Technology Terms and Definitions

ROWAN UNIVERSITY TERMS AND DEFINITIONS

Title: Technology Terms and Definitions
Subject: Information Resources and Technology
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Date Adopted: 09/06/2018
Last Revision: 03/07/2024
Last Review: 02/11/2022

I. PURPOSE

This document is intended to define common definitions and terms used in IRT policies.

II. TERMS AND DEFINITIONS

Term	Definition
Access Control	The use of computer-controlled entry and locking devices to limit and log access to areas of a physical facility, usually by means of a digitally-enclosed identification card or biometric device.
Administrative Safeguards	Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect the University's information assets and to manage the conduct of the University community in relation to the protection of those information assets.
Affiliates	Individuals who are not current Rowan University faculty, staff, or students. Including, but are not limited to, non-employees of Rowan University School of Osteopathic Medicine (SOM), Cooper Medical School of Rowan University (CMSRU), visiting faculty – both long and short term, visiting scholars, researchers, contractors, subcontractors, vendors, external maintenance/contractors, volunteers, volunteer faculty who are not considered "faculty of record," temporary University employees, and summer program participants.

Alumnus/a	An individual who has received a degree from Rowan University. A student who attended classes but did not graduate from Rowan or receive a diploma is not considered an alumnus/a of the university. An alumnus/a will be classified into exactly one of the following subsets: ○ An inactive alumnus/a is an individual that meets all of the below criteria: ○ Has received a diploma from Rowan University on or before July 1, 2019. ○ Does not have an active Rowan NetID Account. ○ An active alumnus/a is an individual that meets all of the below criteria: ○ Has received a diploma from Rowan University on or before July 1, 2019. ○ Has an active Rowan NetID Account. ○ A future alumnus/a is an individual that meets all of the below criteria: ■ Has receive a diploma from Rowan University after July 1, 2019.
Antivirus	Software that runs on either a server or workstation and monitors network connections looking for malicious software. Antivirus software is generally reactive, meaning a signature file must be developed for each new virus discovered and these virus definition files must be sent to the software in order for the software to find the malicious code.
Application Programming Interface (API)	An Application Programming Interface (API) is a computing interface that defines interactions between multiple software components or sub-components.
Application	A computer program that processes, transmits, or stores University information and which supports decision-making and other organizational functions. It typically presents as a series of records or transactions. These records and transactions are generally accessible by more than one user.
Application Administrator	Rowan staff member who is responsible for granting access and providing support on the application to the Rowan community.
Application Manager	The technology manager who is directly responsible for the development, maintenance, configuration, or functional specifications of the application. He or she is also required to implement, operate, and maintain security measures defined by the information owners.

Asset/Information Asset	Defined as (1) all categories of information and data, including (but not limited to) records, files, and databases, regardless of form and (2) information technology facilities, equipment and software owned, outsourced, or leased by the University. This includes all University IT systems and data, including university owned, leased or managed assets.
Authorized User	A person authorized to access information resources specific to their role and responsibilities, and who has conveyed upon them the expectation of “Least Privilege.”
Automated Tools	Software that executes pre-scripted tests on software applications or hardware devices.
Availability	The expectation that information is accessible by Rowan University when needed.
Breach	Any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
Business (Application) Owner	Business unit that purchased the application using University funds allocated to its budget or purchased using a grant. The business owner may be a technology organization for utility services-type applications, such as Banner and MS Exchange.
Business Impact Analysis (BIA)	A process managed by the Office of Emergency Management that determines the financial and operational impact of a disruption to a business, and the requirements for recovering from the disruption. A business unit uses the BIA to list their business-critical functions and processes and supporting applications.
Business Interruption	An event, whether anticipated or unanticipated, which disrupts the normal course of business operations within the university.

Business Unit	Applies to multiple levels of the university, such as a revenue generating unit or a functional unit (e.g., Compliance, Human Resources, Information Resources and Technology (IR&T), Legal, and Finance). It may also be comprised of several departments.
Business-Critical Function/Process	A function or process which, if compromised, presents a severe financial, operational, or regulatory risk to the business unit and/or to the University as a whole. A business-critical function/process may be supported by an information system owned by the business unit or by an information system that is shared across multiple units.
Cable Modem	Cable companies such as Comcast provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.
Cellular Device	Any device that is capable of out-of-the-box support for cellular voice and data services. This includes, but is not limited to, Apple smartphones and Android smartphones.
Cellular Tablet	Any device that is capable of out-of-the-box support for data services. This includes, but is not limited to, Apple tablets and Android tablets.
Census	Survey administered to an entire population.
Change	Any addition, configuration, modification or removal of any Information System or Information Technology Environment.
Change Management	The formal process for making changes to Information Systems or Information Technology Environment.
Cloud Services	Consumer and business products, services and solutions delivered and consumed on-demand, using the cloud service providers' pooled resources, and delivered over a broad network, such as the Internet.
Computer Devices	Any type of device connected to a network that could become infected with a computer virus. Examples of computer devices would be, but not limited to, workstations, servers, laptops, PDAs, etc.

Confidential Data	Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.
Confidential Information	Sensitive information that is used or held by the University. Considerable loss or harm could occur as a result of unauthorized access, use, or disclosure of this information. Examples include pension /retirement benefit information, personal demographics, and home address/phone number.
Confidentiality	The expectation that only authorized individuals, processes, and systems will have access to Rowan's information.
Cryptographic Algorithms	A mathematical algorithm, used in conjunction with a secret key, that transforms original input into a form that is unintelligible without special knowledge of the secret information and the algorithm.
Cryptographic Keys	A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.
CVSS	The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. In addition to a CVSS score, independent threat intelligence sources contribute toward the overall risk rating.
Data Breach	Any security incident that results in unauthorized access or exfiltration of classified data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies and the media. All data breaches should follow the Incident Response Plan.
Default System Service Accounts	Accounts created by a software vendor to facilitate installation or provide out-of-the-box functionality.

Department Funds	Funds originate from the Departmental budget
Dial-Up Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines.
Digital Sign	Any permanently mounted digital screen that is displayed in a shared space with the purpose of providing general information to multiple people including content players, software, and display units.
Digital Subscriber Line (DSL)	A form of high-speed Internet access used over standard phone lines.
Directory Information	Information identified by Rowan that may be released without prior consent of the student. (See Family Educational Rights and Privacy Act policy (00-01-25-05 00) for a comprehensive list of information categorized as Directory Information.)
Due Care	Steps that demonstrate the University has taken responsibility for the activities that take place within the institution, and has implemented the requisite measures to help protect its assets, including its students, faculty, staff, and the community which we serve.
Electronic Mail	A method of exchanging digital messages from an author to one or more recipients
Electronic Media	Physical object on which data can be stored, such as hard drives, zip drives, floppy disks, compact discs, CD-ROMs, DVDs, USB drives, memory sticks, MP3 players (iPod), Personal Digital Assistants (PDA's), digital cameras, smart phones and tapes.
Employee	An Employee is considered any member in an active pay status according to Human Resources at Rowan University. This includes but is not limited to faculty, staff, affiliates, etc.
Encryption	A process by which data is transformed into a format that renders it unreadable without access to the encryption key and knowledge of the process used. It is also defined as a method of converting information or data into a cipher or code to prevent unauthorized access and requires a passcode or other form of confirming identity to decrypt and access the information or data.

Encryption Key	A password, file or piece of hardware that is required to encrypt or decrypt information, essentially locking and unlocking the data.
Enterprise Information System	An information system and/or server providing services commonly needed by the University community and typically provided by IRT units. Departmental information systems provide services specific to the mission and focus of individual departments, administrative units, or affiliated organizations.
EPHI	Electronic Patient Health Information
External Data	Data for which the University is a custodian, such as video or media that are not directly licensed to Rowan University, but are being offered to the Rowan community via an external partnership.
FERPA	Family Educational Rights and Privacy Act. FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA applies to the records of individuals from the point of first registration until death of the individual.
Fiber Optic Service (FiOS)	A data communications service provided by Verizon that uses fiber optic cables to transfer data.
Firewall	A software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set.
Generic Account	An account that is shared among a group of individuals, and typically used for devices like kiosks and clinical workstations. There is no corresponding employee account (i.e., RUID).
GLBA	Gramm-Leach-Bliley Act. Requires academic institutions to implement policies and controls for protecting financial information. An institution that is compliant with FERPA is considered compliant with GLBA.
Guest Account	Acounts provisioned to individuals not employed by ROWAN, but who have a justifiable business reason to access University resources.

High-Performance Computing Resources	All specialty computing systems, whether a single host or clustered hosts, that are used to address compute-bound, memory-bound, I/O-bound, or storage-bound applications or programs.
HIPAA	Health Insurance Portability and Accountability Act of 1996.
HITECH	Health Information Technology for Economic and Clinical Health Act.
Incident Board	The Incident Board comprises of the department heads of Information Resources & Technology (IRT), Office of Compliance and Corporate Integrity, Office of Risk Management, Information Security Office and General Counsel. The board is to be informed of suspected major incidents and to ensure the timely and appropriate engagement of the University's risk mitigation partners and service providers.
Information Resources & Technology (IRT)	The Rowan University department responsible for the governance of all information and technology.
Information Risk	The potential that a given threat will exploit vulnerabilities of an information asset, thereby causing loss or harm to the information asset. It is measured in terms of a combination of the probability of an event and its impact to the University if the confidentiality, integrity, or availability of an asset is compromised. A risk can be financial, operational, regulatory, and/or reputational in nature.
Information Security Office (ISO)	Department responsible to the executive management for administering the information security functions within the University. The ISO is the Rowan University internal and external point of contact for all information security matters.

Information System	Consists of one or more components (e.g., application, database, network, or web) that is hosted in a University campus facility, and which may provide network services, storage services, decision support services, or transaction services to one or more business units. This includes but is not limited to approved, supported, unsupported, or baselined hardware, network, software or applications.
Information Technology Environment	A group of interrelated Information Systems that support the university business and/or operational requirements
Information Technology Infrastructure Library (ITIL)	Provides a cohesive set of best practice to Information Technology Service Management.
Information Technology Security Board (ITSB)	A unified effort jointly managed by the Chief Information Officer and the Director of Information Security, working closely with the department heads of Human Resources, General Counsel, Public Safety, Facilities Services, Faculty Senate, Research and the Department Chair/Administrative Head of other university units, as warranted. The ITSB governs technical and operational security solutions specific to the University's needs. The ITSB will recommend security measures compliant with this policy, and security best practices.
Infrastructure	The hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network.

Integration Levels for LMS	1. Course: The integration installation is bound to the course only and does not impact parts of the LMS system beyond the course. 2. Account: The integration installation is bound to the account level in the LMS and impacts any courses associated with the account. This level requires sufficient testing to ensure that courses associated with the given account are not negatively impacted. 3. System: The integration installation is bound to the entire system or root level in the LMS and impacts all users and courses. This level requires the most testing and vetting to ensure that courses and users across the entire system are not negatively impacted. 4. Pass-through: The integration installation and functionality is such that it serves as a single sign-on feature for its users where all functionality other than authentication is controlled by the third-party system. Effectively, the LMS passes user credentials to the integration's application. 5. Deep: The integration installation and functionality allows two-way data transmission between the LMS and the third-party application (e.g., grading information is shared for assignments).
Integrity	The expectation that Rowan's information will be protected from improper, unauthorized, destructive, or accidental changes.
Internal Information	Non-sensitive information that is used in the daily operations of the University, such as policies, procedures, training materials and internal meeting information.
Labs	A Lab is considered any room that has two or more computers that will be shared or utilized by two or more individuals.
Learning Management System (LMS)	A Learning Management System (LMS) is a resource for delivering, tracking, and managing course instruction.
Least Privilege	Giving every user, task, and process the minimal set of privileges and access required to fulfill their role or function. This includes access to information systems and facilities. Principles of least privilege limit access to the minimal level required for someone to perform their job responsibilities.
Licensed Premise	A licensed premise is the space that Rowan University leases to a licensee.
Licensee	A licensee or lessee is the renter of the leased space. Typically, this is a person or organization that makes installment payments to use or rent the real estate space.
Licensor	A licensor or lessor is the landlord of the leased space. Rowan University is the organization that owns the leased space.

Live Data	Data accessible to users through systems that are in production environment (i.e., live)
Learning Tools Interoperability (LTI)	The IMS Global Learning Consortium Learning Tools Interoperability (LTI) is a standard protocol for secure data exchange between any Learning Management System and another software.
Malicious Software	Computer code that infects a machine and performs a malicious action. This is sometimes perpetrated by computer viruses, worms, trojans, etc.
Mission-Critical Resource	Mission-Critical Resource includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Typical mission-critical services have a maximum downtime of three consecutive hours or less. Mission-critical resources for Information Security purposes include information assets, software, hardware, and facilities. The payroll system, for example, is a Mission-Critical Resource.
Mobile Device	Including, but not limited to, laptops, tablets (iPad, Android, Windows, etc.) smartphones (Android, iPhone, etc.), and mobile broadband cards (also known as MiFi Hotspots and connect cards).
National Institute of Standard Technology (NIST)	NIST is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.
NIH	National Institutes of Health

Overwriting	Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with "00110101 ", followed by "11001010", then "10010111").
PAN	Credit Card Primary Account Number.
Password Circulation	An attempt to bypass the basic password requirement that prohibits reusing the same password within a specified period of time by changing the password repeatedly within a brief period of time in order to be able to reuse the password earlier than intended by the policy.
PCI	Payment Card Industry.
Personal Identifying Information (PII)	Personal Identifying Information includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or info that can be used to uniquely identify an individual
Phishing	Phishing, also known as spoofing, is the term used for deceitful or fraudulent emails designed to trick people into providing personal information that leaves them vulnerable to identity theft, computer viruses and compromised email accounts. The number and sophistication of phishing scams continue to increase. Other types of phishing can include phony websites or phone calls that ask potential victims to supply or verify their personal information.
Physical Safeguards	Physical measures, policies, and procedures to protect the University’s information assets from natural and environmental hazards, and unauthorized intrusion.
Private Information	Sensitive information that is restricted to authorized personnel and requires safeguards, but which does not require the same level of safeguards as confidential information. Unauthorized disclosure or access may present legal and reputational risks to the University.
Privileged Accounts	An account which, by virtue of function, and /or security access, has been granted special privileges within the computer system, which are significantly greater than those available to the majority of users, including but limited to, local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, and application accounts.

Privileged Information	Refers to attorney-client communication.
Production IT Environment	System components used to provide information technology (IT) service to employees, faculty, patients, students, including but not limited to server hardware and associated operating systems, virtual servers, software applications, virtual applications, networks, data storage, air-conditioning, power supply, server rooms, datacenters, networks, and workstations that are part of the University Environment. This includes IT environments managed by IRT, departments, colleges, and vendors.
Protected Health Information (PHI)	Information covered by the Health Insurance Portability and Accountability Act (HIPAA).
Public Information	Information that is intended, or required, to be shared with the public, such as public-facing website content, public meeting minutes, brochures, and press releases.
Public Network	Any network outside the Rowan University network.
Qualtrics Survey Software	Self-service electronic survey tool.
Remote Access	Connection to a data-processing system from a remote location, for example through a virtual private network.

Removable Media	Including, but not limited to CDs, DVDs, storage tapes, flash devices (e.g., CompactFlash and SD cards, USB flash drives), and portable hard drives.
Research Funds	Funds originate from a Research grant
Restricted Information	Highly sensitive information that is used or held by an agency. Statutory or regulatory penalties, notification provisions, or other mandates could result if the information is accessed, used or disclosed in an unauthorized manner. Examples include Protected Health Information (HIPAA /HITECH), FERPA data, social security information, driver's license information, bank account data and federal tax information.
Risk Assessment	A process used to identify and evaluate risks and their potential impact on the University.
Rowan Community	Includes employees (e.g. faculty, staff, administration, physicians, researchers), students, former students, alumni, non-employees (e.g. contractors, vendors, guest affiliates), covered entities, agents and any other third parties of Rowan University.
RUID	Reserved User ID.
Sanitization	To expunge data from storage media so that data recovery is impossible. The most common types of sanitization are destruction, degaussing, and overwriting.
Sanitized	The process of removing sensitive information from a document or other medium, so that it may be distributed to a broader audience.
Secure Backup (Encryption Recommended)	The process of making a backup copy of information for the purpose of data recovery with security safeguards present to ensure the backup copy of the data remains protected from unauthorized access at all times. This may include physical protections as well as encryption to safeguard the backup information.

Secure Area	Areas within a building that house critical information technology services shall be designated as secure areas.
Secure Shell (SSH)	A secure network protocol for secure network communication services between two networked computers.
Security Awareness Training (SAT)	A method to inform users about the importance of protecting information technology systems and assets. SAT teaches security key concepts and best practices, such as creating a strong password, protecting mobile data, following IT Security policy, and reporting security incidents.
Security Awareness Training Program	The vehicle for disseminating security information for the ROWAN Community. Establishing and maintaining an information security awareness and training program will help to protect ROWAN's vital information resources.
Security Control Owner	The Department, Dean, or VP who is responsible for the area that is being secured by a camera and /or control access system.
Security Event	Any observable occurrence that is relevant to information security. This can include attempted attacks or lapses that expose security vulnerabilities.

Security Incident	A security event that poses a threat to the confidentiality, integrity, and/or availability of University information or information systems, such as an attacker posting a Rowan NetID online, stealing a Rowan confidential database, or spreading a virus through the Rowan Network. 1. Minor Incident: A security incident that does not have a significant impact on institutional services and operations. Often, minor incidents are isolated and not the result of targeted attacks. Furthermore, these types of incidents have a prescribed or known method of resolution, such as a patch installation, malware definition update, or configuration change. These types of incidents are generally resolved by following Standard Operating Procedures (SOPs). Examples of these types of incidents include, but are not limited to: a. Incident involving web page defacement. b. Incidents involving non-targeted email phishing. c. Incident involving malware infections where no sensitive data was at risk. 2. Major Incident: A security incident that has the potential for high impact on institutional reputation, services, information, and operations. Major incidents often involve highly sensitive data. These types of incidents may require the involvement of various teams, internal and external, to assist in the response. Examples of these types of incidents may include, but are not limited to: a. Incidents involving critical vulnerabilities as defined by the Rowan Vulnerability Management Program. b. Incidents involving breaches on enterprise systems of record, especially those that result in extended outages. c. Incidents involving systems that are conducting attacks against other Rowan services or against the services of third parties. d. Incidents involving law enforcement agencies. e. Incidents involving successful targeted social engineering, such as spear phishing.

Sensitive Information	Sensitive Information includes all data, in its original and duplicate form, which contains Protected Health Information as defined by HIPAA Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA) Customer record information, as defined by the Gramm Leach Bliley Act (GLBA) Card holder data, as defined by the Payment Card Industry (PCI) Data Security Standard. Sensitive data also includes any other information that is protected by University policy or federal or state law from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, social security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys. Sensitive Information includes all data, in its original and duplicate form, which contains: • “Personal Identifying Information or PII,” as defined by the New Jersey Identity Theft Protection Act. This includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources. • “Protected Health Information or PHI” as defined by the Health Insurance Portability and Accountability Act (HIPAA). • Student “education records,” as defined by the Family Educational Rights and Privacy Act (FERPA). • “Customer record information,” as defined by the Gramm Leach Bliley Act (GLBA). • “Card holder data,” as defined by the Payment Card Industry (PCI) Data Security Standard. • Information that is deemed to be confidential in accordance with the New Jersey Public Records Act. ?Sensitive Information also includes any other information that is protected by University policy or federal or state law from unauthorized access. Sensitive Information must be restricted to those with a legitimate business need for access. Examples of Sensitive Information may include, but are not limited to, Social Security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys.
Service Accounts	Accounts created by to satisfy specific functions, such as communications between systems or to facilitate other operational requirements.
Service Desk	The University technology service team that receives and handles requests for technical support and requests for new or changes to technology and voice services
SIRT	Security Incident Response Team.
Social Media	Refers to tools that allow the sharing of information and creation of communities through online networks of people.
Spam	Unsolicited usually commercial messages (such as Email, text messages, or Internet postings) sent to a large number of recipients or posted in a large number of places. Some spam is merely annoying, while other spam can cause damage to your computer or the entire campus network.

Spear Phishing	An email targeted at a specific individual or department within an organization that appears to be from a trusted source. For example, a spear phishing email could appear to come from someone at Rowan University and target Rowan University students and employees.
Sponsors	Rowan University full-time faculty or staff, who are eligible to initiate the request for affiliate access to Systems or an Affiliate Access Card.
Single Sign-On (SSO)	An authentication process that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.
Standard Access	Standard Access describes access to Secure Areas that contain protected IT Resources and is restricted to a defined set of individuals who are responsible for the operation of computing and network resources and have a business need for regular access to the facility. Standard Access includes the following user groups: Public Safety/EMT/Life Safety Services, Facilities personnel to maintain environmental services, IRT/Infrastructure Services designated personnel and approved Rowan third-party vendors.
Standard Hardware	A supported computer configuration as designated by Information Resources and Technology.
Survey	A method of gathering information from a sample of people. Modes of administration include electronic surveys, paper surveys and telephone surveys.
Survey Owner	Individual responsible for final decisions on all aspects of survey methodology and analysis. This is the person who creates or owns the survey.
Survey Sample	Group of individuals from a population who will be surveyed.
System Administrator/Data Custodian	A System Administrator or Data Custodian is a person who has technical control over an information asset dataset. Usually, this person has the administrator/admin, sysadmin/sysadm, sa, or root account or equivalent level of access. This is a critical role and it must be executed in accordance with the access guidelines developed by the System Owner.

System Owner/Information Owner/Data Owner/Data Steward	A System Owner, Information Owner, Data Owner or Data Steward has administrative control and has been officially designated as accountable for a specific information asset dataset. This is usually the senior most officer or business unit manager in a division who have planning and management or legal responsibility for the information generated within their functional areas. Some examples include the Registrar and student data; the Chief Financial Officer and financial data; the VP of Human Resources and employee data. In most cases, the Data Owner is not the Data Custodian. They must ensure that the level of protection assigned to their information is relative to its classification and sensitivity. For information regulated by HIPAA, FERPA, or GLBA, the information owner is expected to exercise due care when defining its level of protection.
Technical Safeguards	The technology, policies, and procedures used to control access to and protect the University's electronic information and information systems.
Technology	Electronic or digital products and systems that are capable of being used to render information, consume information or manipulate information
Trade-in Cycle	The frequency with which Rowan-owned and supported computers will be replaced. Constitutes a complete lifecycle for a Rowan-owned and supported device from acquisition to disposal.
University Data	Any data related to Rowan University functions that are a) stored on University information technology systems, b) maintained by Rowan faculty, staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).
University Funds	All University funding sources, including, but not limited to, operational budgets, capital budgets, and grants. These funding sources do not include the use of the Student Technology Fee.

University Graduate Student Researcher Stipend	A one-time payment made from University Funds to a graduate student researcher for the purchase of technology.
User	Refers to any member of the Rowan University community, as well as to visitors and temporary affiliates, who have been explicitly and specifically authorized to access and use the University's data or information systems.
Video Surveillance	The use of image capture, processing, transmission and storage equipment for authorized monitoring of public areas. This includes full-motion and still images, use of network transmission capacity, and digital storage and retrieval software. Audio recording is specifically excluded from this definition.
Virtual Private Network (VPN)	Extends a private network across a public network, such as the Internet using secure communication.
Virus Definitions	Periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software. Virus definition files are periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software.
Vulnerability	A vulnerability is a weakness in a system that can be exploited by an attacker to gain unauthorized access to Rowan University data, networks or systems. A vulnerability can be remediated or mitigate. Remediation occurs when the threat can be eradicated whereas mitigation involves minimizing the damage as the vulnerability cannot be fully eliminated.

Vulnerability Management Program	An effective vulnerability management program must be able to prevent the exploitation of vulnerabilities by detecting and remediating vulnerabilities in systems in a timely fashion. Proactively managing vulnerabilities on systems will reduce or eliminate the potential for exploitation and save on the resources otherwise needed to respond to incidents after exploitation has occurred.
Vulnerability Management Team	The Vulnerability Management Team reviews any concerns raised through the implementation of the Vulnerability Management Program at Rowan University.
WiFi	Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A WiFi enabled device such as a PC, mobile phone, or PDA can connect to the Internet when within range of a wireless network.
Workstations	Any device that runs a full desktop operating system, such as Microsoft Windows or Apple macOS.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer