Virginia Commonwealth University
Technology Services

Security Standard for Electronic Confidential Information and Privacy

Effective Date: *April 2006*
Compliance Date: *September 2007*
Revision Date: *August 8, 2007*

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 units that create, receive, transmit, use, disclose and maintain confidential information in electronic format. The purpose is to define the Unit-based performance expectations for the confidentiality, integrity, availability and privacy of University-owned electronic confidential information.

Applied Industry Best Practices of:

- SANS Software Security Institute
- Center for Internet Security Consensus Security Benchmarks
- Open Web Application Security Project (OWASP)
- National Institute of Standards Technology (NIST)

Requirements of the Standard

S1.0

Each VCU unit must establish methods and criteria designed to identify and classify the types of electronic confidential information that are created, used, disclosed, maintained or transmitted by the unit. The following “types” of electronic confidential information have been established by Technology Services as an enterprise-wide classification of “confidential” and must have safeguards applied against unauthorized disclosure or unprotected transmission.

- Protected Health Information;
- Student Education Records;
- Financial Records;
- Contract Information;
- Employee Personnel Records;
- Protected Research and Intellectual Information
- Technical Information;
- Facility and Plant Operations Security Information (floor plans, building control systems and communications systems);
- Investigative and court information

S2.0

Each unit with confidential data must identify a specific position within the organization that is authorized to grant access to and authenticate individuals requesting use or disclosure of such information. The VCU Data Classification Guidelines can be used to help units access the confidentiality of their data and systems.

S3.0

Each unit must have a process that classifies the confidentiality and sensitivity of unit-based data that are created and maintained on information systems and workstations. The VCU Data Classification Guidelines can be used to help units identify data confidentiality.

S4.0

All electronic confidential information, University information systems, servers and workstations are considered to be owned by the University unless otherwise determined by University processes.

S5.0

Each unit must have a process designed to ensure the protection of personally identifiable data under their control from unauthorized access, modification or destructions. Personally identifiable information can be used or disclosed only as authorized by law or regulation and to carry out Unit's operations.

Implementation Guidelines

Technology Services' Information Security Group will periodically perform risk assessments of unit operations and systems in order to identify and protect confidential information**.**

Enforcement

Violation of this standard could result in personnel disciplinary actions.

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 to the VCU Chief Information Officer.

Review Frequency:	Annually or as needed
Authority:	VCU Chief Information Officer VCU Information Security Officer
In Compliance with:	COV ITRM Information Technology Security Management Standard SEC 501-01 VCU Computer and Network Resources Use Policy VCU Data Classification Guidelines