IT END USER COMMUNICATIONS STANDARDS

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy.

The purpose of this document is to support and outline in detail the requirements of the IT End User Communication and Encryption Policy. These requirements are mandatory and must be adhered to by all employees, students, consultants, vendors, IT system administrators and application developers.

This document outlines requirements that must be adhered to when transmitting sensitive data to other parties, and the encryption technologies that must be used for such communications. This document contains requirements that are specific to encryption usage and administration as well as end user messaging.

Encryption encompasses a wide variety of technologies and methodologies for encoding messages and information in such a way that only authorized parties can view them. This Standard defines the various circumstances in which encryption must be used, the deployment standards for each type of encryption, and when each encryption method must be used for end user messaging.

SCOPE

This document is intended for all employees, students, consultants, vendors, IT system administrators and application developers.

REQUIREMENTS

File Transfers

All file transfers of sensitive data must use a secure communication channel. The permitted file transfer protocols are SFTP, FTPS and HTTPS. The password or key should be communicated using a different channel.

Email Transfers

In the event that a file containing sensitive data is to be sent via email, file level encryption must be applied prior to being sent. The password or key required to decrypt the file must not be sent in the same email. The password or key should be communicated using a different channel.

File-level Encryption

When data needs to be transferred to an external entity (e.g., bank) in a file, the data must be transferred securely, or contained in a file format which supports encryption including:

- Password protected zip file or Microsoft Office 2010 or higher encrypted documents
    - The password must never be sent via the same method as the file being transferred. For example, the file might be sent via email and the password given to the recipient by phone

- PGP data encryption
    - Users of this method must keep their private key secure and accessible only to authorized system administrators and applications.

Social Media

Sensitive data must not be made available on any social media system even when communicating directly with an authorized person, e.g., a student. Social media systems are by their very nature insecure and public.

RESPONSIBILITIES

End Users

End users with access to sensitive data must use one of the methods defined above when transmitting sensitive data.

Data Owners

Data owners are responsible for being aware of any sensitive data within their application or system which requires encryption. Data owners are also responsible for ensuring that systems administrators responsible for the application have been notified of these encryption requirements, and that the encryption required has been implemented.

Data owners are also responsible for ensuring that system administrators are notified of any changes or additions to sensitive data requiring encryption.

System Administrators

System administrators are required to implement the appropriate encryption methods as outlined in the "IT Encryption Standards". These requirements are usually identified as part of the project management implementation framework or as provided by the data owner.

System administrators with access to public key encryption certificates and keys are responsible for ensuring that the handling of these certificates and keys is as outlined in the "IT Encryption Standards".

DEFINITIONS	
FTPS	Also known as FTP over SSL. An extension to the FTP protocol which utilizes TLS and SSL encryption protocols
HTTPS	A protocol used for web browsers to access web server content over an encrypted communication channel using Public Key Encryption
SFTP	Also known as SSH File Transfer Protocol. A file transfer protocol which utilizes SSH for the communications channel
SSH	Also known as Secure Shell. An encrypted network protocol for initiating text-based shell sessions on remote machines
PGP (Pretty Good Privacy)	A data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions, and to increase the security of e-mail communications
Social Media System	Any system or application whose purpose is the public sharing of data or messages such as, but not limited to Facebook, Twitter, YouTube, etc.