RADFORD UNIVERSITY

Information Technology Policy and Procedures

Standard: Data and System Classification

Policy Title: Data and System Classification Standard	**Approval Date: 8/10/2010**
Policy ID: 5102s	**Effective Date: 5/18/2020**
Oversight Executive: VP for IT & CIO	**Review Date: 7/1/2023**

1. Purpose

The purpose of this standard is to define data and system classification criteria, responsibilities and requirements.

2. Policy

A. **Data Classifications** – Radford University defines three (3) data classifications used by Data Owners to classify University data:

Highly Sensitive - University data which, because of its potential risk in the event of disclosure, alteration, or destruction, is approved for use only on a very limited basis and with special security precautions. This includes personally identifiable information that can lead to identity theft exposure. The following data is defined as Highly Sensitive:

a. Social Security Number;
b. Driver's license number or state identification number issued in lieu of a driver's license number;
c. Passport or Visa information/number;
d. Financial bank/account numbers, credit card or debit card numbers; or
e. Health information, that if exposed, can reveal an individual's health condition and/or history of health services use.

Protected - University data that is private or confidential, is not intended to be disclosed publicly, and/or is subject to state or federal regulation. Access to Protected data is granted on a need-to-know basis for a specific business use between University staff, IT systems, or other parties when authorized. Examples of Protected data include student data as defined as confidential by the Family Educational Rights and Privacy Act (FERPA), employee performance evaluations, confidential donor information, or other information defined by the University, Federal or State regulations as confidential.

Public - University data intended for general public use (e.g. university course listings, publicity and news articles, directory listings, etc.).

B. **System Classifications** – Radford University defines two (2) system classifications:

Sensitive System– systems where confidentiality, integrity or availability are rated as HIGH.
Non-Sensitive System – systems that are not classified as Sensitive.

3. Procedures

System Owners and Data Owners classify data and system sensitivity using the matrix provided below. Complete the matrix with the following information:

1. **System Name**: enter the name of the system.
2. **System Owner**: enter the name of the System Owner.
3. **Data Owner**: enter the name of the Data Owner.
4. **Data Classification**: classify the data contained within the system as Highly Sensitive, Protected, or Public.
5. **System Sensitivity**: classify the Confidentiality, Integrity and Availability of the system as HIGH, MEDIUM, or LOW depending on the level of impact to business operations.
6. **System Classification**: classify the system as **SENSITIVE** if one or more of the System Sensitivity classifications are HIGH. Otherwise, the system is **NON-SENSITIVE**.

IT System Classification Matrix

IT System Classification Matrix			
System Name:			
System Owner:			
Data Owner:			
Data Classification	**Highly Sensitive**	**Protected**	**Public**
System Sensitivity	**High**	**Medium**	**Low**
Confidentiality: the extent to which data must be protected against unauthorized disclosure to individuals or systems. **HIGH** - unauthorized disclosure of information could be expected to have a ***SEVERE*** adverse effect on university operations, university assets, individuals or university reputation. **MEDIUM -** unauthorized disclosure of information could be expected to have a ***SERIOUS*** adverse effect on university operations, university assets, individuals or university reputation. **LOW -** unauthorized disclosure of information could be expected to have limited to no adverse effect on university operations, university assets, individuals or university reputation.			

Integrity: the extent to which data or information systems must be protected from intentional or accidental unauthorized modification or destruction. **HIGH** - unauthorized modification or destruction of information could be expected to have a ***SEVERE*** adverse effect on university operations, university assets, individuals or university reputation. **MEDIUM -** unauthorized modification or destruction of information could be expected to have a ***SERIOUS*** adverse effect on university operations, university assets, individuals or university reputation. **LOW -** unauthorized modification or destruction of information could be expected to have limited to no adverse effect on university operations, university assets, individuals or university reputation.			
Availability: the extent to which data or information systems are available and accessible for authorized use. **HIGH** - disruption of access to or use of information or an information system could be expected to have a ***SEVERE*** adverse effect on university operations, university assets, individuals or university reputation. **MEDIUM -** disruption of access to or use of information or an information system could be expected to have a ***SERIOUS*** adverse effect on university operations, university assets, individuals or university reputation. **LOW -** disruption of access to or use of information or an information system could be expected to have limited to no adverse effect on university operations, university assets, individuals or university			
System Classification			

The example below shows a completed matrix for ABC Systems:

IT System Classification Matrix			
System Name: ABC Systems			
System Owner: J. Smith			
Data Owner: P. Jones			
Data Classification	**Highly Sensitive**	**Protected**	**Public**
	X		
System Sensitivity	**High**	**Medium**	**Low**
Confidentiality: the extent to which data must be protected against unauthorized disclosure to individuals or systems. **HIGH** - unauthorized disclosure of information could be expected to have a ***SEVERE*** adverse effect on university operations, university assets, individuals or university reputation. **MEDIUM -** unauthorized disclosure of information could be expected to have a ***SERIOUS*** adverse effect on university operations, university assets, individuals or university reputation. **LOW -** unauthorized disclosure of information could be expected to have limited to no adverse effect on university operations, university assets, individuals or university reputation.	**X**		
Integrity: the extent to which data or information systems must be protected from intentional or accidental unauthorized modification or destruction. **HIGH** - unauthorized modification or destruction of information could be expected to have a ***SEVERE*** adverse effect on university operations, university assets, individuals or university reputation. **MEDIUM -** unauthorized modification or destruction of information could be expected to have a ***SERIOUS*** adverse effect on university operations, university assets, individuals or university reputation. **LOW -** unauthorized modification or destruction of information could be expected to have limited to no adverse effect on university operations, university assets, individuals or university reputation.	**X**		

Availability: the extent to which data or information systems are available and accessible for authorized use. **HIGH** - disruption of access to or use of information or an information system could be expected to have a ***SEVERE*** adverse effect on university operations, university assets, individuals or university reputation. **MEDIUM -** disruption of access to or use of information or an information system could be expected to have a ***SERIOUS*** adverse effect on university operations, university assets, individuals or university reputation. **LOW -** disruption of access to or use of information or an information system could be expected to have limited to no adverse effect on university operations, university assets, individuals or university		**X**	
System Classification	**Sensitive**		

4. Definitions

System Owner - the University manager who is responsible for the operation, documentation and maintenance of a University IT system.

Data Owner – the University manager, designated by the System Owner, who is responsible for the policy and practice decisions regarding data. Data Owners approve or deny access to University data.

5. Related Information

IT-5102 Data Storage and Media Protection Policy
IT-5003s IT Security Standard

6. Policy Background

7. Approvals and Revisions

Approved: August 10, 2010 by Vice President for Information Technology & CIO, Danny Kemp

Revised: July 10, 2017
Minor change to reference IT-5003s IT Security Standard, moved roles to definitions, updated classification matrix
Approved: July 10, 2017 by Vice President for Information Technology & CIO, Danny Kemp

Revised: May 18, 2020
Minor wording changes to reference IT-5003s IT Security Standard definitions, updated system classification matrix and definitions.
Approved: May 18, 2020 by Vice President for Information Technology & CIO, Danny Kemp