



OIT 62.603: Encryption

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

University employees and other personnel who have access to sensitive and confidential University information must encrypt files containing sensitive and confidential information to protect it from unauthorized disclosure. Furthermore, the encryption program used must employ proven standard algorithms and must permit properly designated University officials, when required and authorized, to decrypt the files to acquire the information.

II. Purpose

The purpose of this policy is to provide users with relevant guidance concerning data encryption at Norfolk State University as well as their responsibilities pertaining to encryption

III. Scope

This policy applies to NSU employees and other personnel (i.e. supporting vendors, consultants, etc.) who have access to sensitive and confidential University information.

IV. Requirements

Commensurate with sensitivity and risk, NSU or its service provider shall:

1. Define and document practices for selecting and deploying encryption technologies and for the encryption of data.
2. Document appropriate processes before implementing encryption. These processes must include the following components:
 - a. Instructions in the Security Incident Response Plan on how to respond when encryption keys are compromised;

- b. A secure key management system for the administration and distribution of encryption keys; and
 - c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.
3. Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain; however, digital signatures may be utilized for data that is sensitive solely relative to integrity.

Examples of Sensitive or Confidential University Information:

Some examples of sensitive data include social security numbers, credit card numbers, medical history, certain financial data, and other data as defined by FERPA, HIPAA, the Commonwealth of Virginia, or other relevant laws and regulations. Directory information is not considered sensitive.

Acceptable Encryption Standards

The use of proprietary encryption algorithms is not allowed for any purpose unless it has been reviewed by qualified experts and approved by the University's duly appointed Information Systems Security Officer.

Proven standard Encryption methods such as AES, Blowfish, RSA, RC5, IDEA, etc., and encryption keys of 128 bits or higher must be used when encrypting sensitive data.

A One-Way Hash Function must be used to irreversibly encrypt digital signatures, integrity checksums, authentication information including passwords, and similar types of data.

User Responsibilities

Users who have access to sensitive and confidential information are authorized and expected to encrypt data for protection against unauthorized disclosure both while it is being stored and while it is being transmitted as well.

Users must protect sensitive and confidential information wherever it resides - on servers, desktop and laptop personal computers, and even when or if it is placed onto peripheral storage devices such as PDA's, USB/thumb drives, memory cards, computer diskettes and discs, media players, digital cameras, cell phones, etc.

Users must ensure they properly secure any encryption keys associated with encrypted data.

Users must be aware that the U.S. Government has restricted the export of encryption technologies. Those users who are residents of other countries and those who travel to foreign countries must also be aware of the encryption technology laws of those countries as well.

Users who have questions or require assistance concerning encryption should send an e-mail to helpdesk@nsu.edu or call the OIT Help Desk on 823-8678.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

Glossary

FERPA - the Family Education Rights and Privacy Act

HIPAA - the Health Insurance Portability and Accountability Act

Directory Information - The following information has been declared "Directory Information" and may be released by the University without prior consent of the student: name; address; date and place of birth; major field of study; participation in official activities; weight and height of athletic team members; dates of attendance; enrollment status; degree; honors and awards received; and, previous educational agency or institution attended.

Proprietary Encryption - an algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem - a method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem - a method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

One way Hash Function - a cryptographic algorithm which does not require a key and produces an irreversibly encrypted cipher-text. Other names for this are message digest, fingerprint, digital signature, and compression function.

SSL - Secure Socket Layer, a protocol designed to provide encrypted communications on the Internet.

SSH - Secure Shell, a network protocol that allows data to be exchanged over a secure channel between two computers.

Kerberos - a network authentication protocol.

PCAnywhere - a computer program used for remote connectivity and encryption.

PGP - Pretty Good Privacy, a computer program used to encrypt and decrypt data.

Terminal Services - a component of the Microsoft Windows operating system that allows a user to access applications and data on a remote computer over any type of network.

PPTP - Point-to-Point Tunneling Protocol, a method for implementing virtual private networks.

IPSec - Internet Protocol Security, a framework of open standards for protecting communications over Internet protocol networks through the use of cryptographic security services.