Salisbury University

Data Security Policy

PURPOSE

The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of information technology assets and information. Protecting the confidentiality of the information entrusted to the University by Faculty, Staff, and Students is vitally important to maintaining that trust. Effective data classification is paramount to protecting and controlling access to information, which allows the University to ensure confidential data is only accessed by those personnel whose duties require it**.**

SUIT will utilize the definitions and guidelines relating to Public and Confidential Information established by the State of Maryland and relevant laws, such as 2013 Maryland Code §§10-1301 – 1308 to classify and protect its information.

1. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication
8/29/2018	1.1	Ken Kundell	USM update to require encryption standards

SCOPE

This policy is applicable to all University divisions collecting, processing, storing, and transmitting any confidential information, including electronic content and physical media such as paper, discs, and memory storage devices. Ensuring confidential data is accessed only by University staff with a **need-to-know** and implementing proper security controls to prevent unauthorized access will mitigate the risk of a data breach.

BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other

organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx
- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

POLICY

This policy establishes the requirements for the University to provide **due care** and **due diligence** in protecting and handling confidential data. The following subsections describe SUIT's responsibilities for data classification and for managing security controls to prevent unauthorized access (and dissemination).

In addition, the University will adhere to the Institutional Records Management program as required under Regents Policy VI-6.10.

1.1 Data Classification

For more information on data classification, refer to the *SU Public and Confidential Information Policy*. All University information is categorized into two main classifications regarding disclosure:

- Public Information
- Confidential (Non-Public) Information, which includes:
  - Personally Identifiable Information (PII)
  - Privileged Information

The University understands the value of the information it collects, creates, and processes, so data owners must assess and label their data appropriately. Proper classification allows SUIT administrators and information security personnel to create effective system policies, processes, and technologies to restrict users from accessing data inappropriately; security controls will follow a need-to-know model while facilitating security capabilities to identify and track confidential information across the network.

SUIT uses directory services for authorization and access to data. Based on this authorization data owners are assigned access based on security groups and access is removed based on the *SU Account Management Policy*.

Additionally, data has a known tendency to be "migrated" to more places than owners are aware of. Therefore, where feasible, periodic (data) scanning is required; automated tools can detect data-in-transit and determine if data is leaving an agency's network without authorization, such as being sent to the Internet or being transferred to another media

1.1.1 Data Retention

SUIT will develop a retention schedule that defines and documents data retention requirements within the University. University data owners will review inventory data annually and expired data will be archived or purged. This will minimize the risks attributed to data compromise or breach.

1.1.2 Data Storage

SUIT will follow the protections outlined in the *SU Physical and Environmental Policy* and apply the appropriate physical safeguards.

1.1.3 Data Loss Prevention

Once data has been classified, or labeled according to its information type, and security controls are in place, tools should be used, as feasible, to discover data-at-rest in inappropriate locations, such as project files stored on a local system instead of in a shared, secured location. Periodic data discovery can help detect and determine whether confidential data is being stored in systems that may not have the required security controls, thereby putting information at higher risk of compromise.

If data has been properly classified, data loss prevention tools can also scan systems and media with data storage capabilities for specified parameters such as keywords, regular expressions, and meta data tags. Some tools can provide automated analysis for more comprehensive tracking and discovery. Data loss prevention (DLP) is the process and capability of discovering data-in-transit and locating data-at-rest, discovering and tracking the movement of information, and blocking the export of information from a network. For more information regarding media transfers (i.e., USB flash drives, CD/DVD, etc.) refer to the *SU Media Protection Policy*.

1.1.4 Encryption

Encryption technologies should adhere to a minimum standard of AES 128-bit encryption where possible for all confidential data as outlined in the *SU Public and Confidential Information Policy*.

SUIT must have an established process for certificate based encryption which provides the following operational capabilities:

- Certificate issuance
- Certificate association
- Certificate validation

SUIT must have processes and documentation in place to ensure encryption information is not lost through changeover of personnel.

1.2 Access control

Access controls are logical data protections that can be implemented through embedded software or through third-party products. These logical protections include: enforcing security controls across the domain or within network devices, logging and alerting on specific activities (using an aggregating analysis tool), and establishing permission groups to control access to restricted content.

Security controls will be implemented based on data categorization and will abide by policy and regulatory requirements. Access controls will be implemented in such a way that users will be restricted from accessing data not pertinent to their roles or assigned duties. Access controls help prevent large amounts of data from being stolen, in the event of an account compromise. The controls also help protect against insider threats and reduce the scope of compromise by a malicious user.

Physical access controls will be implemented to restrict users to spaces relevant to their work — for instance, users in the finance department should not have access to IT spaces and electrical closets. This will minimize the exposure of data and systems to unauthorized users as well as track access attempts to unauthorized spaces.

Piggybacking, or tailgating, to secured spaces is unauthorized and is considered a policy violation (see *SU Physical and Environmental Protection Policy)*

1.2.1 Network Segmentation

Network administrators can create virtual local area networks (VLANs) for network switches and routers; this is a form of micro-segmentation used to separate the network into smaller units with the effect of controlling for both data-at-rest and data-in-transit. These micro segmentations can be based on physical or logical groups like geography (e.g., all second-floor workstations) or function (e.g., Contracts and Finance Department). With a network divided into logical segments, systems can be prevented from communicating directly to systems in "outside" segments, therefore any compromised host or malicious traffic has a limited scope of compromise and less impact on operations.

SUIT will ensure proper segmentation is in place to protect all University assets. A focus will be placed on defense-in-depth strategies and segmentation will follow a least-privilege model.

1.2.2 Account Management

Users (including administrators) must authenticate to the network to be granted access to the data, applications, and services required to perform their jobs. In order to authenticate, users must have valid accounts on the domain. Accounts must be configured with security controls to enforce least privilege, ensuring minimum levels of access. Users will have access only to the information and resources required to do their jobs and will need to formally request additional access. Ensuring least privilege significantly protects against data theft by limiting what information is accessible to an adversary should a user's account be compromised, such as through a weak password or a user leaving a workstation unlocked. For more information, see *SUIT Account Management Policy*

1.2.3 Group Memberships and Permissions

Group membership typically determines what data and resources a user has access to. SUIT will establish logical (access) groups for core business and mission units, and work with those units to determine the granular requirements for group access to shared stores, services, software, and even remote and system accesses; groups should be configured to enforce least privilege, and can also be used to establish access controls that can be monitored for indications of compromise.

Data owners and creators may also restrict access to specific data, files, or folders based on confidentiality and need-to-know. Data owners may establish groups (permission sets) to authorize user access, and also to ensure that system accounts, such as the backup service account, maintain minimum access for the service functionality. Data may be periodically reviewed to determine correct membership and permission attributes as well as to ensure that data is protected at the level required for its classification

1.2.4 Remote Access

The *SUIT Remote Access Policy* describes more specifically the requirements for remote access. Data security is paramount when external connections are accessing critical resources from potentially untrusted systems or networks, thus exposing agency data to compromise or theft. Restricting remote access to only those users who require it allows those accounts to be monitored closely to prevent unauthorized use and to protect against data breaches.

1.2.5 Mobile Device Access

The SUIT Mobile Device Security Policy describes more fully the requirements to control mobile device usage within the network.

EXEMPTIONS

If an exemption from this policy is required, a SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted.

DEFINITIONS

Term	Definition
Due Care	Using reasonable care to protect the interests of an organization. Developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures that are implemented through an organization's infrastructure.
Due Diligence	Practicing the activities that maintain the due care effort. The continued investigation and application of security into the existing infrastructure of an organization.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties.
Need-to-know	Security principle that confidential information will only be given to people who need it to do a particular job.

ENFORCEMENT

SUIT is responsible for enforcing data security controls and least-access privileges for all University data. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.