Salem STATE | UNIVERSITY

University Administrative Policies
Policy Name: **Information Security Incident Management Policy**
Web Link: www.salemstate.edu/policies

Responsible Office: Information Security **Responsible Official:** Chief Information Security Officer	**Originator of the Policy:** Chief Information Security Officer **Origination Date:** 11/3/2009	**Effective Date:** 12/4/2015 **Revision History:** 1/18/2011; 9/20/16

1. RATIONALE

The Office of Information Security 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.

2. STATEMENT OF POLICY

Salem State University shall maintain an incident response procedure 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 procedure documents 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;
- 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.
- Document incident, identify improvements, and recommend corrective actions, as needed.

3. 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, stake-holders, and/or services. Specifically, an incident is designated as significant if it meets one or more of the following criteria:

- Involve potential disclosure of confidential information (as defined below).
- 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.

A. Confidential Data (high sensitivity)

Generally confidential data is data that is governed by state/federal law or institutional policy. This data requires limited access and stringent security controls.

Data should be classified as confidential when it could seriously damage the mission, safety or integrity of the University, its staff or its constituents. Such data should not be copied or removed from the University's operational control without authorized permission. High sensitivity data may also include, but is not limited to, data associated with investigations, bids prior to award, personnel files, trade secrets, appraisals of real property, test questions and answers, constituent records, academic records, contracts during negotiation, and risk or vulnerability assessments.

Confidential data should be protected at the highest possible degree as is prudent or as is required by law.

B. Sensitive Data (internal use, private, medium sensitivity)

Data should be classified as sensitive when the unauthorized disclosure, alternation or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all University data that is not explicitly classified as public or confidential should be treated as sensitive data. Data in this category is not routinely distributed outside the University. It may include, but is not limited to non-confidential data contained within: internal communications, interim financial reports, minutes of meetings, and internal project reports.

This policy applies to trustees, administrators, faculty, staff and students.

4. POLICY ENFORCEMENT

Violation(s)	It shall be a violation of this policy for data to be received, sent or stored inconsistent herewith.
Potential consequences	Appropriate discipline.
How to report	Contact Chief Information Security Officer

5. REFERENCE DOCUMENTS

Acceptable Use Policy: Salem State University standard for acceptable use of University online services.

Data classification and access policy: Salem State University

Electronic Communication Policy: Salem State University standard for the use of University electronic communications.

Enterprise Information Security Standards: Massachusetts Data Classification Standard, Version 1.0

Executive Order 504: Massachusetts Executive Order regarding the security and confidentiality of personal information Fair Information Practices Act: Massachusetts fair information practice standard (Mass. Gen. L. ch. 66A).

Family Educational Rights and Privacy Act (FERPA): (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Freedom of Information Act: Federal Freedom of Information Act (FOIA).

Gramm-Leach-Bliley Act (GLBA): The Gramm-Leach-Bliley Act applies to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.

HIPAA Security Regulations: Federal compliance guidelines for the Health Insurance Portability and Accountability Act of 1996

Incident Management Policy: Salem State University standard for the management of incidents involving online services or University data sources used by the University community.

Identity Theft Law: Massachusetts law relative to security freezes and notification of data breaches (Chapter 82 of the Acts of 2007).

Public Records Division: Massachusetts Public records resources as provided by the Secretary of the Commonwealth

Website Privacy Policies: Massachusetts requirements for agency website privacy.

6. CONTACT(S)

Subject	Office or Position	Telephone Number	Email
Policy Clarification	CISO	978-542-2745	tcesso@salemstate.edu

7. APPROVALS/ENDORSEMENT/NOTICE REQUIRED

Level	Title & Name	Signature	Date
Chair or Director of Department or Office	CISO/Thomas Cesso		
Dean or Assistant Vice President	Gene Labonte		
Vice President	John Keenan		
P.E.C. Initial Review			
P.E.C. Final Review			
All University Committee			
President	Patricia Maguire Meservey		
Board of Trustees (notice)			

8. REVIEW CYCLE

Initial review after 12 months