Effective Date of Policy: 5/1/25
Responsible Department: Information Technology
Last Update: First Version
Permanent or Temporary/Interim Policy: Permanent

Data Security Policy

Purpose

The purpose of this data security policy is to ensure that all data generated, transmitted, and stored by Roanoke College is safeguarded from unauthorized access, use, disclosure, modification, or destruction. This policy is designed to protect the confidentiality, integrity, and availability of all College data, including but not limited to student records, financial information, research data, and intellectual property (including student work).

Policy

All individuals or entities with access to Roanoke College data are responsible for complying with this policy, as well as any other relevant policies, procedures, or regulations. Specific responsibilities include:

1. Protecting College data from unauthorized access, use, disclosure, modification, or destruction.
2. Using only Information Technology approved devices, systems, and networks to access and store College data.
3. Not sharing your individual account credentials with anyone other than Information Technology when needed for technical support.
4. Not sharing system passwords, access codes, or other authentication credentials with unauthorized individuals or entities.
5. Reporting any suspected or actual data security incidents, breaches, or violations to the Chief Information Officer or member of the IT leadership immediately.
6. Complying with all legal and regulatory requirements related to data security and privacy, including but not limited to FERPA, HIPAA, and PCI DSS.

Data Classification

Roanoke College data must be classified based on its sensitivity, criticality, and confidentiality. The following classifications are used:

1. Public: Data that is intended for public dissemination and does not contain any sensitive or confidential information.

2. Internal: Data that is intended for internal use only and is not intended for public dissemination. This data may contain some sensitive information.
3. Confidential: Data that is highly sensitive and confidential, such as student records, financial information, research data, and intellectual property.

Data Handling

All individuals or entities with access to Roanoke College data must adhere to the following guidelines:

1. Public data can be shared freely without restriction.
2. Internal data can be shared within the College community on a need-to-know basis, and only with individuals who have a legitimate business need to access the data.
3. Confidential data must be protected from unauthorized access, use, disclosure, modification, or destruction. Access to confidential data must be strictly controlled, and only authorized individuals or entities should be granted access.

Access Controls

Access to Roanoke College data must be strictly controlled, and access controls must be implemented to ensure that only authorized individuals or entities can access the data. Access controls must include the following:

1. Authentication: All individuals or entities accessing Roanoke College data must be authenticated using strong passwords, two-factor authentication, or other appropriate authentication mechanisms.
2. Authorization: Access to Roanoke College data must be authorized based on the individual or entity's role, responsibilities, and business need.
3. Monitoring: All access to Roanoke College data must be monitored, and any suspicious activity must be reported immediately.

Data Storage and Transmission

Roanoke College data must be stored and transmitted securely to prevent unauthorized access, use, disclosure, modification, or destruction. The following guidelines must be followed:

1. Data storage: Roanoke College data must be stored on secure servers, systems, or devices that are maintained by Roanoke College and updated regularly.
2. Data transmission: Roanoke College data must be transmitted using secure channels, such as SSL/TLS, VPN, or other appropriate encryption mechanisms approved by Information Technology.
3. Backup and recovery: Roanoke College data must be regularly backed up and tested for integrity and recoverability.

Definitions

“Public Data” Data intended for public dissemination that does not contain any sensitive or confidential information.

“Internal Data” Data intended for internal use only, which may contain some sensitive information and is not meant for public dissemination.

“Confidential Data” Highly sensitive and confidential data, such as student records, financial information, research data, and intellectual property.

“Authentication” The process of verifying the identity of individuals or entities accessing Roanoke College data using strong passwords, two-factor authentication, or other appropriate mechanisms.

“Authorization” Granting access to Roanoke College data based on the individual's or entity's role, responsibilities, and business need.

“Data Security Incident” Any suspected or actual event that compromises the confidentiality, integrity, or availability of Roanoke College data.

“Data Transmission” The process of transferring Roanoke College data using secure channels, such as SSL/TLS, VPN, or other encryption mechanisms approved by Information Technology.

“Data Storage” The practice of storing Roanoke College data on secure servers, systems, or devices maintained by the College and updated regularly.