INFORMATION TECHNOLOGY
CODE OF CONDUCT

INTRODUCTION

Individuals working in Salve Regina University information technology and related areas (indicated in this document as "covered individuals") at Salve Regina, at its Rhode Island locations, including Newport as well as affiliated academic centers, hold positions of trust.

We operate and safeguard Salve Regina's central information technology assets, including networks, computers, telephones, access controls, information and databases. We provide technology-related services that are vital to the smooth functioning of the University and to the members of the University community. In these roles, every one of us must adhere to the highest professional and ethical standards.

The IT Code of Conduct applies to all covered individuals, including student employees, as well as to all others who work in information technology and related areas at Salve Regina as contractors, temporary staff, visitors or in any other capacity, on a full-time or part-time basis, it does not form a contract. Accessing Salve IT systems, services and data constitute the acceptance of the IT Code of Conduct policy. Failure on anyone's part to comply with these standards may lead to disciplinary action, up to and including revocation of access to salve systems and technologies, dismissal and referral as appropriate to authorities for legal action. Salve Regina IT reserves the right to amend this IT Code of Conduct at any time and without notice, at its sole discretion in good faith.

The purpose of this document is to help all of us become and remain familiar with the IT Code of Conduct. Seven guiding principles summarize the code. Information about each principle is provided in related sections of the code.

GUIDING PRINCIPLES

1. Stay familiar and comply with the policies, laws and regulations that affect your Salve Regina responsibilities.
2. Safeguard the confidentiality, privacy and security of Salve Regina communications.
3. Safeguard the accuracy, privacy and security of Salve Regina data and records.
4. Safeguard Salve Regina services, systems, premises, property and equipment from damage, disruption, attack or intrusion.
5. Fulfill requests for information or conduct investigations concerning Salve Regina data or facilities only with the express authorization of IT management as listed int he appendix.
6. Abide by copyright and intellectual property policies and ownership agreements.
7. Prevent personal interests from influencing Salve Regina business dealings.

For clarification of any item in the document or of any related University policy,
Please consult your supervisor, manager or director at your specific campus location.

I. COMPLIANCE

Guiding Principle: Stay familiar with and comply with the policies, laws and Regulations that affect your Salve Regina responsibilities.

Relevant policies, laws and regulations include, but are not limited to, Salve Regina employment policies and specific Salve Regina information technology policies, as well as e-commerce law, copyright law, The Family Educational Rights and Privacy Act 1974 (FERPA), The Health Information Portability and Accountability Act (HIPAA), the Financial Services Modernization Act, The Gramm-Leach-Bliley Act (GLBA) and Data Governance Policy and Data Governance Process and Procedures document. With the increasing complexity and interdependence of job responsibilities across information technology at Salve Regina and more broadly across Salve Regina's educational community, as well as the continuing evolution of associated Salve Regina policy and public policy, it can be a challenge to keep current. Individuals are helped to fulfill their obligations to remain current through information and links on the Salve Regina IT and various other staff websites, briefings about relevant policies, laws and regulations, as well as guidance and training available through Salve Regina Human Resources, Salve Regina professional development, town halls and other meetings, and departmental announcements.

II. SALVE REGINA COMMUNICATIONS

Guiding Principle: Safeguard the confidentiality, privacy and security of Salve Regina communications. The principle of privacy is addressed extensively in United States federal, state and local laws. Federal law prohibits unauthorized disclosure of communications of any kind (voice, data, email or other non-voice communication) transmitted over Salve Regina's networks or the public or private networks that Salve Regina utilizes, or even the fact that a transmission was sent or received.

1. Keep confidential what you see and hear when handling transmissions that use voice, data, facsimile and other technologies, as well as when on-site visits providing any Salve Regina information technology or related service. Information from any communication or the fact that a communication has taken place may not be used for your personal benefit or for the benefit of others. However, if you learn of an emergency involving immediate danger of fatality or serious injury, immediately contact the Salve Regina Office of Safety and Security at (401) 341-2325 and/or 911, or the appropriate public safety office at your Salve Regina campus location. Then, immediately report that contact and the related information to Salve Regina IT management, your immediate supervisor or to the relevant individual for your location referenced in the appendix to this code.
2. Except when explicitly authorized by information technology management, do not comply with any information requests. Refer to Salve Regina IT management or to the relevant individual for your location referenced in the appendix to this code any subpoena or other request for information. Examples of these requests include:
    a. Who is talking or has talked on a circuit?

   b. Who communicates or has communicated by email or other electronic means?
   c. Who transmits data to or from a particular location on Salve Regina's campus data networks, or the Internet?
   d. Where the specific location a person or computer is transmitting to or receiving from?
   e. What has been communicated?
   f. What is the nature of the business being handled?
3. Keep unlisted phone extensions, e-mail addresses and related data confidential. Some telephone extensions, e-mail addresses and other data are not listed in University directories for specific reasons. Such information should not be disclosed, except when explicitly authorized by Salve Regina IT management or the relevant individual for your location referenced in the appendix to this code.
4. Listening to, reading, monitoring, recording voice or data communications, as well as permitting such behavior by others are all prohibited activities, except to the extent that you have been authorized to do so in the performance of your job.
5. Making calls, sending e-mail or using any Salve Regina account, database or system via methods that fail to leave normal accounting records, logs or like documentation is prohibited. Third-party and collect charges to Salve Regina telephone numbers are prohibited. It is against Salve Regina policy to apply for a calling card billable to the University unless authorized to do so.
6. Do not permit the installation or use of any device which permits anyone to listen to, record, observe or access the content of any communication transmitted over the Salve Regina network or observe that a communication has taken place, except if explicitly approved by Salve Regina IT management. Any indication that someone has attempted to violate the privacy of a communication should be reported immediately to Salve Regina IT management at *cyberincident@salve.edu*. Examples of this behavior include attempts to gain access to circuits or records, connect monitoring devices, obtain password files or network data, conduct unauthorized network monitoring, obtain unauthorized access to databases or services, or obtain billing information.
7. Establishing unauthorized means to enable anyone to access University Services is prohibited. Do not permit anyone to connect any device to Salve Regina facilities unless you are authorized to do so and unless the device is connected in accordance with Salve Regina IT practice, is installed in a safe manner, and is intended for legal use. Using a device or technique that manipulates or avoids billing arrangements to defraud the University is not allowed.
8. Accessing Salve Regina systems and services requires the use of devices that meet the compliance standards established by the Office of Information Technology. Employees and contractors that require access to sensitive data in most cases will be issued a managed device for this purpose. Sensitive data includes but is not limited to PHI, PII, FERPA, HIPAA and GLBA .

III. SALVE REGINA DATA AND RECORDS

Guiding Principle: Safeguard the accuracy, privacy, and security of Salve Regina Data and records.

1. Accurate and reliable data are essential for University operations. Data kept on systems managed by Salve Regina IT and/or serviced by individuals from Salve Regina IT or related areas include a wide range of subjects and must be always kept accurate and available for authorized purposes. This data should be disclosed only to authorized University personnel with a legitimate need to know.
2. Be vigilant in safeguarding records and data, including paper files and computerized records, and sensitive information on any sort of mobile device. Records containing sensitive information and data about individuals require especially attentive protection to safeguard individual privacy and to ensure their confidentiality, integrity, availability, and auditability.
3. If the work you perform entails servicing computers owned by or assigned to other members of the University community, it is your responsibility to maintain the privacy, security and integrity of the contents of the computer. You may not read, copy or transmit any data or information found on that computer without the consent of the person responsible for the computer. Backups of the contents of the computer must be properly secured, in accord with practices approved by Salve Regina IT management.
4. Sensitive data should not be left in a public place where others may view them. Public places may include unattended fax machines, printers, or shared computer workstations, as well as your personal workspace. In an open workspace, take extra care to ensure that sensitive data are not left on an unattended computer screen or out in the open. Cabinets and computers that include these records must remain secured and accessed only for authorized purposes. All backups must be properly secured.
5. The willful, unauthorized destruction, alteration, attempted destruction or alteration of Salve Regina data, as well as making false entries or failing to make correct entries in Salve Regina data, are violations of University policy and, in some instances, of the law.
6. Report to Salve Regina IT management or to the relevant individual for your location referenced in the appendix to this code anyone who tries or is suspected of trying to alter, destroy, steal or obtain unauthorized access to records or data.
7. Ensure proper disposal of data containing University information, whether recorded on paper, magnetic media, optical media or any other format, and properly dispose of computers, multifunctional printers or other electronic storage devices according to the Salve Regina asset management requirements, and the Salve Regina standard for destruction and disposal of electronic equipment and data.
8. Be mindful of the Salve Regina data classification table, especially concerning restricted data.

IV. SALVE REGINA FACILITIES, SYSTEMS AND SERVICES

Guiding Principle: Safeguard Salve Regina services, systems, premises, property and equipment from damage, disruption, attack or intrusion. Information concerning the facilities, systems and services that Salve Regina IT and related areas plan, provide or use could be of interest to someone who seeks to misuse or destroy them. Be careful to prevent inadvertent disclosure of sensitive information, including information about Salve

Regina's physical plant, plans for service, future construction, restoration procedures and security procedures. Privileged access should not be breached. Report any violation or suspected violation to Salve Regina IT management or to the relevant individual for your location referenced in the appendix to this code.

1. Access to Salve Regina information technology facilities, systems and equipment is restricted to authorized Salve Regina IT staff, Salve Regina personnel, consultants and vendor personnel. Exercise extreme care to prevent unauthorized access to facilities, systems and services and disclosure of data, passwords, identification media and information, and sensitive procedures. Loss or theft of keys or access devices used for entry into controlled-access areas should be reported immediately to Salve Regina IT management or to the relevant individual for your location referenced in the appendix to this code. Covered individuals have a special responsibility to safeguard administrative access to systems and databases. *If you learn of an emergency involving immediate danger to Salve Regina facilities or encounter an unauthorized person in them, immediately contact the Salve Regina Office of Safety and Security at (401) 341-2325 or the appropriate public safety office at your campus location.* Then immediately report that contact and the related information to Salve Regina IT management or to the relevant individual for your location referenced in the appendix to this code. If you suspect that a Salve Regina system has been breached, report it immediately to Salve Regina Office of Information Technology at *cyberincident@salve.edu*.
2. Do not divulge sensitive information concerning Salve Regina's information technology plans, facilities, services, operating arrangements or other internal activities to anyone, including another Salve Regina employee, who is not authorized to know it. Locations of equipment, circuits, trunks, cables and systems should not be shared with unauthorized persons. Do not display, disclose or transmit information from or about physical and/or technology security systems, including lock and surveillance systems, as well as cybersecurity tools and methods to anyone outside Salve Regina information technology without permission from Salve Regina IT management or from the relevant individual for your location referenced in the appendix to this code.
3. Comply with building admissions procedures established by the Salve Regina Office of Safety and Security at each Salve Regina location. Report to Salve Regina IT management or to the relevant individual for your location referenced in the appendix to this code any attempts to enter controlled Salve Regina information technology space by someone who may be unauthorized to do so.
4. Covered individuals are responsible for the protection and integrity of equipment issued to them for on-campus or off-site use. Policies covering the proper use of office and off-site equipment are issued periodically and must be followed. Personally owned equipment should not be used in the support of Salve Regina University business unless authorized by the Office of Information Technology.
5. Access to Salve Regina systems and services requires the use of devices that meets the compliance standards established by the Office of Information Technology. Employees and contractors that requires access to sensitive data in most cases will be issued a managed device for this purpose. - Sensitive data includes but is not limited to PHI, PII, FERPA, HIPAA and GLBA.

V. REQUESTS CONCERNING INVESTIGATIONS OR INFORMATION

Guiding Principle: Fulfill requests for information or to conduct investigations concerning Salve Regina data or facilities only with the express authorization of Salve Regina IT management.

1. Any court order, warrant or subpoena requesting such investigation or release of Salve Regina records or information must be referred first to the chief information officer or to the senior relevant individual for your location referenced in the appendix to this code for consultation with University counsel. You may not take individual action to comply with the request.
2. Refer all requests from other Salve Regina offices or non-Salve Regina organizations or individuals for information or investigations of records or facilities managed by Salve Regina IT or related areas to the relevant individual for your location. You may not take individual action to comply with the request.

VI. PROPRIETARY AND COPYRIGHTED INFORMATION

Guiding Principle: Abide by copyright and intellectual property policies and ownership agreements. Work products and software created by covered individuals working in Salve Regina IT and related areas at Salve Regina as part of their job responsibilities are owned by Salve Regina University.

1. Except for internal use by Salve Regina IT or related areas, any copyrighted materials, including copyrighted publications and vendor documentation should not be copied without the permission of the copyright owner. This includes manuals, newspapers, trade journals, magazines and other publications, as well as copyrighted materials distributed in other media such as audio and video.
2. It is Salve Regina's policy not to use software unless it has been properly licensed and paid for and is registered as required with the manufacturer. If copyrighted software is licensed to an individual, it is against policy to share it, even within the office.
3. Software and work products, whether developed or customized by the University, are proprietary to Salve Regina. They should not be shared with anyone outside of our workgroups without express permission of Salve Regina IT management or the relevant individual for your location. We recognize that sharing appropriate information with certain communities inside and outside the University can provide significant benefit in the pursuit of our duties. This guideline is not meant to preclude such normal and customary exchanges of information, including the sharing of code where appropriate and authorized. Nevertheless, it is expected that official copyright policies and guidelines will be observed.
4. In general, in software acquisition agreements, Salve Regina agrees not to take any action, such as reverse assembly or reverse compilation, to devise a source code equivalent of vendor software delivered in object code form. Such actions are therefore not permitted.
5. Covered individuals, from time to time, may enter into specific non-disclosure agreements with vendors. We must act in accordance with these agreements,

taking care to not disclose trade secrets, private, financial, technical and business information.

6. While rates that Salve Regina pays for services are typically public knowledge, do not disclose either the rates or the bills and invoices that reflect the rates unless authorized to do so by Salve Regina IT management or the relevant individual for your location.

VII. SALVE REGINA BUSINESS DEALINGS

Guiding Principle: Prevent personal interests from influencing Salve Regina business dealings. Be aware that relationships with a supplier might create a conflict of interest or might appear to impair independence of judgment on behalf of the University. Purchasing decisions should be made in accordance with the established policies and guidelines of Salve Regina IT or the relevant offices for your location and of the University. When in doubt, seek guidance from your immediate supervisor.

1. Maintaining certain interests outside of Salve Regina IT and related areas while an individual fulfills fiscal responsibilities at Salve Regina may potentially create a conflict of interest. Fiscal responsibilities include managing budgets, preparing budget recommendations, authorizing expenditures, managing contracts and other financially influential responsibilities. Designated covered individuals with such responsibilities are expected to disclose potential conflicts of interest to Salve Regina IT management or to the relevant individual for your location.
2. Exercise good judgment when negotiating purchases or contracts on behalf of the University. Avoid making such arrangements or commitments with any supplier or contractor with whom you have a personal interest, either direct or indirect, except under the express direction of Salve Regina IT management or the relevant individual for your location.
3. No financial or contractual commitments for material or services may be made on behalf of the University, except with the express approval of an authorized University officer and/or director, including but not necessarily limited to the chief financial officer, controller, chief Information officer or authorized department executive.
4. In general, accepting or soliciting, even indirectly, gifts, loans, "kick-backs," special privileges, services, benefits, or unusual hospitality is not permitted. Exceptions can be made for promotional materials of nominal value, such as coffee mugs, calendars, T-shirts, modest entertainment expenses, etc. Gifts of extraordinarily large value, including exorbitant hospitality, should be reported to Salve Regina IT management or to the relevant individual for your location.

Document History:
a. Initial WIP Draft, Jan-02-2020 – IB
b. Revised (Content), Oct-06-2021 – Cyber Incident Response Team
c. Revised (Formatting), Oct-07-2021 - TA