UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-4003	**Policy Title:**	Information Security Policy
Effective:	05/14/2018	**Responsible Office:**	Information Services
Date Approved:	05/14/2018	**Approval:**	Vice President and Chief Information Officer
Replaces Policy Dated:	N/A	**Responsible University Official:**	Vice President and Chief Information Officer

PURPOSE:

This policy and related standards define the framework upon which the University of Richmond's [the "University"] information security program is established and maintained. The policy provides direction for information security related policies, standards, procedures, and guidelines to ensure the confidentiality, integrity, and availability of University information resources.

SCOPE:

This policy applies to anyone who accesses University data, systems, or networks as well as those who design, implement, or manage those information resources.

INDEX:

POLICY STATEMENT:

IRM-4003.1 – Definitions

Application Owner – A business or functional position responsible for managing a business application.

Data Steward - A University official with executive responsibility over a University division or department. Data stewards are those individuals listed as the responsible party in the University's Records and Retention Schedule.

EDUCAUSE - A nonprofit association dedicated to the advancement of higher education through the effective use of information technology. Members include representatives from institutions of higher education, higher education technology companies, and other related organizations.

Family Educational Rights and Privacy Act (FERPA) - A Federal law enacted to protect access to student records and provide control over the disclosure of information from these records.

General Data Protection Regulation (GDPR) – A European Union privacy law enacted to protect the data and privacy rights of natural persons in the Union.

Gramm-Leach-Bliley Act (GLBA) - A Federal law enacted to control how financial institutions deal with the private information of individuals.

Health Insurance Portability and Accountability Act (HIPAA) - A Federal law enacted to set national standards for the security of electronic-protected health information.

Higher Education Information Security Council (HEISC) – Supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.

Information Security Program – The administrative, technical, or managerial controls used to protect the confidentiality, integrity, and availability of sensitive or protected information that is stored, processed, or transmitted by the University and its affiliates.

Information Security Standard – Specifies requirements for compliance with University information security and technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment, and management of information resources.

National Institute of Standards and Technology Special Publication 800-53 Revision 4 (NIST SP800-53r4) – Provides a catalog of security and privacy controls for information systems and organizations that process sensitive data. It is a risk management framework that is widely used to establish and manage security programs and information technology risks.

Payment Card Industry Data Security Standard (PCI DSS) - A comprehensive set of payment application security requirements designed to ensure the confidentiality and integrity of credit card data.

Red Flags Rule - Requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations.

Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) – Computer security incident response team supporting the research and education community notifying higher education institutions of infected hosts and suspicious network traffic.

User – any individual, including but not limited to faculty, student, staff, contractors, visitors; who access and use University information resources or data.

Virginia Alliance for Secure Computing and Networking (VASCAN) - An organization formed to help strengthen information technology security programs within Virginia. The Alliance was organized and is operated by security practitioners and researchers from several Virginia higher education institutions.

IRM-4003.2 – Policy Statement

The University is required to develop, implement and maintain a comprehensive information security program containing administrative, technical, and operational controls. The University's information security program is based upon best practices recommended in NIST SP800-53r4 and is appropriately tailored to the University's size, complexity, and the nature of its activities.

The program also incorporates security requirements of applicable regulations including, but not limited to, FERPA, PCI-DSS, GLBA, HIPAA, GDPR, and Red Flags Rule. Professional organizations, such as EDUCAUSE, VASCAN, HEISC, and REN-ISAC serve as resources for additional security best practices.

NIST SP800-53r4 and other sources noted above are used to guide development and ongoing enhancement of additional information security policies, as needed.

IRM-4003.3 –Roles and Responsibilities

The Vice President and Chief Information Officer is the institutional point of contact for information security and is responsible for designating the Director of Information Security to coordinate and oversee the information security program.

The Director of Information Security has delegated authority for the selection and implementation of security controls and manages the overall information security program.

Vice presidents, deans, associate/assistant vice presidents and academic/administrative unit leaders shall be responsible for identifying critical and sensitive functions. In addition, they and their staff are responsible for the security, confidentiality, availability, and integrity of data and software stored on individual workstations and centrally managed computer systems to the extent that they have access and or access control.

Vice presidents, deans, associate/assistant vice presidents, and academic/administrative unit leaders are required to designate a data steward for any information resource under their control. They must also designate an application owner for any information resource not centrally managed by Information Services.

This policy also places responsibility on deans, associate/assistant vice presidents and academic/administrative unit leaders to: 1) require appropriate computer use as specified in the policy Acceptable Use Policy, 2) ensure compliance with information technology policies and standards by people and services under their control, and 3) implement and monitor additional procedures as necessary to provide appropriate security of information and technology resources within their area of responsibility.

All users of university information technology resources are required to adhere to the requirements detailed in University of Richmond's Information Security standards and policies related to information security and technology.

IRM-4003.4 – Applicable Regulations

A. Red Flags Rule of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Public Law 108-159, Section 114
B. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
C. General Data Protection Regulation (GDPR) (EU) 2016/679

D. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
E. General Data Protection Regulation (GDPR) (EU) 2016/679
F. Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Public Law 106–102, 113 Stat. 1338
G. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
H. Payment Card Industry Data Security Standard (PCI DSS)
I. SACSCOC *Principles of Accreditation* 12.5 (Student Records)

RELATED POLICIES:

A. Acceptable Use Policy
B. Data Security Policy
C. Policy for Payment Card Acceptance and Security
D. Privacy of Student Records (FERPA) Policy
E. Identity Theft Prevention Program (Red Flags Rule)
F. Legal Notice - Privacy Policy

POLICY BACKGROUND:

Revision History: New Policy 5/14/2018
Revised Related Policies 02/24/2021

POLICY CONTACTS:

Vice President and Chief Information Officer, Information Services
Director of Information Security, Information Services