1. Policy: Glossary of Definitions for Information Security Standards

Issued: Approved on December 1, 2022 and shall be effective on September 1, 2023.
Revised:
Last Reviewed: February 2023

2. Policy Purpose:

The purpose of this document is to provide meaning and definition to terms used throughout Rivier Information Security Standards.

3. Scope and Application:

This glossary is applicable to the Standards as they apply to all Rivier University business units, subsidiaries, employees, contractors, and third-party service providers and to all Rivier systems.

4. Definitions:

Position or Office	Responsibilities
Anti-malware	refers to software programs, deployed by Rivier, to prevent and remove software that is malicious in intent from information systems as well as individual computing devices.
Audit	refers to the review of adherence to regulatory guidelines and standards to which Rivier and its employees are responsible.
Authentication	refers to the action of verifying the identity of a user or process.
Business Impact Analysis	refers to the process used to define critical business functions and the impact of downtime to those services. This process also defines the people and technology that support these functions and what recovery requirements are needed to ensure minimal disruption.
Business Owners / Risk Owners / Information Asset Owners	refer to the individual or organizational unit who has business authority or responsibility for a unit of Rivier Information or other Rivier Information Assets. Owners are accountable for identifying and managing risk factors that may impact the confidentiality, integrity, and availability of Information within their business function or span of organizational control.
Business Resiliency	refers to the ability of Rivier employees and information systems to quickly react to disruptions while maintaining continuous business operations.
Common Vulnerability Scoring System (CVSS)	refers to a published standard that provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.
Confidential Information	as defined in section 5.2 of the Information Classification Standard, refers to Rivier Information not classified as either Restricted or Public Information. Also, the Confidential Information classification applies by default to Rivier Information that is not otherwise classified as either

	Restricted or Public Information. Please see the Information Classification Standard for examples of Confidential Information.
Cryptography	is the practice of transforming data so that it is interpretable only by authorized persons.
Disaster Recovery	refers to the recovery of information systems that support critical business functions after a significant event that could possibly cause downtime and a disruption to business services.
Rivier Information	as defined in the Information Security Policy, refers to a body of knowledge or data obtained, produced, organized, shared, or managed by Rivier over the course of its business operations. Rivier information may be shared or stored in a physical or electronic manner or may take the form of the spoken word. Rivier information is not easily replaced without funding, skill, knowledge, resources, time, or any combination of these factors. Therefore, Rivier information is considered a critical resource from the standpoint that it is used to build knowledge, accomplish business objectives, and sustain or create organizational value.
Rivier Information Asset	refers to Rivier Information, Rivier Information Systems, facilities, and other resources or activities related to processing Rivier Information. The value of an Rivier Information Asset is determined by the volume and impact of organizational activities and requirements that rely on them to achieve business objectives.
Rivier Information Systems	refers to computing hardware, software and media components, including websites and web-based services for creating, collecting, processing, storing or delivering Rivier Information, or supporting operational tasks that involve Information. These computing hardware, software and media components are owned, leased, subleased, licensed, sublicensed, or subscribed to and primarily controlled or managed by Rivier.
Rivier Staff	refers to all Rivier employees – faculty and staff, contractors and temporary staff.
Encryption	refers to the process of rendering information and data unreadable to unauthorized systems and users.
Information Security	("InfoSec") refers to the team who is responsible for defining and managing implementation and continuous improvement of Rivier's Information Security Program, as defined in section 4.5 of the Information Security Policy.
Information System Owners	(or "System Owners") refers to those individuals responsible for computing hardware, software and media components that collect, process, store, or deliver Information, or perform operational tasks that involve Information. System Owners are responsible for defining the processes to meet the business objectives or requirements established by Business Owners / Risk Owners / Information Asset Owners.
Information User (or "User")	refers to an individual authorized to access, use, share, or store Rivier Information.
Malware	refers to software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing	refers to false emails that are sent from malicious actors that imitate those sent from reputable companies or coworkers to coax the user into providing sensitive information (such as passwords) or to click on malicious links.
Private/Trusted Network	refers to an Rivier controlled or IS approved network that will have rules and protections established to create a more secured environment.
Public Information	as defined in section 5.2 of the Information Classification Standard, refers to all Information approved for, and intentionally released to, the public domain. Though risk factors associated with it may result in little or no risk to Rivier, Public Information may still be controlled and protected to ensure its integrity and availability.
Public/Un-Trusted Network	refers to a network that the general public can access with little restrictions or networks that have unknown security controls and have not been approved by INFOSEC as trusted.
Remote Access	refers to accessing Rivier information systems and networks from a location other than a designated Rivier office space.
Restricted Information	as defined in section 5.2 of the Information Classification Standard, refers to the most sensitive classification of Rivier Information. Restricted Information refers to non-public Rivier information that is not classified as Confidential Information. Examples include, but are not limited to, student education records, personal data, contact information, electronic health information, cardholder data (e.g., credit card payment account numbers and related data), authentication secrets (e.g., passwords or login tokens used to access Information Systems), as defined in the Information Classification Standard.
Role-based Access	refers to a method of controlling User access to information or network resources based on the role of the individual. A User's privileges to information or network resources is usually further defined or restricted in relation to their ability within an Information System to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the enterprise.
Software as a Service (SaaS)	refers to an application or service that is accessible over the internet and generally doesn't require any software to be installed locally.
Technical Vulnerability	refers to a flaw or weakness in an information system that can leave it open to attack.
Third Party Service Providers	(or "Third Parties") are external business entities with whom Rivier enters into an agreement with and which have access to, store, or process Rivier Information. Third Parties may also have access to, or may manage, Information Systems.
Vulnerability Scan	refers to the automatic inspection of an information system to determine potential weaknesses and exploitation paths for would be attackers.

5. Contacts:

Division/ Department	Position or Office	Contact Information

Information Technology	CIO	603-897-8630 / itsupport@rivier.edu