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

Information Technology Policy – Cybersecurity Incident Response

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. The cybersecurity incident response policy contains the University's requirements governing faculty, students, staff and other members of the community in their use of the University's information technology resources as relates to reporting and managing cybersecurity incidents which may arise.

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. A select group of technologists with specialized skills comprises our cybersecurity incident response team. The incident response team will respond to all detected and reported cybersecurity incidents -email: cyberincident@salve.edu- on a 24x265 basis; consistent with the guidelines set forth herein.

General Principles:

It is the policy of the Salve Regina University to handle information security incidents so as to minimize their impact on the confidentiality, integrity, and availability of the Universities systems, applications, and data. An effective approach to managing such incidents also limits the negative consequences to both the University and individuals, and improves the Universities ability to promptly restore operations affected by such incidents.

It is especially important that serious information security incidents that may result in disruptions to important business processes are promptly communicated to the appropriate University officials so that they are involved early in decision - making and communications. In addition, compliance with various federal and state regulations requires expeditious reporting of certain types of incidents.

While information security incidents are not always preventable, appropriate procedures for incident detection, reporting and handling, combined with education and awareness of the Salve Regina University community, can minimize their frequency, severity, and potentially negative individual, operational, legal, reputational, and financial consequences.

Goals:

The goals of establishing a successful incident management capability include:

- Mitigating the impact of IT security incidents.
- Identifying the sources and underlying causes of IT security incidents and unauthorized disclosures to aid in reducing their future likelihood of occurrence.
- Protecting, preserving, and making usable all information regarding the incident or disclosure as necessary for forensic analysis and notification.
- Ensuring that all parties are aware of their responsibilities regarding IT system security incident handling.
- Protecting the reputation of the University.

Definitions:

1. An *information security incident* is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy.

   Examples of information security incidents include but are not necessarily limited to:
   - Computer system intrusion.
   - Unauthorized or inappropriate disclosure of sensitive institutional data.
   - Suspected or actual breaches, compromises, or other unauthorized access to Salve Regina University systems, data, applications, or accounts.
   - Unauthorized changes to computers or software.
   - Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for University work) used to store private or potentially sensitive information.
   - Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, and/or applications.
   - Interference with the intended use or inappropriate or improper usage of information technology resources.

   While the above definition includes numerous types of incidents, the requirement for central security incident reporting, regardless of malicious or accidental origin, is limited to serious incidents as defined below.

   Occurrences such as incidental access by employees or other trusted persons where no harm is likely to result will usually not be considered information security incidents.

2. A serious incident is an incident that may pose a substantial threat to University resources, stakeholders, and/or services. An incident is designated as serious if it meets one or more of the following criteria:

   - Involves potential, accidental, or other unauthorized access or disclosure of sensitive institutional information (as defined below).

- Involves legal issues including criminal activity, or may result in litigation or regulatory investigation.
- May cause severe disruption to mission critical services.
- Incident includes active threats.
- Incident is widespread.
- Incident is likely to be of public interest.
- Incident is likely to cause reputational harm to the University.

3. Sensitive information is defined as information whose unauthorized disclosure may have serious adverse effect on the Universities reputation, resources, services, or individuals. Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive. Sensitive information includes personally identifiable information such as protected health information (PHI), Federal Education Right to Privacy Act (FERPA), Personal Identifiable Information (PII), Social Security numbers, credit card numbers, birthdates, and any other information designated as sensitive by the University data governance committee.

Scope:

This policy is platform and technology neutral, and applies to the entire University, including the Newport Campus, Warwick Campus, any and all other affiliates.

Specifically, the scope of this policy encompasses:

- Faculty, and staff;
- Third-party vendors, who collect, process, share or maintain University institutional data, whether managed or hosted internally or externally;
- Personally, owned devices of members of the Salve Regina University community that access or maintain sensitive institutional data.

Guidelines:

1. All users of University IT resources must report all information security incidents to:
    - The University Chief Information Security Officer (CISO) at Irving.Bruckstein@salve.edu as well as to the Salve IT Cybersecurity incident response team at cyberincident@salve.edu.
    - The employees' direct supervisor

2. Any event that appears to satisfy the definition of a serious information security incident must be reported.

3. It is expected that incident reporting, from identification to reporting will occur as soon as possible no later than within 24 hours.

4. Some information security incidents may also be criminal in nature (e.g., threats to personal safety or physical property) and should immediately be reported to the Salve Regina University office of Public Safety and Security; concurrent with the incident notification described within this policy.

5. To avoid inadvertent violations of state or federal law, individuals and departments may not release information, electronic devices, or electronic media to any outside entity, including law enforcement organizations, before making the notifications required by this policy.

6. Privacy and Confidentiality of Sensitive Information:
    - Information related to campus security information security incidents is classified as sensitive under Salve Regina Universities Policies and Regulations Manual.
    - When University staff report, track, and respond to information security incidents, they must protect and keep confidential any sensitive information.
    - Incident data retained for investigation will exclude any sensitive information that is not required for incident response, analysis, or by law, regulation, or University policy.

Roles and Responsibilities:

A. The University Chief Information Officer ---in Consultation with the University Cybersecurity Incident Response Team - is the ultimate authority for interpretation and implementation of this policy, as well as for coordinating serious information security incident communications. The Office of University Human Resources will be provided with and retain relevant records and evidence pertaining to all serious incidents for a period of three years after the occurrence of the event. For incidents involving unauthorized disclosure of PHI, PII, or FERPA records will be retained for six years.

B. Salve Regina University Information Technology will oversee, coordinate, and guide the incident management process to promote a consistent, efficient, and effective response, including compliance with applicable breach notification laws and regulations.

C. All Salve IT staff serve as the information security provider for Information and Technology Services at all Salve Regina University campus locations and all affiliates.

D. The CISO shall
    1. Convene, when appropriate, a multi--- department Computer Security Incident Response Team (CSIRT)
    2. Collaborate and coordinate with other University offices including applicable compliance and communication offices.
    3. Take appropriate steps to preserve forensic evidence.
    4. Lessons learned meetings should be conducted for all serious information security incidents to review the effectiveness of the incident handling process, prevent recurrence of similar incidents, and identify potential improvements to existing security controls and practices.
    5. Conduct ongoing information security incident reporting education and awareness for the Salve Regina University community.

E. Users of University Information Technology Resources: All faculty, staff, and workforce members must report serious information security incidents to the CISO and the Salve Regina University Cybersecurity incident response team within 24 hours of becoming aware of the incident.

F. Security Unit liaisons: The Security Unit Liaison is a staff member that has been designated by the department dean or director to provide departmental oversight of information security, communicate and coordinate related activities with the University CISO, evaluate and respond to non---serious incidents, and coordinate departmental response to risk assessments and audit requests. Liaisons also develop and implement departmental - level policies, procedures, communications, and educational awareness programs consistent with University wide guidance.

G. Security unit liaisons or their designees must report suspected serious incidents (reported to or identified by them) within the 24 hour timeframe. When an incident involves the types of sensitive information below, the liaisons must also report the incident to the following parties:

- All incidents must be reported to the CISO and CIO at (cyberincident@salve.edu)
- If an incident involves a potential crime it must be reported to the University Director of Public Safety at michael.caruolo@salve.edu.
- If an incident involves payment card information (PCI), a Salve Regina University merchant must report the incident to the Chief Financial Officer at hallb@salve.edu.
- Security departmental liaisons and associated Salve Regina University IT staff will appropriately support the CISO in incident handling and post incident investigations and will evaluate and respond to information security incidents in accordance with University and departmental policies and procedures.

H. The University FERPA Officer, Alissa Bertram, Director of Records & Registration, will inform CISO of serious incidents reported to the office of the Registrar.

I. Third Party Vendors and Contractors: Salve Regina has an ownership, stewardship or custodial interest in all University data, parties that are contractually bound to limit the access, use, or disclosure of Salve Regina University information assets. These third party vendors or entities shall report potential or actual incidents to the University per the terms of their contract and/or the Universities' data protection addendum.

Violations and Sanctions:

Violations of this policy may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non - reappointment, discharge, dismissal, and/or legal action per Salve Regina University Policies and Regulations.

In addition to University disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

By adopting this Policy the University recognizes that all its faculty, students, staff and other members of the University community are bound not only by the Policy but also by local state and federal laws related to electronic media, copyrights, privacy and security. Each member of the University community is expected to be familiar with the foregoing laws.