Salisbury University

Wireless Access Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of information technology assets and information. Implementation of wireless network access offers new challenges in balancing access to information and ensuring security is properly designed and integrated.

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 official SUIT supported use of wireless access deployments. The following policy requirements ensure the secure use of wireless technologies while prohibiting unauthorized wireless devices and access points within the network infrastructure.

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

SUIT will ensure all wireless deployments meet the requirements outlined below. To effectively implement a wireless infrastructure, SUIT must have a wireless security plan that accounts for the proper deployment of wireless assets as well as for mitigation of the associated risks inherent in these technologies.

Security requirements for mobile devices are outlined in the SU-*MobileDeviceAccessPolicy*.

5.1 Internal Wireless Access

SUIT must have a wireless security plan that establishes mandatory security controls and implementation requirements before an authorized wireless access point is installed or deployed on its network. The table below identifies the requirements for the SUIT wireless access security plan.

.

#	Name	Requirement
A	Wireless Deployment Process	The wireless security plan must have standardized processes and procedures for the consistent configuration, installation, and deployment of authorized, commercial-grade wireless access points.
B	Physical Security	Wireless devices must be installed: ▪ So that, where possible, unauthorized users are prevented from accessing, tampering with, or damaging the physical devices ▪ Utilizing best practices for optimum signal coverage
C	Perimeter Restriction	Access points must be deployed strategically to minimize or eliminate the signal strength beyond the building perimeter while allowing enough signal overlap so devices within the perimeter can roam available channels. ▪ This allows users to move around and maintain a consistent network connection, e.g., moving from cubicle to a meeting room.
D	Authorization Requirements	For internal Local Area Network (LAN) deployments (accessing confidential, internal resources): ▪ Where possible, wireless access points will be designed to require both device verification and user authentication ▪ Wireless networks will be segmented to prevent unauthorized connections from scanning or accessing other internal segments, i.e., preclude lateral movement across wireless segments

E	Trust Level Separation	Deployment of wireless access points must account for and restrict access based on established trust levels, e.g., guest wireless service cannot access internal resources or data.
F	Segmentation	Any guest wireless access point must be *completely segmented from the internal LAN* and all connection attempts, direct or lateral, from the guest segment to the LAN must be prevented. No cross connection or bridge will be permitted.
G	Security Requirements	All access points must: ▪ Utilize the latest security and encryption features, including passwords with strong **entropy** ▪ Change default administrator credentials ▪ Change default **SSID** ▪ Disable **SNMP** (or change the default string if utilized and require the latest encrypted version) ▪ Use an authentication protocol like variants of Extensible Authentication Protocol (EAP) or use a RADIUS server ▪ Incorporate event-logging and log-forwarding to SUIT associated management and logging systems. ▪ Where possible, require mobile device security verification

5.2 Guest Wireless Access

Agencies might require guest wireless services for visitors or as a courtesy to the public. This constitutes an untrusted connection and must be explicitly placed in the DMZ — with no access to any internal network resource. The wireless security plan must ensure network separation for guest Internet-access deployments.

The SUIT Acceptable Use Policy (AUP) will be provided where possible for guest networks.

All SUIT employees who use a personal device on the SUIT network are bound by the AUP.

5.3 Wireless Security Threats

Common threats against wireless access points and devices include but are not limited to the following: Eavesdropping, Tampering, Spoofing, Denial of Service, and Rogue Access Points . The wireless security deployment will use defense-in-depth strategies to mitigate or eliminate these threats.

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
Entropy	A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret.
Simple Network Management Protocol (SNMP)	Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
Service Set Identifier (SSID)	A sequence of characters that uniquely names a wireless local area network (WLAN).

8. ENFORCEMENT

SUIT is responsible for managing the wireless network 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.