Salisbury University

Security Policy Management

1. PURPOSE

As new threats and the technologies to combat those threats emerge it is vital for organizations to stay current with their policies and procedures to effectively protect their assets. It is vital that the Salisbury University (SU) Security Policies be continually maintained and updated by Information Technology representatives who are knowledgeable in the field and aware of industry standards, practices, and regulations. The Salisbury University Information Technology (SUIT) department is responsible for, and committed to, maintaining the SU Security Policies that help ensure the right controls and procedures are in place to protect Salisbury University.

2. REVISION HISTORY

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

3. SCOPE

This policy is applicable to the maintenance and approvals of all official **SU IT Security Policies** referenced in the definitions section below.

4. POLICY

The Salisbury University Information Technology (SUIT) department is responsible for the continual maintenance and updating of **SU IT Security Policies** as new threats, standards, regulations and business needs emerge. The SU Security Policies affect all employees, students, and affiliates of the University and as such it is important that the impact of the policies be understood and approved by the appropriate shared governance bodies and the Executive Committee. The most effective policies are ones that have involvement, feedback, understanding and buy-in from both the campus community and leadership.

After the initial review period and approval of **SU IT Security policies** by the relevant constituents, it is important however that the policies be able to be maintained and updated regularly so they can remain relevant and effective at protecting Salisbury University assets. **SU IT Security Policies** must be reviewed by the SUIT department annually and submitted to the CIO for review. Technological or editorial updates to policies are the responsibility of the SUIT department and updates will be sent to the Salisbury University Chief Information Officer (CIO) for initial approval and, at the CIO's discretion, impact from those changes will be shared with the relevant areas of campus. New policies or if the CIO determines the updates to be substantive changes that significantly alter an existing policy will be sent through the Executive Committee and shared governance bodies by the CIO. The specific procedures required to execute the standards from each respective **SU IT Security Policy** shall be maintained and updated separately by the SUIT department.

SU will report annually, by August 15th, to the USM CIO on the status of its IT Security Program.

5. EXEMPTIONS

There are no exemptions allowed from this policy, all affected SU IT Security Policies must be updated and managed in the manner described within this policy.

6. DEFINITIONS

Term	Definition
SU IT Security Policy	The following policies constitute the larger body of policies referred to as the **SU IT Security Policy**: • SU Account Management Policy • SU Asset Management Policy • SU Boundary Protection & Internet Access Policy • SU Cloud Services Policy • SU Configuration Management Policy • SU Continuous Monitoring Policy • SU Cybersecurity Incident Response Policy • SU Data Security Policy • SU Email Security Policy • SU Endpoint Protection Policy • SU Media Protection Policy • SU Network Documentation and Access Policy • SU Patch Management Policy • SU Physical and Environmental Policy • SU Public and Confidential Information Policy • SU Remote Access Policy • SU Security Assessment Policy • SU Security Policy Management (*This Policy*) • SU Third Party Interconnection Policy • SU Virtualization Policy • SU Wireless Access Policy • SU Data Security Policy

7. ENFORCEMENT

SUIT is responsible for managing and maintaining the SU IT Security Policy and accountable to the Executive Committee of Salisbury University, the Maryland Office of Legislative Auditors, and University System of Maryland Auditors. The Chief Information Officer (CIO) of Salisbury University will be responsible for ensuring compliance with the requirements defined in this policy.