Data Classification Policy

I. PURPOSE

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 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.

II. 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 an electronic, digital or optical format. Data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on equipment covered under this policy.

III. POLICY
Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The proper classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All University data should be classified into one of three sensitivity levels, or classifications:

**A. Confidential (High Sensitivity)**

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. Examples of High Sensitivity data include data protected by state or federal privacy regulations, such as: Social Security numbers, credit card numbers, bank account numbers, student records and medical records. 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. Such guidelines include, but are not limited to the following:

- When stored 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 by members of the public, visitors, or other persons without a need-to-know.
- 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 destroyed when no longer needed by shredding (for paper records) or degaussing (for electronic records) in accordance with University policy.

**B. Sensitive (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.

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 destroyed when no longer needed by shredding (for paper records) or degaussing (for electronic records) in accordance with University policy.

C. Public (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. Examples of Public data include press releases, annual reports, course information, press releases, publicly accessible web pages and research publications. 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.

These classifications of data should be performed by an appropriate Data Steward. Data Stewards are senior-level employees of the University who oversee the lifecycle of one or more sets of Institutional Data.

IV. Required Considerations for Classification

The considerations listed below must be evaluated by the University’s Data Stewarts when assigning classifications to their data.

Laws, Regulations, Policies and Standards

The Data Stewarts are required to ensure that all laws, regulations, policies and standards to which their data is subject are met. Examples of laws and regulations that give or restrict access to data and apply to certain University departments include the Fair Information Practices Act, the Tax Information Security Guidelines for Federal, State and Local Agencies and Entities IRS Pub 1075, the Health Insurance Portability Accountability Act (HIPAA), Public Records Law, Massachusetts Identity Theft Law, Family Educational Rights and Privacy Act (FERPA), the Federal Rules of Civil Procedures’ references to electronic discovery, the guidance issued by the Supreme Judicial Court regarding electronic discovery in state court and agencies’ enabling legislation, regulations and policies and other laws that give or restrict access to data. Finally, the University must take into consideration existing Salem State policies and standards while implementing and evaluating their data classification assignments. Questions regarding laws, regulations, policies and standards that apply to specific agencies and departments should be directed to the Information Security Officer or University legal counsel.

Potential harm to the individuals to whom the data pertains

It is imperative to take into consideration any potential harm or adverse impact that the compromise of data may have on the parties to whom the data pertains. This consideration pertains to, but is not limited to client data, personally identifiable information and medical information.
Risk of loss of confidentiality

Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Therefore, in appropriately assigning data with a classification level, Data Custodians must evaluate what the risk is for unauthorized access to classified data and what likely impact that loss would have.

University Mission and Business Objectives

Data Custodians should be aware of the unique missions and business objectives of the University and their departments and should take those needs into consideration when evaluating their data classifications. In some cases, the University may be obligated to share as much of its data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the Data Custodian to ensure that those objectives are met, adequate controls need to be in place and in effect to address data integrity, security and availability.

Combining or Aggregating Data

At the point at which data is combined or aggregated its classification level should be reviewed. Some data may have little or no sensitivity in isolation, but may be highly sensitive when combined with other data. In some cases, aggregation of large quantities of a single data type can reveal sensitive patterns and/or plans and may facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous types can have similar effects. In general, the sensitivity of a given data element is likely to be greater in combination than in isolation (e.g., association of an account number with the identity of an individual and or institution).

Data Sharing Agreements and Contractual Requirements

Interagency Service Agreements (ISAs), Memoranda of Understanding (MOU's), grants, contracts and other written agreements between the University and external entities may include agreements regarding data sharing and the use, disclosure and maintenance of data, as determined by the data classification of the Data Custodian. The recipient agency or department's data classification must align with any such requirements. Further, if an agreement states that the recipient agency or department may further share the data, the subsequent recipients must adhere to the requirements of the original classification, unless the data has been de-identified or otherwise modified such that a different classification is required.

Industry Standards

There are several industry standards that may be helpful to Data Custodians in determining how to classify their data and in some instances the University may be obligated to comply with certain industry standards. For example, Data Custodians classifying the data related to credit card transactions are subject to the Payment Card Industry Data Security Standards (PCI DSS). Other examples of industry standard references can be found at the end of this document.

Up-stream and down-stream considerations
It is important for Data Custodians to consider how data will be used and what impact the intended use should have on the classification assigned to the data.

**Intellectual Property**

Data Custodians must take into consideration any intellectual property rights owned by an entity other than the University while implementing and evaluating their data classification assignments.

**V: Data Classifications**

The goal of information security, as stated in the Salem State’s Information Security Policy, is to protect the confidentiality, integrity and availability of Institutional Data. Data classification reflects the level of impact to the University if confidentiality, integrity or availability is compromised.

Unfortunately there is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when federal laws require the University to protect certain types of data (e.g. personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from Federal Information Processing Standards (“FIPS”) publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

<table>
<thead>
<tr>
<th>SECURITY OBJECTIVE</th>
<th>POTENTIAL IMPACT</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>limited</strong> adverse effect on University operations, University assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>serious</strong> adverse effect on University operations, University assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>severe or catastrophic</strong> adverse effect on University operations, University assets, or individuals.</td>
<td></td>
</tr>
<tr>
<td>Sensitive: Guarding against improper information modification or destruction, and includes ensuring information on repudiation and authenticity.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>limited</strong> adverse effect on University operations, University assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>serious</strong> adverse effect on University operations, University assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>severe or catastrophic</strong> adverse effect on University operations, University assets, or individuals.</td>
<td></td>
</tr>
<tr>
<td>Public: Ensuring timely and reliable availability to and use of information.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>limited</strong> adverse effect on University I operations, University</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>serious</strong> adverse effect on University operations, University</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>severe or catastrophic</strong> adverse effect on University operations, University</td>
<td></td>
</tr>
</tbody>
</table>
As the total potential impact to the University increases from Public to Confidential, the classification of data should become more restrictive and move up in impact. If an appropriate classification is still unclear after considering these points, contact the University’s Information Security Officer for assistance.

VI. ROLES AND RESPONSIBILITIES

Chief Information Officer:

The Chief Information Officer, acting at the Salem State University Information Security Officer (ISO), has overall responsibility for the security of the University’s information assets and is responsible for disseminating and providing interpretation of this and other policies related to security. Responsibilities of the ISO include:

- ensuring that appropriate data classification policies are delegated throughout the University to various University services, departments and other units.
- acting as Data Custodian for all University information not otherwise assigned;
- ensuring adequate security technology is applied to information resources in keeping with their classification;
- ensuring that the University’s data classification policies and practices meet all Federal, State and University data security policies or are complied with on a timely and prudently acceptable basis;
- annually reviewing, in conjunction with the Data Custodians, that all data classifications remain relevant, are complete and any required changes are being adequately addressed on a timely basis.
- ensuring that a recording of these processes is adequately and effectively maintained.

University Vice Presidents:

Will ensure that all information sources in their areas of responsibility are appropriately classified and all policies regarding this classification are being adhered to adequately. In addition, they are responsible for:

- designating and managing the efforts of one or more data custodians for all information resources maintained in their area of responsibility;
- ensuring that all staff in their areas have the training and support necessary to recognize data in accordance with this policy; and
- approving access authorization of all information uses in their area of responsibility having a data classification of Confidential or Sensitive;
Data Custodians:

Are responsible for making decisions about the use and protection of information in their custody. These responsibilities include:

- the accuracy and completeness of data and information;
- the classification of data as confidential (subject to privacy laws), sensitive (non-public salary information) or public;
- the identification and minimization of risks and exposures;
- supporting the Information Security Officer in the follow-up actions required to take appropriate actions in the resolution of all data classification needs;
- the annual review, in conjunction with the Information Security Officer that all data in their area of responsibility is accurately identified and properly classified and that no changes are necessary.

VII. POLICY CONFLICTS

In some circumstances, strict adherence to the rules for data dissemination as described under these standards will be inconsistent with the requirements of the Public Records Law, Mass. Gen. L. c. 66, section 10. Where the University’s compliance with these standards, University policies or classifications adopted hereunder conflict with the requirements of the Public Records Law, the Public Records Law takes precedence and the University must meet its requirements.

VIII. VIOLATION OF POLICY

The University Information Security Officer must be notified in a timely manner if data classified as Confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place.

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.

IX. SUPPLEMENTAL REGULATIONS AND STANDARDS

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

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.


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.


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.