1. **Purpose**
The purpose of this standard is to clearly define the roles, responsibilities and definitions of data and system classifications at Radford University.

2. **Roles and Responsibilities**
These roles and responsibilities are assigned to individuals, and may differ from the Radford University role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. These roles and responsibilities should be included in individual job descriptions.

**System Owner**
The System Owner is the Radford University business manager responsible for having an IT system operated and maintained. IT Systems may have only one System Owner. The System Owner’s responsibilities include the following:

- Require that the IT system users complete IT security awareness training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.

- Manage system risk and develop any additional information security policies and procedures required to protect the system in a manner commensurate with risk.

- Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

- Designate a System Administrator for the system.

- Complete annual role-based training.

**Data Owner**
The Data Owner is the Radford University manager responsible for the policy and practice decisions regarding data, and is responsible for the following:
- Evaluate and classify sensitivity of the data.

- Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

- Communicate data protection requirements to the System Owner.

- Define requirements for access to the data.

- Complete annual role-based training.

**System Administrator**
The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists Radford University management in the day-to-day administration of IT systems, and implements security controls and other requirements of Radford University's information security program on IT systems for which the System Administrator has been assigned responsibility. System Administrators must complete annual, role-based training. System Administrators may not be a Data Owner or a System Owner. Each system should have at least two System Administrators (one primary, one secondary).

**Data Custodian**
Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

- Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

- Establishing, monitoring, and operating IT systems in a manner consistent with Radford University Information Security policies and standards.

- Providing Data Owners with reports, when necessary and applicable.

- Completing annual role-based training.

**IT System Users**
All users of Radford University IT systems including employees, contractors and vendors are responsible for the following:

- Reading and complying with Radford University IT policies.

- Reporting breaches of IT security, actual or suspected, to the ISO.

- Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

- Completing annual IT Security Awareness training.
3. **Data Classifications**
   Radford University has three (3) data classifications for use by Data Owners when classifying 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. A few examples of highly sensitive data are social security numbers, financial card numbers and passport information. For a more detailed definition of Highly Sensitive Data please read Radford University Policy 5102 (Data Storage and Media Protection).

   **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.).

4. **System Classifications**
   Radford University Data and System Owners have two (2) system classifications for use when classifying systems.

   - **Sensitive** – The system is sensitive based on confidentiality, integrity or availability.
   - **Non-Sensitive** – The system is not sensitive.

   Note – The system classification must be **Sensitive** and the data classification must be **Highly Sensitive or Protected** when any single criteria has a rating of high.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**An Example IT System/Data Element**

<table>
<thead>
<tr>
<th>System Classification:</th>
<th>Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Classification:</td>
<td>Highly Sensitive or Protected</td>
</tr>
</tbody>
</table>
5. **Definitions**

**Data Classification:** The process of categorizing data based on confidentiality, integrity and availability.

**System Classification:** The process of categorizing systems based on confidentiality, integrity and availability.

**Role based training:** Specific annual training that addresses the roles and responsibilities of System Owners, Data Owners, Data Custodians and System Administrators. This training is in addition to annual IT Security Awareness training.

**Confidentiality:** Only authorized users may access the system and its data. It is imperative that unauthorized access does not occur.

**Integrity:** Only authorized data alterations by authorized users. It is imperative that unauthorized alterations (to system or data) do not occur.

**Availability:** The system is reliably made available and accessible. It is imperative that the system be made available for business purposes.

6. **Approvals and Revisions**

Approved by: Vice President for Information Technology & CIO