

Area of Responsibility: BUSINESS INTELLIGENCE AND TECHNOLOGY

Responsible Contact: DIRECTOR

Policy Identification: INFORMATION SECURITY

Effective Date: DATE (Revised: 08/18/2019)

**PURPOSE**

This policy and related standards define the framework upon which the Virginia Union University’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.

**POLICY**

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 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, Family Educational Rights and Privacy Act (FERPA), Payment Card Industry Data Security Standard  (PCI-DSS), Gramm-Leach-Bliley Act  (GLBA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), General Data Protection Regulation(GDPR), and Red Flags Rule. Professional organizations, such as EDUCAUSE, VASCAN, HEISC, and REN-ISAC serve as resources for additional security best practices.

Roles and Responsibilities:

The Director of Business Intellegence and Technology 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 Regarding the Use of Technology and Information Resources, 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 Virginia Union University’s Information Security standards and policies related to information security and technology.

**GLOSSARY**

Family Educational Rights and Privacy Act (FERPA)- The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children’s education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records.

Payment Card Industry Data Security Standard  (PCI-DSS) – The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.

Gramm-Leach-Bliley Act  (GLBA) – The *Gramm*-*Leach*-*Bliley Act* requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides [data privacy](https://searchcio.techtarget.com/definition/data-privacy-information-privacy) and security provisions for safeguarding medical information. The law has emerged into greater prominence in recent years with the proliferation of health [data breaches](https://searchsecurity.techtarget.com/definition/data-breach) caused by cyberattacks and [ransomware](https://searchsecurity.techtarget.com/definition/ransomware) attacks on health insurers and providers.

General Data Protection Regulation(GDPR) – The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

Red Flags Rule – The Red Flags Rule calls for financial institutions and creditors to implement **red flags** to detect and prevent against identity theft. Institutions are required to have a written Identity Theft Prevention Program (ITPP) to govern their organization and protect their consumers.

EDUCAUSE – Educause is a nonprofit association in the United States whose mission is "to advance higher education through the use of information technology".

VASCAN– VASCAN is an alliance that brings together Virginia higher education security practitioners who developed and maintain security programs widely emulated by other institutions, and researchers who create cybersecurity instruction and research programs nationally recognized for excellence.

HEISC – The Higher Education Information Security Council (HEISC) is an organization whose mission is to support higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.

REN-ISAC - The Research and Education Networks Information Sharing and Analysis Center (REN-ISAC) serves over 620 member institutions within the higher education and research community by promoting cybersecurity operational protections and response. REN-ISAC also acts as the Computer Security Incident Response Team (CSIRT) for the research and education community at large, including non-members.

**GOVERANCE – COMMITTEE OR COMPLIANCE ORGANIZATION** (if applicable)