Policy Owner:	Information Technology Department
Applicability:	University Faculty, Staff, Students, and all University Guests utilizing IT Services.
Revision Date:	October 1, 2019

Information Technology Policy

Policy Statement:

The University has computer and Internet resources for faculty, staff, students and other authorized individuals to use in support of Salve Regina's academic research and instructional and administrative objectives. University e-mail and internet resources are for business use only. Personal use during work hours is prohibited. After-hours use with supervisor approval is permitted. Users are responsible for all transactions made with their identification (ID) codes. The Computer and Network Use Policy contains the University's philosophy and requirements governing faculty, students, staff and other members of the community in their use of the University's information technology resources and data.

The Office of Information Technologies provides a wide array of support and related IT functions for faculty, staff, students and all guests requiring IT support. The Office of Information Technologies consists of three departments; they are Administrative Systems (Department 50103), IT (Department 50115 – including Network Infrastructure, Technical Services, IT Help Desk, and Network Services), and the User Support Services (Department 20102 – including University Computer Labs (in McKillop Library, Antone Academic Center, and the Center for Adult Education in Warwick), Classroom Technology, Training Workshops, Media Services and the University Card Office. The major responsibilities of these three departments and their respective groups are as follows:

Administrative Systems: Department 50103

Administrative Systems: Staff is fully involved with the support, integration, and enhancements of the Ellucian Administrative Information System with Colleague, Web Advisor, Ellucian Portal, and Self-Service as well as SAP's Business Objects reporting system. Further, in-house staff is available for implementation, project management and technical support for personal computer applications, local network applications and web applications used to satisfy individual, departmental, interdepartmental, and campus wide requirements; included in this set of applications are 25Live (Event Scheduling), IMC (Security), Workgroups (Design Services), Heartland (Salve ID Card system), SoftDocs (Document Imaging and eForms), Adirondack Housing Manager (Residential Life), and PowerFaids (Financial Aid), among others.

IT: Department 50115

Network Services: staff provides in-house support for all data communication connection points, wired and wireless networks on the Admin network (and collaborates with Cox Business Services on the network for Resident Halls), data network switches, network traffic management, and overall security for the network serving the Salve campus outside of the Resident Halls; in addition, staff provides enhancements and support of Cisco's Unified Communications Manager (CUCM) Voice over IP system; further, staff designs, supports and installs network solutions for intradepartmental, interdepartmental, and Internet data communication requirements such as security, anti-virus protection, file storage and sharing, physical and virtual server environment, database systems, data backup, disaster recovery, Ricoh Multi-Function Devices (MFD) for printing, Pharos Print Management system, email (Office 365), and web browsing. Staff also supports the network requirements at the Center for Adult Education site in Warwick and the Digital Forensics Labs (Newport and Warwick).

Help Desk Technology Service Center: Located in the garden level of the McKillop Library, the Center provides help and guidance for any Salve Regina student faculty or staff member who has technology needs. The Helpdesk provides direct access to Helpdesk and Technical Services staff member for help with many issues including: wired and wireless networks on campus, network credential and access control information and general application software usage, and hardware issues for both PC and Apple products. Students who buy into the recommended laptop program are provided with in house support. Students bring their own non recommended computer are provided best effort within our current hardware and software certifications.

Help Desk staff: serves as primary contact for University's technology help and service request system. The help desk staff are tier one technicians who record and track pertinent technology-related entries, escalate and dispatch help based on the type need, if necessary; The Help Desk extension is (401-341)-7777 and email address is helpdesk@salve.edu.

Technical Services Staff: provide tier 2 support at the Help Desk for all faculty, staff, and student technology. The staff is responsible for supporting software and hardware troubleshooting and repair on over 5000 University owned technology devices; further, staff is responsible for obtaining, configuring, installing, and keeping an accurate inventory of all new University computers, printers, and software. This includes configuration and support of current technology in PC Labs, Mac labs, Library's Digital Commons area, and the Center for Adult Education site in Warwick. The Technical Services Staff also provide technology expertise for the University's learning management system, which is Canvas.

Network Infrastructure: staff supports physical cabling projects (for voice, video and data) particularly related to building space renovations and building facilities construction; staff also supports Cisco Voice over IP requests for voice system and the voice messaging system assistance by campus community, switchboard operation and serves as vendor and association liaison with communications-related vendors.

User Support Services: Department 20102

User Support Services (USS) of the Office of Information Technology (IT), in McKillop Library, Room 002, provides technology support for classrooms, lecture halls, and huddle spaces throughout campus. There are over 125 supported locations on campus.

USS issues student IDs from the Card Office at McKillop 002. Replacement IDs are printed upon request M-F, 8:30 a.m.- 4:30 p.m. There is a fee to students for replacing lost University IDs.

USS provides support for Digital Signage across campus in conjunction with University Relations and other IT support areas.

Computer labs are in the Antone Academic Center, McKillop Library, O'Hare Academic Center, and the Center for Adult Education in Warwick. We provide access and support to both PC and Mac computers, printing, scanning, multimedia services, media services and classroom technology.

In the Antone Academic Center, we provide support for two Mac labs and a Mac digital photo lab. In McKillop Library Room 004, we provide a lab for learning, testing, and certifications in Microsoft applications and many other certifications. Also in McKillop are three PC labs in rooms 005, 006, and 007; in O'Hare, a Digital Forensics Lab is in Room 261; in the Center for Adult Education in Warwick, we support a PC computer lab, technology in nine classrooms, a testing/certification area, and a second Digital Forensics Lab.

Immediate assistance in any lab or classroom technology location is through a Help Desk call at (401) 341-7777, option 1, and expected in 5 minutes or less.

The computer labs in McKillop and Antone are open seven days for 80 hours per week throughout the semester. Patrons are required to have a valid Salve Regina ID card, to follow a code of ethics for computing, and to log in with their University-issued network ID.

Professional staff and student lab monitors provide assistance during all User Support Services operating hours. Software assistance is available for Microsoft Office and other applications.

Schedules indicating availability are posted outside of each computer lab. Computer labs are used for formal teaching, supporting curricula, workshops and individual learning assignments. Utmost attention is paid to making the labs and their resources available for student needs.

Media Services (MS) provides students, faculty and staff with assistance as it relates to the equipment loans and services of hardware, and related recording and editing projects. These services include but are not limited to hardware distribution (sound systems, projectors, laptops, screens, easels, etc.); video filming; and editing and transferring videos.

Editing Policy: Media Services will assist any student, faculty, or staff member wishing to edit. Requestors are expected to follow the University policy on copyrighted materials.

Duplicating Policy: Media Services will not knowingly duplicate any copyrighted material unless written permission from the copyright holder, or authorized representative, is obtained and submitted to MS along with the material to be copied. This includes duplicating videos, audio recordings, etc.

Media Services loans out equipment to students, faculty and staff. A valid Salve Regina University identification card must be shown for loans. All equipment will be available for instructional purposes and University business. Media Services sets up and strikes equipment within the University for student presentations, lectures, meetings, conferences, and workshops. Forty-eight-hour notice is required before setups and depend on available equipment. A week's notice is required for videotaping lectures or student presentations. Please make an appointment for editing.

USS - (401) 341-2985 including Media Services - (401) 341-2221 can be reached at their location in the Garden Level of the McKillop Library. Office hours are Monday - Thursday 8:00 a.m. - 10:00 p.m., Friday 8:00 a.m. - 5:00 p.m., Saturday 10:00 a.m. - 5:00 p.m., and Sunday 12:00 p.m. - 10:00 p.m.

Data Security Policy: University Wide

The purpose of this section is to define the Salve Regina University's Information Data Security Policy. Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today's environment because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems creates a unique vulnerability for our organization. The University has adopted the following Information Security Policy as a measure to protect the confidentiality, integrity and availability of Institutional Data as well as any Information Systems that store, process or transmit Institutional Data.

Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize the ability to provide service, violate business contracts, student privacy, or reduce credibility and reputation with students, community and partners. This Policy therefore discusses:

1. Data content
2. Data classification
3. Data ownership
4. Data security

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, including but not limited to unauthorized or inappropriate access, generation, use, modification, disclosure, or destruction. This Policy applies to all of the University's employee, financial, student or otherwise confidential data that exist, in any of the processing environments. The processing environment is considered to be, collectively, all applications, systems, networks and data storage (electronic or otherwise) owned, managed or operated or operated or managed by the University's agents.

This Policy defines the University's overall security and risk control objectives. The premise for the Policy can be stated as:

> *"Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorized persons or entities."*

This embodies the principle of least privilege. This document forms part of the conditions of employment for all employees (including student employees), a part of the contractual agreement for vendors, suppliers, and third party processors or agents, hereafter referred to as vendors.

Breach of Policy and Enforcement:

A breach of this Policy could have severe consequences to the University, and its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Misuse resulting in a breach of any part of this Policy may result in disciplinary action at the discretion of the University's Administration. Severe, deliberate, or repeated breaches of the Policy may be considered grounds for instant dismissal; or in the case of a University vendor, termination of their contracted services with recovery of costs by the University. All University employees and vendors are bound by these Policies and are responsible for their strict enforcement.

Scope of the Policy:

This Policy applies to all University and student data that exist in any University processing environment, on any media during any part of its life cycle ("Institutional Data"). The following entities or users who have access to Institutional Data are covered by this Policy:

- Full or part-time employees of the University
- University vendors or processors
- Other persons, entities, or organizations

Data Life Cycle:

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this Policy through the different life cycle phases of data. Users of data are personally responsible for complying with this Policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this Policy.

Data Usage:

All users that access University or student data must do so only in conformance to this Policy. Uniquely identified, authenticated and authorized users only may access data. Each user must ensure that University data under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality. Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Transmission:

All users that access University or student data to enable its transmission must do so only in conformance to this Policy. Where necessary, data transmitted must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. No proprietary or confidential data may be transmitted electronically; including via e-mail, without the approval of the University's Chief Information Officer.

Data Storage:

All users that are responsible for the secure storage of University or student data must do so only in conformance to this Policy. Where necessary, data stored must be secured via cryptographic mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights. No proprietary or confidential data may be stored in the user's local media (computer hard drives, CD, DVD, etc.) without prior approval of both the data owner and the Chief Information Officer. Proprietary or confidential data in printed format must be safeguarded and stored in premises or a secured location (i.e. Bank Vault) contracted by the University. At any given time, the data may not be stored in any format in any personal device or any other location not specifically approved by both the data owner and the Chief Information Officer.

Data Disposal:

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process. The University shall develop and implement procedures to ensure the proper disposal of various types of data. These procedures shall be made available to all users with access to data that requires special disposal techniques.

Data Security Policy Statement:

Goals. This Policy has been written with the following goals in mind:

- To educate University users and vendors about their obligation for protection of all data.
- To ensure the security, integrity, and availability of all University and student data.
- To establish the University baseline data security stance and classification schema.

Processing environment. The University processing environment that this Policy applies to is comprised of:

Applications: Application software is system or network-level routines and programs designed by (and for) system users and students. It supports specific business-oriented processes, jobs, or functions. It can be general in nature or specifically tailored to a single or limited number of functions.

Systems: A system is an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data that is used in a production or support environment to sustain specific applications and business organizations in their performance of tasks and business processes.

Networks: A network is defined as two or more systems connected by a communication medium. It includes all elements (e.g., routers, switches, bridges, hubs, servers, firewalls, controllers, and other devices) that are used to transport information between systems.

Data Security Responsibilities: The University, through its Chief Information Officer, is responsible for:
Defining the security requirements, controls, and mechanisms applicable to all data.
Defining the methods and guidelines used to identify and classify all data.
Defining the procedures for identifying data owners for all data.
Defining the labeling requirements for all data.
Defining all other data security usage, processing, transmission, storage, and disposal processes and procedures.
Defining the procedures necessary to ensure compliance to this Policy by all University users and vendors.
Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognized in industry.

Management Responsibilities: The University shall use its best efforts to ensure that faculty/staff, vendors, students and others comply with this Policy.

Other Responsibilities: Other organizations affiliated with the University shall have responsibilities to comply with this Policy, such as:
All University agents, vendors, content providers, and third-party providers that process University or student data shall have a documented security policy that clearly identifies the data and other resources and the controls that are being imposed upon them.
All University agents, vendors, content providers, and third-party providers that access the University processing environment and its data or provide content to it shall have a security policy that complies with and does not contradict the University Policy.
All agents, vendors, content providers, and third-party providers must agree not to bypass any of the University's security requirements.

Policy Review: It is the responsibility of the University through the Chief Information Officer to facilitate the review of this Policy on a regular basis. Because of the dynamic nature of the Internet, this Policy should be reviewed at least annually. The President's Cabinet and University Attorney should, at a minimum, be included in the annual review of this Policy.

Data Classification: Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data. To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Student Data or Proprietary University Data. The University, through its Chief Information Officer, is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. All data found in the processing environment must fall into one of the following categories:

Public University data: Public University data is defined as data that any entity either internal or external to the University can access. The disclosure, use or destruction of public University data will have limited or no adverse effects on the University nor carry any significant liability.

Proprietary University Data: Proprietary University data is any information that derives its economic value from not being publicly disclosed. It includes information that the University is under legal or contractual obligation to protect. The value of proprietary University information to the University would be destroyed or diminished if such information were disclosed to others. Most University sensitive information should fall into this category. Proprietary University information may be copied and distributed within the University only to authorized users. Proprietary University information disclosed to authorized external users must be done so under a non-disclosure agreement.

Confidential University Data: Confidential University data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of confidential University data can have adverse effects on the University and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. University confidential information must not be copied without authorization from the identified owner.

Confidential Student Data: Confidential student data is defined as data that only authorized internal University entities or specific authorized external entities can access. The disclosure, use, or destruction of confidential student data can have adverse effects on the University and student relations and possibly carry significant liability for the University. Confidential student data is entrusted to and may transit or is stored by the University (and others) over which they have custodial responsibility but do not have ownership. (Examples of Confidential student data including student bank or credit card information, or other data considered private.)

Public Student Data. Public student data is defined as data that any entity either internal or external to the University can access. The disclosure, use, or destruction of public student data will have limited or no adverse effects on the University or the student and carry no significant liability. Public student data is entrusted to and may transit or be stored by the University (and others) over which they have custodial responsibility but do not have ownership.

Data Ownership: In order to classify data it is necessary that an owner be identified for all data. The owner of data is responsible for classifying their data according to the classification schema noted in this Policy. If an owner cannot be determined for University data, the University, through its Chief Information Officer, must act as its custodian. The default classification for all data not classified by its owner must be either confidential student data or proprietary University data. The University, through its Chief Information Officer, is responsible for developing, implementing, and maintaining procedures for identifying all data and associated owners.

Non-disclosure Agreements: On occasion, data may need to be released to entities outside of the University. When a legitimate business reason exists for releasing sensitive information, a written and signed Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.