Virginia Commonwealth University
Information Security Standard

Title: **Data Classification Standard**

Scope: This document provides the classification requirements for all data generated, processed, stored, transmitted, or used by all VCU faculty, staff, students, contractors, business partners, IT service providers, and other employees on behalf of VCU. This document is not intended to be used with data that is personally owned by individual employees, where if lost or stolen, has no negative impact on VCU.

Any unauthorized access or loss of Category I data or equipment containing Category I data should be reported according to the instructions defined in section VI of this standard.

Approval Date: February 6, 2012

Effective Date: February 6, 2012

Compliance Date: July 1, 2012

Authority: VCU Information Security Officer

Review Frequency: Annually, or as needed

Revision History:

Version	Date	Revision Issuance
0.1	June 1, 2011	Initial draft complete
0.2	July 15, 2011	Reviewed by TS Directors
0.3	August 22, 2011	Modifications made to definitions
0.4	September 6, 2011	Reviewed by TAC
0.5	February 6, 2012	Final modifications
1.0	February 6, 2012	Standard approved

This standard supersedes the following archived standards:
VCU Data Classification Guidelines – January, 2008
VCU Security Standard for Electronic Confidential Information and Privacy – April 2006

Table of Contents

Contents

I. PURPOSE

This standard defines the categories of data generated, processed, stored, transmitted, or used by the Virginia Commonwealth University. This document is intended to be used by VCU data stewards to determine the sensitivity of the data used within their environment. Further, this standard delineates the requirement for the identification and classification of data used within the VCU.

II. DEFINITIONS

Breach Notification – Notification to the general public of the compromise of personal information through various communication mechanisms as required by the federal and state regulations and statutes.

HIPAA Covered Entity - Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities. Covered entities can be institutions, organizations, or persons.

Researchers are covered entities if they are also health care providers who electronically transmit health information in connection with any transaction for which HHS has adopted a standard. For example, physicians who conduct clinical studies or administer experimental therapeutics to participants during the course of a study must comply with the Privacy Rule if they meet the HIPAA definition of a covered entity.

Data Custodian - An individual or organization in physical or logical possession of data for Data Stewards. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems. The Data Custodians are directly responsible for the physical and logical security of the systems that are under their control.

Data Steward – The Data Steward is a University director or equivalent employee who oversees the capture, maintenance and dissemination of data for a particular academic or business operation. The Data Steward is responsible to ensure data quality, develop consistent data definitions, sensitivity classifications, determine data aliases, develop standard calculations and derivations, define security requirements, document all appropriate “business rules” and monitor data quality within the source system and/or data warehouse. The Data Steward is also responsible for communicating data protection requirements to the Data Custodian; defining requirements for access to the data.

III. CATEGORIZATION

The following section of this document delineates the categories of data generated, processed, stored, transmitted, or used by all VCU faculty, staff, vendors, and other employees on behalf of VCU. All aforementioned data is to be classified into one of the following three categories.

Category I.

All data that require breach notifications in the event of improper release as governed by Federal, State, industry regulations, and / or other civil statutes. Improper access and / or release of such data can result in potential regulatory sanctions, fines and damage to the institution's mission and reputation. Category I data includes all non-publicly available personally identifiable information (PII) that contain any combination of the identifiers as defined in *Appendix A: Personally Identifiable Information.*

Additionally, if the department, division, or individual is considered a *HIPAA covered entity*, or is tasked to handle protected health information *(Appendix B)* from a *HIPAA covered entity* in the course of providing a health care service, then any combination of identifiers defined in *Appendix B* is considered Category I data.

Publicly available information such as the directory information that is lawfully made available to the general public is not considered as Category I information. The FERPA directory information as defined by the Virginia Commonwealth University is shown in *Appendix C*. All other student educational information not specifically listed, including grades, courses, days and times of course meetings, withdrawals and suspensions are considered Category I data.

Category II.

All proprietary data that if improperly released has the potential to cause harm to the institution, its mission or its reputation, but do not require breach notifications. Such data includes proprietary and properly de-identified research information, operational documentations, contractual information, intellectual property, internal memorandums, salary information, and all other information releasable in accordance with the *Virginia Freedom of Information Act (Code of Virginia 2.2-3700).*

Category III.

All non-proprietary data that is considered publicly available for unrestricted use and disclosure, where if lost or illegitimately modified, these data will generate no negative impacts to individual departments, schools, colleges, or the institution as a whole. Such information is available to all members of the University community and to all individuals and entities external to the University community. Such data can make up public website information,

public press release, public marketing information, directory information, and public research information.

IV. REQUIREMENTS

A. Each VCU academic or administrative unit, in conjunction with its Data Steward, must establish methods and criteria designed to identify, classify, and document the classification of the types of data that are generated, stored, processed, disclosed, transmitted, or used by the unit in accordance to the categories defined in this standard.

B. The classification of data must be reviewed by the VCU unit on an as needed basis, or every three years.

C. Data Stewards, in conjunction with Data Custodians, shall identify the type(s) of data handled by each VCU IT system in which their data is captured, maintained or disseminated.

D. The Data Steward, in consultation with Data Custodian, shall determine whether their data is subject to Federal or state regulatory requirements.

E. The Data Steward, in consultation with Data Custodian shall determine the level of potential harm of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.

F. The Data Custodian shall classify the IT system as sensitive if any type of data handled by the IT system is used to generate, store, process, or transmit Category I information.

G. The Data Custodian shall review the IT system and data classifications with the Data Steward and obtain Data Steward's approval of these classifications.

H. The University Information Security Officer (ISO) shall verify and validate that all VCU IT systems and data have been classified for sensitivity.

I. The ISO shall communicate approved IT system and data classifications to Data Custodians, Data Stewards, and end-users.

J. The ISO shall use the information documented in the sensitivity classification as a primary input to the Risk Assessment process

V. EXCEPTION REQUESTS

Exceptions to these standards may be requested by submitting an Information Security Policy and Standard Exception Request Form to the VCU Information Security Officer according to information ownership. This form is located in the *Appendix D* of this document.

The Information Security Officer shall have authority to approve or deny any exception request. In the event a request is denied, the requesting party may submit an appeal to the respective Chief Information Officer for final arbitration.

VI. REPORTING LOSS OR THEFT OF EQUIPMENT OR DATA

In the event a computer workstation, mobile device, or storage media is lost or stolen, the theft or loss must be reported immediately to the VCU police at 828-1196. In the event that Category I data is suspected to be improperly accessed, lost, or stolen, the theft or loss must be reported immediately to the VCU Information Security Office at 828 – 1015.

VII. COMPLIANCE

Compliance with this Data Classification Standard is the responsibility of all individuals who generate, store, process, transmit, or use VCU data. This standard establishes standards for these individuals' actions in recognition of the fact that these individuals are provided unique system and information access, and that non-compliance to this agreement will be enforced through sanctions commensurate with the level of infraction.

Violation of any of the foregoing requirements may subject an individual to temporary loss of access to information, and in severe cases, disciplinary action including, but not limited to, suspension or dismissal, in accordance with the *Employee Standards of Conduct*, the *University's Rules and Procedures*, the *Promotion and Tenure Policies and Procedures*, the *University Policy for Administrative and Professional Faculty and Faculty Holding Administrative Appointments*, and/or any other applicable University procedures. In addition, non-compliance may be violations of local, state, or federal laws or regulations. Violations may result in penalties such as fines and imprisonment.

All individuals who generate, store, process, transmit, or use VCU data are expected to read, understand and agree to the responsibilities defined in this standard and any published revisions of this standard.

Appendix A. Personally Identifiable Information (Category I)

FERPA (Family Educational Rights and Privacy Act), GLBA (Gramm-Leach Bliley Act), and the Code of Virginia place significant privacy and security requirements on educators, administrators, and researchers. The following section lists personally identifiable information as defined by the *Code of Virginia 18.2-186.6* and *Code of Virginia 32.1-127.1:05*.

Names, including first name or first initial, and last name in combination with ***and linked to*** anyone or more of the following identifiers:

1. Any information related to an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or

2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

3. Social Security Number

4. Driver's license number or state identification card number issued in lieu of a driver's license number

5. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

Appendix B. Protected Health Information (Category I)

HIPAA (Health Insurance Portability and Accountability Act) defines 18 identifiers. Protected Health Information is defined as Information containing any one or combination of the following 18 identifiers associated with a person's past, present, or future:

- physical or mental health or condition; or
- delivery of or payment of health care services

1. Names
2. All geographic subdivisions smaller than a state (except the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000).
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers and telecommunication access codes
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers, including driver's license, state or federal identification numbers, employee identification numbers, and professional certification numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retina, and voice prints
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual including mother's maiden name and electronic signatures.

Appendix C. FERPA Directory Information

The following information is defined as the FERPA directory information by the Virginia Commonwealth University and is publically available. Students may request that this data is not released to the public. Additional information regarding to FERPA may be obtained from the *VCU enrollment services website*.

1. Student name
2. Date admitted
3. Birthdate
4. Mailing address and telephone number
5. Local address and telephone number
6. University e-mail address
7. Semesters of attendance
8. Major(s)
9. Minor
10. Specialization
11. School
12. Full- or part-time status
13. Classification (freshman, sophomore, etc)
14. Degree sought
15. Honors and awards
16. Degrees and dates received
17. Participation in officially recognized intercollegiate sports, weight, height, hometown, parents' names and previous school(s) attended (for members of athletic teams)
18. Photograph
19. Emergency Contact Information
20. Student ID (V number)

Appendix D. Exception Request Form

VCU Information Security Policy and Standard Exception Request Form

Requester Name / Role:	Unit Name:
Authoritative Unit Head:	Contact Phone:
Requirement to which an exception is requested:	Date:

1. Provide the business or technical justification:

2. Describe the scope, including quantification and requested duration (Not to exceed 1 year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify any unmitigated risks:

6. When will compliance to policy or standard be achieved?

By submitting this form, the Authoritative Unit Head acknowledges that they have evaluated the business issues associated with this request and accepts any and all associated risks as being reasonable under the circumstances.

Authoritative Unit Head Signature: _____

Date:

VCU / VCUHS Information Security Officer (ISO) Use Only	
Approval: ☐ Approved ☐ Denied	Comments:
Signature: _____	Date:

VCU / VCUHS Chief Information Officer (CIO) Use Only (Used for Appeal)	
Approval: ☐ Approved ☐ Denied	Comments:
Signature: _____	Date: