Salisbury University

Public and Confidential Information Policy

1. PURPOSE

The establishment of data classification levels is an important part of ensuring the protection and dissemination of potentially confidential data. Salisbury University's Department of Information Technology (SUIT) is committed to managing the confidentiality, integrity, and availability of information processed, stored, or transmitted by its networks, systems, and applications (IT Systems). SUIT will utilize the definitions and guidelines as established by the State of Maryland and relevant laws, such as 2013 Maryland Code §§10-1301 – 1308 (Md. State Govt. Code §§ 10-1301 to -1308), relating to Public and Confidential Information to classify and protect its information.

2. 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 identifier definition

3. SCOPE

This policy is applicable to all information that is processed, stored, or transmitted via SUIT Assets owned or operated by Salisbury University (SU) as well as vendors, contractors, individuals, or other entities providing services for, or on behalf of, SU. Confidential information can include all information and digital content produced, processed, collected, and stored electronically, on paper or other physical media. All employees, contractors, and vendors of SUIT resources are responsible for adhering to this policy.

4. 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

5. POLICY

This policy establishes the requirements for SU to provide due care and due diligence in protecting and disseminating confidential data. This policy identifies what is considered 'confidential information' and the measures required to protect this information.

a. General

All SU information is categorized into two main classifications with regard to disclosure:

- Public Information
- Confidential Information
    - Personally Identifiable Information (PII)
    - Restricted Information

In addition to following Maryland law related to confidential information, SUIT systems that process, store or transmit other protected types of information such as Protected Health Information (PHI) and payment card information (PCI) must abide by the relevant regulation and standard.

If an employee is uncertain of the classification of a particular piece of information, the employee should contact his or her manager or Information Security Services (ISS) for further instruction and clarification. Maryland law does not relieve an agency from a duty to comply with other requirements of federal law.

b. Public Information

Public information is information that has been declared publicly available by a SU official with the explicit authority to do so, and can be freely given to anyone without concern for potential impact to the State of Maryland, its employees, or citizens**.**

SENSITIVITY**:** Low; Data intended for public disclosure

IMPACT**:** Loss of data would not have an adverse impact on the mission of the University, safety, finances, or reputation.

EXAMPLE**:** News articles, campus maps, web pages intended for public use.

c. Confidential Information

Confidential information is non-public information and is defined by the sub-categories described in the following sections.

Personally Identifiable Information (PII)

PII is defined as data elements such as an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image combined with one or more of the following:

- A Social Security number;
- a driver's license number, state identification card number, or other individual identification number issued by a unit;
- a passport number or other identification number issued by the United States government;
- an Individual Taxpayer Identification Number; or
- a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

SENSITIVITY**:** High; Protection of data is required by law or regulation

IMPACT**:** Loss of data would have a significant impact on the mission of the University, safety, finances, or reputation.

EXAMPLE**:** HIPAA Data, SSN, Credit Card, Financial Account Numbers, Driver's License, Passport or visa numbers, Donor contact and non-public gift information.

Restricted Information

Restricted information is any information protected from public disclosure.

SENSITIVITY**:** Moderate; Data not generally available to the public

IMPACT**:** Loss of data would have a mildly adverse impact on the mission of the University, safety, finances, or reputation.

EXAMPLE**:** Research data, information in non-disclosure agreements, financial data, contracts, facility information, student records, campus ID numbers, information regarding infrastructure

d. Guidelines for Handling Confidential Information

Where possible, it is important to classify information so every individual that comes in contact with it knows how to properly handle and protect it. Confidential information, if disclosed, could result in a

negative impact to the State of Maryland, its employees, or citizens and shall be identified and handled according to the requirements shown in the table below.

#	Control Area	Protection Required
A	Access Control	Access to PII data should be limited to individuals with a business need. Who have signed confidentiality agreements.
B	Storage	Control physical access to system media (paper or digital) and protect confidential data using encryption technologies or other substantial mitigating controls (such as Data Loss Prevention, Network Security Event Monitoring and other network controls) Storage is prohibited on removable/portable media and public unauthenticated sites and systems without approval from the CIO.
C	Transit	Confidential data should be encrypted while in-transit wherever possible.
D	Identifiers	Confidential data should not be used as identifiers
E	Disposal/Destruction	See Media Protection Policy for further disposal instructions.

e. Breach Requirements

Breach requirements of Personally Identifiable Information are outlined within 2013 Maryland Code §10-1301. Under the Maryland statute, a breach is considered to be any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a unit." Additionally, if a unit discovers or is notified of a breach, it must conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information of the individual has resulted in or is likely to result in the misuse of the information.

After an investigation is concluded, the unit must determine if notification is required under the specific circumstances. A unit or nonaffiliated third party is not required to notify an individual of a breach if the personal information of the individual was secured by encryption or redacted and the encryption key has not been compromised or disclosed. See 2013 Maryland Code §§10- 1301-1308 for further information on notification requirements.

NOTE: This policy provides guidance for compliance with specific portions of the Maryland Code §§10-1301-1308, but does not supplement, replace or supersede the Maryland law itself. Agencies and associated vendors or contractors of executive agencies are responsible for independently complying with all provisions of Maryland law and other regulations/standards that affect specific types of Confidential Data, such as PHI (covered under the Health Insurance Portability and Accountability Act).

6. EXEMPTIONS

The requirements of this policy are established by Federal and Maryland laws and standards; there are no exemptions to this policy.

7. ENFORCEMENT

Any personnel responsible for the deliberate or inadvertent disclosure of confidential information may, pending the results of an investigation, be held liable and subject to disciplinary action, including written reprimand, suspension, termination, or possibly criminal and/or civil penalties.