1. **Purpose**
The purpose of this standard is to define data and system classification responsibilities and requirements.

2. **Policy**

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

- **Highly Sensitive** - University data which, because of its associated legal restrictions or potential security ramifications, is approved for use only on a very limited basis and only with special security precautions. This includes personal information that can lead to identity theft exposure. A few examples of highly sensitive data are social security numbers, financial card numbers and passport information.

- **Protected** - University data individually requested and approved by a Data Owner for a specific business use and which is subject to the general provisions associated with university information security policy and may be subject to state and or federal law. One example of protected data would be FERPA protected data.

- **Public** - University data which can be shared without restriction with the general public (e.g. university course listings, publicity and news articles, directory listings, etc.).

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

- **Sensitive** – a system is classified as Sensitive based on confidentiality, integrity or availability. Systems containing Highly Sensitive data automatically classify as Sensitive.

- **Non-Sensitive** – a system is classified as Non-Sensitive when confidentiality, integrity or availability are low and/or the Data Classification is Public.

3. **Procedures**
System Owners and Data Owners classify systems using the matrix provided below. Confidentiality, Integrity and Availability are rated as High, Medium, or Low depending on the level of impact to the business operations.
### Example IT System/Data Classification Matrix

<table>
<thead>
<tr>
<th>Criteria</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality:</strong> Only authorized users may access the system and its data. It is imperative that unauthorized access does not occur.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrity:</strong> Only authorized data alterations by authorized users. It is imperative that unauthorized alterations (to system configuration or data) do not occur.</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Availability:</strong> The system is reliably made available and accessible. It is imperative that the system be made available for business purposes.</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Classification:</th>
<th>Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Classification:</td>
<td>Highly Sensitive</td>
</tr>
</tbody>
</table>

### 4. Definitions

**System Owner** – University business manager responsible for having an IT system operated and maintained. IT Systems may have only one System Owner.

**Data Owner** – University managers responsible for the policy and practice decisions regarding 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