Information Security Incident Management Policy

I. PURPOSE

The Office of Information and Technology Services at Salem State University works collaboratively with Federal, State and local enforcement agencies to identify, notify, report and mitigate information security incidents that may occur in the University. This policy serves to minimize the negative consequences of such incidents and to improve the University’s ability to promptly restore operations affected by such incidents. The policy also strives to ensure incidents are promptly reported to the appropriate authorities, that they are consistently and expertly responded to, and that significant incidents are properly monitored and mitigated.

II. SCOPE

An Information Security Incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of University information resources; interference with information technology operations; or violation of explicit or implied provisions embodied in the University’s Acceptable Use or related security policies. Examples of information security incidents include (but are not limited to):

- Computer security intrusion;
- Unauthorized use of systems or data;
- Unauthorized change to computer or software;
- Loss or theft of equipment used to store private or potentially sensitive information;
- Denial of service attack;
- Interference with the intended use of information technology resource; or
- Compromised user account

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

- Involves potential unauthorized disclosure of sensitive information (as defined below);
- Involves serious legal issues;
- May cause severe disruption to critical services;
- Involves active threats;
- Is widespread; or
- Is likely to raise public interest.

Sensitive information is defined as information whose unauthorized disclosure may have serious adverse effect on the University’s 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, social security number, credit card numbers, and any other information designated as sensitive by the University data custodians or executive personnel.
III. POLICY

Salem State University shall create an Incident Response Program for responding to and mitigating information security incidents involving University resources or those attributable to service providers acting on behalf of the University. The Incident Response Program shall have documented procedures that are repeatable and thorough, yet flexible enough to respond to an ever-changing threat environment. These procedures shall minimally be designed to support the following needs:

- Detect and record incidents from both on-campus sources and from service providers as applicable;
- Provide initial incident support;
- Assess the damage to University information or information resources in terms of confidentiality, integrity, or availability;
- Perform proper archiving and confiscation procedures needed to secure the incident evidence prior to any investigative activities;
- Classify and prioritize incidents based on impact and urgency to the University or members of the University community;
- Notify others outside of the incident response team in accordance with incident reporting and/or breach notification responsibilities;
- Investigate and diagnose incidents;
- Resolve incidents and recover service per agreed upon service levels;
- Fully document the response activities from start to finish, closing the incident; and
- Perform follow-up to include annual testing, process improvement, and future risk mitigation training.

IV. INCIDENT MANAGEMENT RESPONSIBILITIES

The Incident Response Program shall include the identification of those key personnel that shall comprise an Incident Response Team capable of effectively managing and coordinating the information security incident with all internal, external and law enforcement agencies required to effectively manage even the most serious of incidents. This Incident Response Team shall have the knowledge and authority to ensure that the following cornerstones of incident management can be properly initiated, developed and implemented:

**Prepare:** Establish, sustain and improve the procedures of the Incident Response Program;

**Protect:** Make those changes in the infrastructure to protect systems or mitigate an ongoing computer security event.

**Detect:** Categorize, correlate and prioritize events and assign them to someone for further investigation and possible response; and
**Respond:** Plan, coordinate and carry out effective communications and responses to incidents.

**V. VIOLATION OF POLICY**

Violation of this policy may subject a user to disciplinary action under appropriate University disciplinary procedures. The University may take such action as necessary, in its discretion, to address any violation(s) under this policy.

**VI. DISCLAIMER**

The University reserves the right to change this policy at any time without notifying the audience affected by the policy.

**VII. SUPPLEMENTAL REGULATIONS AND STANDARDS**

- **National Incident Management System**: Incident management guidelines from Homeland Security.
- **Incident Response Guidelines from NIST**: Guidelines and incident documentation published by the National Institute of Standards and Technology, Computer Security Resource Center.
- **Incident Management 101, SANS Institute**: Guidelines for Incident Management.
- **Defining Incident Management Processes for CIRTS**: Provided by Carnegie Mellon University's Computer Emergency Response Team (CERT).