Salisbury University

Security Assessment Policy

1. PURPOSE

Salisbury University's Department of Information Technology (SUIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of University networks, systems, and applications within the scope of its authority. This policy sets standards for Risk Assessment, Vulnerability Assessment, and Penetration Testing as an overall approach to mitigating exploitation and data compromise posed by cyber attackers and vulnerabilities.

This policy mandates the SUIT department's responsibility to evaluate risk within the University and determine how to eliminate, mitigate, or accept those risks.

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 all SUIT environments and assets owned or operated by any department supported by, or under the policy authority of, Salisbury University (SU). SUIT will be responsible for determining risk, developing the security assessment processes in accordance with the requirements in this policy, and providing assessment guidance.

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 mandates the requirements for conducting security assessments within SU. Performing proper risk assessments is the foundation of the SUIT Security Program. Managing risk ensures that all University and third-party systems and connections comply with established standards and that processes are in place to mitigate the risks of potential compromise.

SU utilizes a risk analysis worksheet for all systems, internal or hosted, to determine the risk level of the system to the University. A thorough review of the system is conducted to evaluate its connections to other systems, data stored, processed, and transported, and the access and use of the system. Evaluation of the data and associated data categorization can be found in the Public and Confidential Information Security Policy.

Based on the outcome of the risk analysis additional controls may be implemented to ensure the availability, integrity, and confidentiality of the system and associated data.

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

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.