Salisbury University

System Protection Policy

1. PURPOSE

Server and **endpoint** security management is an approach to network security that requires, and ensures, server and endpoint systems comply with specific criteria before being granted access to the network. Server and endpoint protection are important aspects of maintaining the confidentiality, integrity, and availability of information.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication
09/17/2018	1.1	Ken Kundell	USM update to expand coverage for servers

3. SCOPE

This policy is applicable to all devices managed by Salisbury University IT (SUIT), physical or virtual, that are connected to the university networks through a physical, wireless, or VPN connection. SUIT will be responsible for establishing system protection capabilities in accordance with the requirements in this policy, and for providing those capabilities to the Enterprise managed systems.

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 describes an overall strategy to implement server and endpoint security within Salisbury University. SUIT shall implement system security by observing the requirements outlined in the sections below.

5.1 General Requirements

#	Name	Requirement
A	Server and Endpoint Security	Protect and secure SUIT managed servers and endpoints.
B	Process	Establish processes and rulesets for the configuration of server and endpoint systems.
C	Automated System Protection	Implement an automated system security mechanism to support the protection and detection of server and endpoint systems, where possible.

5.2 Access Control

Access controls must be implemented where possible at the software level as well as the device level to ensure server and endpoint protection. The University must establish access control in accordance with the requirements described below.

#	Name	Requirement
A	Least Privilege	Access should be limited to only those authorized users necessary to accomplish the assigned tasks in accordance with organization missions and business functions.
B	Privilege Levels	Establish non-privileged and privileged levels of users.
C	Privileged Access	Prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards and countermeasures where possible.
D	Endpoint Device-based Encryption	Employ full device or container encryption to protect the confidentiality and integrity of information on an endpoint device, where possible.

5.3 Server and Endpoint Security Capabilities

Server and endpoint protection software should be configured where possible to perform the capabilities outlined in the table below.

#	Name	Requirement
A	Prevent Program Execution	Prevent malicious program execution in accordance with threat intelligence and behavior analysis.
B	Automated Malicious Component Detection	An automated mechanism detects the presence of malicious hardware, software, and firmware components on, or attempting to gain access to, an endpoint device and takes the following actions, some of which may require manual approval or review: ▪ Disables network access by such components ▪ Isolates the components ▪ Notifies SUIT Staff or agency equivalent
C	Process Level Privilege Management	Prohibit user installation of software without manually executing the software using separate administrative credentials or manual elevation of the installation process utilizing rights management where possible.
D	Host Intrusion Prevention System (HIPS) Capability	Implement host-based protection, such as up-to-date anti-malware and exploitation prevention.
E	Firewall	Implement host and/or network level firewall protections to provide appropriate system segmentation.
F	Antivirus	Implement software that will prevent, detect and remediate malware infections on individual computing devices and IT systems, and ensure definitions are up to date and downloaded from a vendor source.
G	Aggregation of Notifications	Where possible, aggregate security notifications and alerts into a central analysis tool (e.g., **Security Information and Event Management (SIEM)**.

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
Endpoint	Defined as an SU owned computer hardware device such as workstations (desktop computers, laptops, and tablets).
Server	Managed enterprise system maintained by SUIT (web servers, e-mail servers, file servers, database servers, directory servers, application)
Security Information and Event Management (SIEM)	Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

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.