Appendix C - Definitions

Boot Disk Encryption- The process of encrypting all data on the bootable media of a system, the media responsible for starting the operating system.

Ciphertext - Information that has been encrypted, making it unreadable without knowledge of the key.

Compression - The process of reducing the size of files by repackaging them into another format which can later be decompressed in order to retrieve the files.

Compensating Controls–The protective measures required to mitigate the risk posed by unencrypted Sensitive Data that meet all the following criteria:
- Established segmentation or abstraction at the network layer
- Restriction of access to the data by IP or MAC address, application or service, user account or group, and data type.
- Restriction of logical and physical access to the data
- Prevention and detection of attacks against the data

Cryptanalysis - The study of techniques for attempting to defeat cryptographic techniques and, more generally, information security services.

Cryptography - The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication.

Cryptosystem - A general term referring to a set of cryptographic primitives used to provide information security services.

Decrypt/Decipher/Decode - Decryption is the opposite of encryption. It is the transformation of encrypted information back into a legible form. Essentially, decryption is about removing disguise and reclaiming the meaning of information.

Departmental Server – A computer on a network designed and authorized to manage networked departmental resources.

Encrypt/Encipher/Encode - Encryption is the transformation of information into a form that is impossible to read unless you have a specific piece of information, which is usually referred to as the "key." The purpose is to keep information private from those who are not intended to have access to it. To encrypt is essentially about making information confusing and hiding the meaning of it.

Encryption Algorithm - A set of mathematically expressed rules for encoding information, thereby rendering it unintelligible to those who do not have the algorithm decoding key.

Encryption Key - A special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message.

External Devices - Any device capable of reading and/or writing digital information. Examples include USB flash drives, external hard drives, and writable media such as CDs and DVDs.

File Encryption - The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided.

Folder Encryption - Encryption of individual folders on a storage medium and permitting access to the encrypted files within the folders only after proper authentication is provided.

FTP – A network protocol used to transfer data from one computer to another through a network.

Full Disk Encryption - Encryption of all data on the hard drive used to boot a computer, including the computer's operating system. Access is permitted to the data only after successful authentication with the full disk encryption product.

Internal Information - The classification of data defined by the University's Data Access policy that is intended for use by and made available to members of the University community who have a business need to know. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business need.

Legally/Contractually Restricted Information – The classification of data defined by the University's Data Access policy that is required to be protected by applicable law or statute (e.g., HIPAA, FERPA, or the Illinois Personal Information Protection Act), or which, if disclosed to the public could expose the University to legal or financial obligations.

PDA (Personal Digital Assistant)–Computing devices commonly known as hand-held or palm-top devices, distinguishable from laptop PCs. Examples include the RIM Blackberry, and Palm Treo.

SDA – Self Decrypting Archive - An encrypted archive that can be decrypted independent of the client software used to encrypt the original archive.

Sensitive Data – A generic term for data/information identified as Legally/Contractually Restricted Information.

Secure FTP (SFTP) – A combination of technologies that allow FTP software to perform secure file transfers. Typically involves the use of an SSH-based file transfer. FTP/SSL uses an SSL/TLS layer in order to encrypt the standard FTP protocol.

Smartphone - A mobile phone offering advanced capabilities beyond a typical mobile phone, often with PC-like functionality. Examples include the Blackberry, iPhone, and Droid.

SSL/TLS – Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide authentication, confidentiality and data integrity between two communicating applications, typically within a web browser.

Virtual Disk Encryption - Encryption of a container which can hold many file and folders and permitting access to the data within the container only after proper authentication has been provided.

Volume Encryption - Encryption of an entire volume, only permitting access to the data after the proper authentication is provided.