Salisbury University

Media Protection Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is responsible for, and committed to, managing the confidentiality, integrity, and availability of Salisbury University (SU) networks, systems, and applications within the scope of its authority. As part of the commitment to confidentiality, SUIT is focused on protecting Salisbury University against information loss by ensuring data is tracked and access is limited whenever possible to only those personnel with **need-to-know**.

This policy directs SUIT to control portable and writeable media assets, such as external hard drives, DVDs, and USB flash drives, to minimize the risk of confidential data loss and to reduce the risk of unauthorized disclosure resulting in a possible data breach.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

It is the responsibility of every user to protect confidential information from unauthorized disclosure; and agencies, as data owners, must ensure both portable (e.g., removable) and writable media containing confidential information is controlled, tracked, securely stored, and properly disposed of. This policy is applicable to all SUIT managed assets owned by Salisbury University.

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

Writable media, such as DVDs, USB flash memory, and external hard drives, have become common tools in IT environments, but the portability that makes them useful and convenient presents a serious risk of data loss or breach. Users with write-access to media can transfer confidential data to a disc or memory card and walk out the door with it, either maliciously stealing the information or accidentally exposing the media to possible compromise. The lack of strong data-management poses significant risks to controlling agency information and incurs potential financial liability should the information be publicly disclosed.

5.1 Data Security

Due to the inherent interconnectedness of systems in a trusted network, users may have access to data stores, shared applications, network-available resources, and they require the ability to burn CDs or DVDs or store data on USB flash memory drives or external hard drives. However, portable media shall not be used to transfer confidential or sensitive data among parties if an electronic means of secure file transfer is, or can be made, reasonably available.

5.2 Controlling Writeable Media Assets

SUIT will track issued media and, when no longer needed, will collect and properly dispose of them, such as shredding old hard drives, to ensure no confidential information can be retrieved. This will help ensure data that is contained on old hardware is destroyed instead of casually tossed in a trash bin. Dumpster diving (the process of looking through garbage for confidential or valuable information by an adversary) may reveal confidential information that can be used to compromise the network, e.g., specifics of information technology assets used,

5.3 Data Sanitation

SUIT will ensure that any writeable media being repurposed is properly sanitized to prevent transfer of confidential data to unauthorized parties. Otherwise, all writeable media with confidential information will be properly destroyed to prevent unauthorized exposure of confidential data. All electronic storage media must be sanitized in compliance with SU's document-retention policy and litigation hold procedures.

Disposal decisions should be made at the discretion of SUIT based upon the classification of the data, level of risk, and cost to SU. Additionally, the procedures performed to sanitize electronic media should be documented and retained to enable audit verification

5.4 Secure Virtualization Planning & Deployment

The security of a virtual environment should be factored into the entire system development lifecycle, from planning to deployment, to maximize effective security and minimize the cost of security.

5.5 Devices Sent for Repair or Maintenance

Any device that contains writeable media that has to be sent offsite from SU for repair or maintenance will either have the media removed from the device or the media will be sanitized prior to being sent for repair.

6. EXEMPTIONS

If an exemption from this policy is required, an 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**.**

7. DEFINITIONS

Term	**Definition**
Information Media Assets	SU owned and IT managed digital media types such hard disk drives.
Need-to-Know	Security principle that confidential Information will only be given to people who need it to do a specific job.

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. 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.