Encryption

Policy 404 seeks to protect the University from legal and financial liability due to the loss or theft of personal information. Encryption is the University’s preferred method for protecting personal information since it affords a legal “safe harbor” from both physical and many types of electronic loss.

The policy also recognizes that there are circumstances where an organization may not utilize encryption because its data stores are “otherwise protected.” In those cases, it must be understood by the organization that they have increased their financial liability as well as increasing the risk profile of the University.

Each organization is responsible for creating an implementation plan that specifies a timeline for encrypting all personal information. If the organization is not going to utilize encryption, they must include in their implementation plan precisely what information is not being encrypted and how it is going to “otherwise protect” that information.

Definitions:

Mobile Devices: Laptops, tablet PCs, Blackberry’s, Personal Digital Assistants, external hard drives, tapes, diskettes, CDs, DVDs, USBs and similar mobile technologies.

Desktops: A device that is not intended to be mobile and is intended to reside in a permanent unmovable location. These devices are generally in locations that provide a modicum of physical security.

Server: A device that is not intended to be mobile and resides in a permanent unmovable location. These devices are generally in locations that provide a variety of access controls that guarantee they cannot be physically lost.

Risks:

The greatest risk to the University losing personal information is from mobile devices. Although these devices do not normally contain large amounts of personal information, their physical vulnerability, coupled with the large number of devices, makes them the primary means by which the University might lose personal information. It is effectively impossible to guarantee a mobile device’s physical security, and therefore, encryption is the only technique available to protect personal information stored on mobile devices.

The second largest risk to the University losing personal information is from desktop devices. Because of the University’s trusting and open culture, many people have physical access to desktop devices that contain information that they would not normally have access to. Additionally, the theft by electronic means is a possibility and encryption enhances the desktop’s overall security.

The least likely risk to the University losing personal information is from its servers. In general, these devices are in physically secure locations and there is little chance of them being physically lost. But the theft by electronic means is a possibility and encryption enhances the server’s overall security.
Specifications:

1. Key lengths...
   - Symmetric encryption key length of no less than 128
   - Public key encryption key length of no less than 2048
   - Elliptic curve key length of no less than 256
   - Hash key length of no less than 256
   - MAC key length of no less than 256

2. Cryptography algorithms...
   - AES - Advanced Encryption Standard
   - Twofish
   - Serpent
   - MARS
   - RC6
   - RC4
   - Blowfish
   - RSA
   - Rabin
   - DESX
   - Triple-DES