Virginia Commonwealth University
Technology Services

Security Standard for Transmission of Confidential Data Through Email

Effective Date: ***July 2007***
Compliance Date: ***August 2007***
Review Date: ***August 2008***

Revisions:

Version	Date	Revision Issuance
1	April 2006	Initial draft
2	August 2007	Revisions
3	January 2008	Revisions

.

Scope: This standard is applicable to all University organizational units and contracted business associates that transmit University-owned confidential information using Email (including attachments).

Definitions:

- Confidential Data is defined as any data of which the compromise with respect to confidentiality, integrity and/or availability could have a material adverse effect on University interests, the conduct of University programs or the privacy to which individuals are entitled. See the Data Classification Guidelines located on the VCU security website for information on the criteria for classifying confidential data based on:
  - confidentiality, which addresses sensitivity to unauthorized disclosure
  - integrity, which addresses sensitivity to unauthorized modification
  - availability, which address sensitivity to outages

- Encryption is defined as the process of transforming readable data (plaintext) into a form that is unreadable (ciphertext) by all except the person possessing the key to decrypt the data. Encryption can protect the confidentiality of the data during transmission and at rest.

Applied Industry Best Practices of:

- SANS Security Institute
- National Institute of Standards Technology (NIST) Guidelines on Electronic Mail Security
- Health Insurance and Portability and Accountability Act Security Rule
- Health Insurance and Portability and Accountability Act Privacy Rule

Requirements of the Standard

S1.0 – Encryption of Confidential Data in Email

S1.1- University faculty, staff and contractors may not transmit confidential data via email and/or email attachments unless the message and attachments are encrypted.

S2.0 – Protection from Unauthorized Access

S2.1 – To prevent the possibility of unauthorized access, email messages containing confidential data may not be downloaded to local folders in the email client or in any other way stored on local storage media.

S2.2 – Email accounts that are used for transmitting confidential data must comply with the University's standards for strong passwords and the password must be protected from exposure.

Implementation Guidelines

- **Email Encryption:**
  - For transmission of email messages containing confidential data within the University, encryption of these messages can be accomplished by enabling the encryption feature in Lotus Notes or Mail Anywhere.
  - For transmission of email messages containing confidential data to external recipients (i.e. over the Internet) encryption of these messages can be accomplished using a third party encryption technology such as PGP or Thawte or by using a self-decrypting archive file that uses a unique key issued to the recipient.

.

Enforcement

Violation of this standard could result in disciplinary actions and/or the suspension of email privileges.

Exceptions

Requests for exceptions to the requirements of this standard should be made to the VCU Chief Information Officer. Please use the Security Standard Request for Exception form that is located on the VCU security website and send the completed form (by hard copy or email) to the VCU Chief Information Officer.

Review Frequency: Annually or as needed

Authority: VCU Chief Information Officer
VCU Security Officer

In Compliance with: VCU Security Standard on Electronic Sensitive Information and Privacy
COV ITRM Information Technology Security Standard SEC 501-01
HIPAA Security and Privacy Rules:

- 164.312(a) (1) Unique User Identification
- 164.312(b) Audit Controls
- 164.312(d) Authentication
- 164.312(c)(1) Integrity
- 164.312(e)(1) Transmission Security, Encryption
- 164.310(d) Backup and Storage