University Administrative Policies
Policy Name: **Data Classification and Access Policy**
Web link: http://www.salemstate.edu/policies/

Responsible Office: ITS **Responsible Official:** Chief Information Officer/Chief Information Security Officer	**Originator of the Policy:** Chief Information Officer/Chief Information Security Officer	**Effective Date:** May 2009 **Revision History:** Nov 2015

1. RATIONALE

Data are some of the most valuable assets any institution of higher education owns, and, as is in the case with all valuable assets, they need to be protected accordingly. What constitutes "accordingly" is mostly driven by legal, academic, financial and operational requirements and is based on the criticality and risk levels of the data. Protecting data assets while supporting academic, operational and research missions that require collaborative work and the open sharing of knowledge can be a difficult balancing act. Therefore, the need to properly protect that data is critical to the University's core mission. One of the most important steps in protecting data appropriately is to determine classification levels for the data, and then to proceed with the actual classification of all of the University's valuable data assets. This document describes a standard data classification scheme, the required considerations for continued classification and data lifecycle management requirements needed to accomplish that goal.

These standards ensure that the University develops and maintains data classification levels and controls that are compliant Federal and State regulations, as well as with the SSU Information Security Policy, and the SSU Information Security Program submitted annually for review by the Commonwealth's Information Technology Division (ITD), which addresses the security of information collected, used or maintained within electronic systems.

2. STATEMENT OF POLICY

The Salem State University Data Classification and Access Policy identifies three data categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect the information against unauthorized access.

The Data Classification and Access Policy applies to data owned by the University. University-owned data includes all paper and electronic data prepared, supplied, used or retained by University employees, within the scope of their employment, or by agencies or affiliates of the University, under a contractual agreement. This policy covers all data created through all University operations.

This policy classifies University data into three categories – Confidential, Sensitive and Public. These categories are expected measures to protect University data and are outlined below.

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 is subject to the most restricted distribution and must be protected at all times. 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 to the highest possible degree as is prudent or as is required by law. Guidelines include, but are not limited to the following:

- Systems which store or process Confidential data in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures applied in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
- Must not be disclosed to parties without explicit management authorization.
- Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access.
- When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Must be securely destroyed when no longer needed per Commonwealth Records Retention Policy.
- Exposure to an unauthorized 3rd party must be reported to the Information Security Office.

Confidential Data examples include:

- Social Security Numbers
- Bank Account number
- Credit or Debit card number
- Protected Health Information
- Driver's License number
- Human Subjects research
- Employee background checks

Data Access Requirements

Access to Confidential data is limited and defined by roles. Approved authorization is required from the supervisory role and/or the Data Steward.

Data Storage & Transmission Requirements

Confidential data is to be stored only on university file shares or within university databases.

Confidential data in paper form is to be secured at the end of the work day. Confidential data in paper form is to be shredded at the end of use in SSU approved locked shred bins.

In the rare case when confidential data are used**,** the data must be encrypted at rest and in transit when used outside of IT systems.

Sensitive Data (Internal Use, Private, Medium Sensitivity)

Data should be classified as Sensitive when the unauthorized disclosure, alteration 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.

Sensitive *Data examples*

- FERPA data
- Internal communications
- Minutes of meetings
- Internal project reports
- Financial Aid Award
- Payment History
- Student Bill
- Grades
- Test scores
- Advising records Employee evaluation
- Employee background check
- Search committee
- Affirmative action
- Donor or prospective donor
- Credit report

Data Access Requirements

Access to Sensitive data is limited and defined by roles. Approved authorization is required from the supervisory role and/or the Data Steward.

Data Storage & Transmission Requirements

A reasonable level of security controls should be applied to Sensitive data, such as:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Must not be posted on any public website.
- Must be securely destroyed when no longer needed by cross shredding (for paper records) or overwriting at least 7 times (for electronic records).

Public Data (General Use, Low Sensitivity)

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of such data.

Public Data examples

- FERPA directory information
- Campus maps
- Directory information as listed on the SSU web site
- Press releases
- Campus events
- Admission requirements
- Academic program information

Data Access Requirements N/A

Data Storage & Transmission Requirements N/A

3. SCOPE

This policy is applicable to all University students, faculty and staff, contractors, volunteers, students and to all others granted use of Salem State University information resources. Every user of these resources has a responsibility toward the protection of this information; some offices and individuals have very specific responsibilities.

This policy refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all data sources found on equipment owned, leased, operated, contracted, by the University, or equipment used by University staff in their travel or home environments. This includes laptops, personal digital assistants, telephones,

wireless devices, laptops, personal computers, workstations, minicomputers and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

For purposes of these standards, data is information maintained in any form including electronic, digital or optical format as well as paper. Data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on equipment covered under this policy.

4. RESPONSIBILITIES

Department/Data Type	Data Owner
HR	AVP Human Resources
Financial Aid	AVP Enrollment Management
Health Services	Dean of Students
Institutional Advancement	VP Institutional Advancement
Enrollment	AVP Enrollment
Police Services	Chief of Police
Finance	CFO
Admissions	VP Enrollment Management
Bursar	AVP Enrollment Management
IT	CIO
Faculty Evaluations	Provost
Human Subject Research	Provost

5. 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 Data Owner and/or Chief Information Security Officer

6. REFERENCE DOCUMENTS

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

SSU Information Security 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

Payment Card Industry – Data Security Standard (PCI-DSS): The industry standard for the secure processing of credit card transactions.

Fair Information Practices Act: Massachusetts fair information practice standard (Mass. Gen. L. ch. 66A).

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

Family Policy Compliance Office (FERPA): Federal law that protects the privacy of student education records.

7. CONTACT(S)

Subject	Office or Position	Telephone Number	Email
Policy Clarification	CISO	978-542-6446	painsworth@salemstate.edu

8. APPROVALS/ENDORSEMENT/NOTICE REQUIRED

Level	Title & Name	Signature	Date
Chair or Director of Department or Office	CIO/CISO Patricia Ainsworth		
Dean or Assistant Vice President	N/A		
Vice President	VP Administration John Keenan		
P.E.C. Initial Review			**9/28/2015**
P.E.C. Final Review			**10/26/2015**
All University Committee (notice)			
President	Patricia Maguire Meservey		
Board of Trustees (notice)			

9. REVIEW CYCLE

Initial review after 12 months