Salisbury University

Remote Access Security Policy

1. PURPOSE

Personnel are increasingly using tools to work remotely. Personnel with **remote access** privileges may access confidential information or resources that must be protected and tracked, especially when accessed from a network or client with a less rigorous security posture than Salisbury University (SU). These remote accessing systems may be considered untrusted when they are not controlled by the SU (e.g., an employee's personally owned laptop) and pose a risk for data loss or unauthorized disclosure.

The Salisbury University Department of Information Technology (SUIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of Salisbury University (SU) networks, systems, and applications within the scope of its authority. This includes ensuring that remote connections to the SUIT network or any network managed by Salisbury University from an outside entity does not endanger the security posture of the 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 all employees, contractors, vendors and agents of Salisbury University. SUIT will be responsible for ensuring the security of remote access connections in accordance with the requirements in 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

Remote access is defined as any access to an agency information system by a user communicating through an external network such as, for example, the Internet. **Virtual Private Network (VPN)** or equivalent technology should be used when remotely accessing information systems. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption for authentication of access credentials and transmission of data.

5.1 General

Remote access methodologies used within SUIT systems will follow the general requirements outlined below wherever possible.

#	Name	Requirement
A	Approved Methods of Remote Access	SUIT must authorize and monitor all remote access capabilities used on University systems. Approved methods of remote access may include: ▪ Direct Application Access — provides direct access to an application, e.g., user logs into an application IP address ▪ Virtual Desktop Infrastructure (VDI) ▪ Remote Desktop Control — provides direct access to a system (and its applications) from a remote location ▪ Tunneling (via VPN) — provides a secure communication channel through which information can be transmitted between networks
B	Business Need	Remote access privileges must be given only to those employees with a clear business need as determined through approval of their supervisor or through an approved exemption.
C	Storage of Confidential Information	Storage of confidential information on any non-University owned device is prohibited. Confidential information may not be stored on any University owned, portable device, without prior written approval from the SU Chief Information Officer (CIO).
D	Privilege of Remote Access	It is the responsibility of employees and contractors with remote access privileges to ensure that they employ wherever possible the same security measures and practices as when using an on-site connection. A user with remote access privileges must exercise **due diligence** to protect the device used and information accessed during remote access sessions (see *Acceptable Use Policy*)

E	Compliance with All Policies	All remote access users will comply with all SUIT Cybersecurity Policies and may not perform illegal activities or use the access for outside business interests.

5.2 Requirements

Remote access methodologies used within SUIT systems will have, or be configured to have, the functionalities outlined below wherever feasible/applicable:

#	Name	Requirement
A	Authorized Methodology	External Agencies who wish to implement remote access solutions to the SUIT or Enterprise network must obtain prior, written approval from SUIT through the SU CIO or other delegated authority. SU Employees can seek authorization through requesting access from SUIT with their business need justification per 5.1.B.
B	Multifactor Authentication	Remote access methodologies shall use multifactor authentication for added security measures, where feasible.
C	Centralized Authentication	Remote access methods that are capable of using a centrally managed authentication system such as Active Directory shall do so.
D	Time-out Requirements	Duration of user sessions should be limited where feasible:
E	**Split Tunneling** Forbidden	Reconfiguration of a user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
F	Encryption	▪ All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize encryption for transmission of access credentials and data ▪ Remote access connections must use 128-bit or greater encryption to protect data in transit
G	Anti-virus Updates	All hosts that are connected to State internal networks via remote access technologies must have up-to-date antivirus software implemented.
H	Patching Cadence	All hosts that are connected to SU internal networks via remote access technologies should have current operating system security patches installed.
I	User Specific Account	Remote access will be allowed only with the use of unique user credentials.
J	Password Protection	Remote access passwords are to be used only by the individual to whom they were assigned and not to be shared.
K	Server Security	Remote access connections must use the most comprehensive cryptographic protocol available whenever possible (such as TLS 1.2 currently) to ensure data is protected while in transit.
L	Logging	All remotely-connected sessions must have logging enabled (to a syslog server) to collect the connection and authentication details.

N	Remote Access Control Lists	Due to remote access utilizing centralized authentication wherever possible, account controls are in place per the SU Account Management Policy that ensures only authorized individuals are allowed to connect.

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
Remote Access	Ability to access non-public State-managed network resources through a device not directly connected to a Salisbury University network such as a home computer connected through the internet.
Split Tunneling	A computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same or different network connections.
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

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.