implemented in conjunction with full disk encryption.

Product(s):

BitLocker, Symantec Endpoint Encryption, PGP Desktop, VeraCrypt

OS-Integrated Product(s):

BitLocker

https://www.it.northwestern.edu/policies/dataencryption.html 1/4

9/6/22, 7:19 PM Information Security Policy and Standards: Data Encryption: Information Technology - Northwestern University

Preferred Product(s):

Symantec Endpoint Encryption

b. **Email Encryption**

Scenario:

Email-specific products integrate encryption into the email client, allowing messages and attachments to be sent in an encrypted form transparent to the user. This is most appropriate for departments whose users require frequent and regular encryption of email communications. Most departments can make use of a broader range of file/folder encryption products to encrypt individual files and folders.

Product(s):

PGP Desktop

c. **External Devices Encryption**

Scenario:

External devices such as hard drive, DVDs, CDs and USB flash drives can be encrypted in their entirety. Data on these systems can be considered secure without access to the key and encryption software.

Product(s):

Cryptainer LE, PGP Desktop, VeraCrypt

d. **File Encryption**

Scenario:

Individual or multiple files can be encrypted separate from the host operating system. These encrypted archives can be stored in different locations such as network shares, external hard drives or be transmitted securely via e-mail.

Product(s):

7-Zip, Cryptainer LE, Disk Images, EFS, FileVault, PGP Desktop, VeraCrypt, WinZip, WinSCP, WinZip

OS-Integrated Product(s):

Disk Images, EFS, FileVault

e. **Folder Encryption**

Scenario:

Folders containing data can be encrypted separate from the host operating system. These encrypted archives can be stored in different locations such as network shares, external hard drives or be transmitted securely via email.

Product(s):

7-Zip, Cryptainer LE, Disk Images, EFS, FileVault, PGP Desktop, VeraCrypt

OS-Integrated Product(s):

Disk Images, EFS, FileVault

f. **Full Disk Encryption**

Scenario:

Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area.

Product(s):

BitLocker, Symantec Endpoint Encryption, PGP Desktop, VeraCrypt

Preferred Product(s):

PGP Whole Disk Encryption

g. **Mobile Device Encryption**

Scenario:

Mobile devices such as PDAs and smartphones allow users to exchange, transfer and store information from outside of the office. The extreme portability of these devices renders them susceptible to theft or loss. The Northwestern IT Information Security Office recommends the use of standardized devices such as laptops for storing, transmitting or processing Sensitive Data.

Product(s):

BlackBerry Content Protection (BlackBerry Content Protection is not available on all BlackBerry devices), iPhone Encryption h. **Transport-Level Encryption**

https://www.it.northwestern.edu/policies/dataencryption.html 2/4

9/6/22, 7:19 PM Information Security Policy and Standards: Data Encryption: Information Technology - Northwestern University

Scenario:

Secure transport client/server products provide transport-level encryption to protect data in transit between the sender and recipient in order to ensure delivery without eavesdropping, interception or forgery. This scenario requires the appropriate configuration of a server in order to allow clients to connect in a secure manner.

Product(s):

FileZilla, PSFTP, SCP, WinSCP

**Forms/Instructions**

**Step 1 - Data Classification**

Data classification is the process of assigning a level of sensitivity to data and determining to what degree the data needs to be controlled and secured. Differentiating between data of little or no value and data that is highly sensitive is crucial when selecting and deploying an encryption solution.

The process of classifying data is rarely simple. It is most often a collaborative process requiring the active participation of data owners who have the greatest familiarity with the data, and who are indispensable in accurately identifying the value of individual and aggregated data items.

**Step 2 - Product Selection & Implementation**

Encryption products should be selected based on the type of encryption they offer and the technical details of the system on which they will be installed, such as operating system. Most products are available for only one operating system, some are available for multiple operating systems, some are platform specific and are included as part of a standard installation. Guidelines below and Appendix D - Encryption Products include scenarios and product details.

**Step 3 - Key Creation**

The construction of encryption/decryption keys should follow the established standards detailed above (Definitions, c. Key Construction (/../policies/dataencryption#keyconstruction) ).

**Step 4 - Key Management**

Encryption products use one or more cryptographic keys to encrypt and decrypt the data that they protect. Some products support the use of a recovery key that can be used to recover the encrypted data if the regular key is lost. If a key is lost of damaged it may not be possible to recover the encrypted data. Departments need to ensure that all keys used in a storage encryption solution are secured and managed properly to support the security of the solution.

Extensive key management should be planned which will include secure key generation, use,storage and destruction. Considerations should be made as to how these key management practices can support the recovery of encrypted data if a key is inadvertently disclosed,destroyed or becomes unavailable. Specific technical options should be tied to particular products.

Departments need to ensure that access to encryption keys is properly restricted. Authentication should be required in order to gain access to keys (passwords, tokens,etc.). The keys themselves should be physically secured with at least two upper-level trustees assigned access.

**Step 5 - Key Recovery**

The technical and procedural processes that are established and followed in order to retrieve or change encryption keys in a controlled and safe manner are referred to as key recovery.In the event of compromise or loss all affected keys must be revoked and/or changed and redistributed. Some products incorporate key recovery as a technical feature.

**Satisfies ISO 27002 10.8.4, 10.9.1, 10.9.2, 12.2, 12.3**

https://www.it.northwestern.edu/policies/dataencryption.html 3/4

9/6/22, 7:19 PM Information Security Policy and Standards: Data Encryption: Information Technology - Northwestern University

**Last Review Date:**

December 2013

**Original Issue Date:**

August 2008

**Revision Dates:**

August 2008

October 2008, March 2009, September 2010, March 2012, September 2014, August 2018 Additional Information:

Appendix A - Encryption Products and Site Reference (/../bin/docs/AppendixA.pdf) Appendix B – References (/../bin/docs/AppendixB.pdf)

Appendix C - Definitions (/../bin/docs/AppendixC.pdf)

Appendix D - Encryption Products (/../bin/docs/AppendixD.pdf)

Address

**Information Technology**

1800 Sherman Ave

Evanston, IL 60201

Phone number

847-491-4357 (1-HELP)

Email Address

consultant@northwestern.edu (/mailto:consultant@northwestern.edu)

Share feedback about this page (/../forms/feedback/comments.html)

https://www.it.northwestern.edu/policies/dataencryption.html 4/4