Encryption Security Standard

Information Technology Security Standard #3, v0.2

Standards Name: Encryption Security Standard

Original Release Date: 8/21/2007
Latest Revision Date: 10/18/2007

Authority: This standard was approved by the Information Security Council, acting as representatives of the CIO and the Technology Leadership Committee (TLC). It derives its authority from the CIO, the owners of University Data and the campus Information Technology (IT) community.

Summary: This standard provides the security requirements for applying encryption techniques to sensitive information. It is based on the Information Security Standard and associated requirements from other IT security standards.

Applicability/Scope: Applies to all Users and Administrators of systems that house or manipulate University Data.

Responsible Office: ITS/CIO.

Overview

University Data is a vital asset to Syracuse University and any improper handling of that information can lead consequences including legal action, loss of reputation, loss of service and other impacts on the business of the University. University Data must be protected against unauthorized access and modification, with the safeguards chosen according to the risks involved. The increasing use of mobile devices (laptops, PDA's, flash drives, etc.) and of web-based applications place University Data at greater risk than ever before, and demand additional measures be taken as the sensitivity of the data increases. As defined in the Syracuse University Information Security Standard, University Data classified as Enterprise or Confidential will require specific protections, depending on its physical location. One of the key methods for protecting information that must traverse or exist in less secure places is the use of encryption. Encryption suites protect the information against unauthorized reading and unauthorized changes. Note that user credentials (e.g., NetID and password) are also considered Confidential Information and require the same kinds of protections as any other sensitive information, since they provide the access to the systems that house the information.

The following standard explains what encryption steps need to be taken to minimize risk to sensitive University information in various locations. It applies to all University-owned data in electronic form.

Data on Servers

Confidential Data:

- Servers will be housed and backed up as defined in the Server Security Standard under "High Security." This includes specific requirements for all devices and media holding the Confidential Data. In cases where backup media is not encrypted, administrators must keep inventories of what records are held on the media, so that in the event of a data exposure, it's possible to know the scope of the problem. For example, "tape contained a database table x which held all grades for all students in course y during the 2007-2008 academic year."
- All administrative logins to the server for managing the system will occur over encrypted channels using industry-standard protocols.

Enterprise Data:

- All administrative logins to the server for managing the system will occur over encrypted channels using industry-standard protocols.

Data on Mobile Devices and Desktops

Confidential and Enterprise Data:

- Desktops, laptops, and all associated removable media must be encrypted whenever the device may possibly leave a secured area. The encryption must protect the entire device, not just specific files. Desktops located in open areas (accessible to people who are not authorized to login to the machine or work in the area) and which manipulate Confidential information must also employ whole-disk encryption. Encryption tools and techniques will be defined by campus IT Security and must be installed and configured by University IT staff.
- All encryption keys must be stored separately from the device they protect and must be recoverable by the unit's technical support staff.

Confidential Data:

- Data covered by the New York State Disclosure laws may not be stored on these kinds of devices without approval of campus IT Security and the VP with oversight of the data in question, even if encryption is applied.

Data on the Network

Confidential and Enterprise Data:

- All such data passing over the Internet or over insecure campus network links must be encrypted, either at the network layer (e.g., IPsec as used within VPN's), the transport layer (e.g., SSL as used within web applications), or the application

layer (e.g., PGP mail). All campus network links that pass through non-administrative buildings must be treated as insecure. Only traffic contained within server rooms or other well-controlled locations may be excluded from the encryption requirement. FTP must be replaced with SSH, HTTP with HTTPS, etc., on all insecure links.

- All credentials passing over the network must be encrypted, again with the exception for well-controlled server environments. This means that ftp and other cleartext protocols may not be used for cross-building data transfers.
- All wireless traffic, which is inherently open to eavesdropping (it's just radio) must be protected by encryption. The "AirOrange" wireless network must be used with additional encryption mechanisms. Campus employees MUST use AirOrangeX for all wireless activity whenever possible.

Applications

- Commercial applications, including outsourced services, must protect the University data as required by law and any relevant industry standards (e.g., PCI). Contracts with vendors, consultants, and other third parties must include language about protection of the University Data and should specify where encryption will be used.
- All user and administrative logins must occur over encrypted channels.