Salisbury University

Network Documentation and Access Policy

1. PURPOSE

Network documentation is critical to efficient troubleshooting, onboarding personnel, and recovery in the event of a data loss or an integrity-impacting event. Network documentation should be created and updated regularly to ensure accuracy. Additionally, the establishment of network access controls protects both the network and data when a policy is not met by a user or device. The Salisbury University Information Technology (SUIT) department is responsible for, and committed to, managing the confidentiality, integrity, and availability of University information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that networks are properly documented, configured, and accessed by University or approved users.

This policy mandates the creation of network documentation and network access-control standards for the University Network.

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 utilized by the University. SUIT will be responsible for documenting the network architecture of the University in accordance with the requirements of 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 outlines the level of network documentation required by SUIT, who has access to network documentation, and how changes to the network environment must be handled and communicated to stakeholders. Furthermore, this policy establishes the requirement to implement network access controls through device and user authentication where possible to maintain the security posture of a network.

5.1 Network Component Documentation

Agencies must maintain an inventory of their network components in an asset-management repository in accordance with the SU Asset Management Policy. Asset inventory and network device documentation will follow the requirements outlined below.

#	Name	Requirement
A	Asset Management and Configuration Baseline	Network structure and configuration shall be documented and maintained through applicable management platforms to keep all relevant data (i.e. Name, description, location) NOTE: See SU *Configuration Management Policy* and SU *Asset Management Policy* for further details.
B	Enterprise Requirements	SUIT must keep up-to-date documentation of all network assets
C	Confidentiality of Network Documentation	All network documentation is considered restricted information, and will only be released as necessary outside of SUIT. ▪ Network documentation may be released to other personnel on a need-to know basis ▪ These restrictions apply to network documentation in any form, whether written reports or topology diagrams

5.2 Network Topology Diagram Requirements

SUIT must create a network topology diagram that identifies the major network nodes and interconnections. All Network Topology Diagrams (NTD) should be physically verified if automatic mapping software is utilized and should include both physical and logical information with lines indicating directional relationships where possible. All changes to NTD should be documented and updated when the physical topology changes.

5.2 Network Access Control

SUIT will restrict access to University network infrastructure to only authenticated and/or authorized users. Where possible both device and user authentication will be implemented.

5.3 Change control

Changes applied to network devices (including boundary and control devices) must be approved in accordance with the SU Configuration Management Policy.

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. ENFORCEMENT

SUIT is responsible for managing the network infrastructure for the University. 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.