



OIT 62.204: IT System and Data Sensitivity Classification

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

IT System and Data Sensitivity Classification addresses protecting University information and IT systems commensurate with sensitivity and risk, including system availability needs. This is a central component of the University information security program and allows the University to determine how these factors apply to its IT systems and data.

II. Purpose

The IT System and Data Sensitivity Classification policy identifies the steps necessary to classify all IT systems and data according to their sensitivity with respect to the following three criteria:

- Confidentiality, which addresses sensitivity to unauthorized disclosure;
- Integrity, which addresses sensitivity to unauthorized modification; and
- Availability, which addresses sensitivity to outages.

Sensitive data is 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. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. The University must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

The ISO shall:

1. Identify or require that the Data Owner identify the type(s) of data handled by each University IT system.
2. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.

Example: Some IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc.

3. Determine or require that the Data Owner determine the potential damages to the University 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.

Example: Data Owners may construct a table similar to the following table. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration of one way to accomplish this.

System ID: ABC123	Sensitivity Criteria		
Type of Data	Confidentiality	Integrity	Availability
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

4. Classify the IT system as sensitive if any type of the data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.

Note: The University should consider classifying IT systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability.

5. Review IT system and data classifications with the Agency Head or designee and obtain Agency Head or designee approval of these classifications.
6. Verify and validate that all University IT systems and data have been reviewed and classified as appropriate for sensitivity.

7. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.
8. Require that the University prohibit posting any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating controls, and all residual risks.
9. Use the information documented in the sensitivity classification as a primary input to Policy 62.206 Risk Assessment

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.