UF UNIVERSITY of FLORIDA
Information Technology

Standard

Standard: TS0006.02	Category: Technical Security	Version Date: 2/1/2017
Title: Electronic Communications and Data Transmission Standard		Effective Date: 2/15/2017
Originating Unit: Information Security Advisory Committee		Last Review: 2/1/2017
Review Resp: HIPAA Security Officer		Next Review: 2/1/2020

Purpose:

The purpose of this standard is to specify required safeguards for electronic communications and data transmission.

Reference:

1. Policy TS0006: Electronic Communications and Data Transmission Standard
2. Policy: Electronic Mail http://www.it.ufl.edu/policies/email/policy-electronic-mail/
3. eTools Assessment http://www.it.ufl.edu/community/guidelines/etools-assessment/

Standard:

1. Electronic Mail:
    a. Mailboxes and calendars will require user authentication to access
    b. Digital certificates will be installed on email servers for service authentication
    c. Email clients and servers will have transmission encryption for SMTP, POP3, and IMAP services.
    d. Antivirus and spam protection will be configured and maintained.
    e. UF email may not be auto-forwarded to a non-UF email system.
2. Instant Messaging:
    a. Will require user authentication.
    b. Clients and services will have transmission encryption.
    c. Will not be used for file transfer; where practicable clients will be configured to prohibit file transfer.
    d. The University provided or approved instant messaging service, such as Microsoft Skype for Business, must be used for instant messages that might contain HSC Restricted information.
3. File Transfer Protocols (HTTP, FTP, SSH, etc.)
    a. Will be configured to require user or process authentication
    b. Will be configured with transmission encryption.
    c. A security evaluation must be performed of the destination site prior to establishing a connection for purposes of Restricted data transmission.
4. Web Browsers:
    a. Will have transmission encryption.
    b. Will be configured to prevent caching when data is delivered via an encrypted session.

5. Due to the high risk of inadvertent unauthorized disclosure of Restricted data, peer to peer (P2P) file sharing programs are prohibited on HSC computers and networks. In addition, personally owned computers detected with P2P file sharing programs will be prohibited from accessing the HSC network.