Salisbury University

Third Party Interconnection 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. This includes ensuring that acceptable security measures are in place, and that acceptable risk levels are maintained, when new network connections are made between the University and third party entities.

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 ensuring the security of third party 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

The requirements governing secure third-party connections are listed in the table below. In addition to the table below a third party agreement must be signed by all parties.

#	Name	Requirement
A	Planning	Third party interconnections will be planned in advance. Planning will be conducted in accordance with industry best practices and federal and state guidelines and standards.
B	Security Assessments	Third party interconnections must conform to a risk assessment exercise performed by SUIT.
C	Compliance with SUIT Cybersecurity Policies	Insofar as the third party has connectivity to University systems or networks, or access to University data, the third party will comply with all applicable SUIT Cybersecurity Policies.
D	Confidentiality and Non-Disclosure	Insofar as any data, systems, or networks to which the third party has access are considered confidential to the University, the third party must sign Confidentiality and Non-Disclosure Agreements (NDA).
E	Technical Documentation of Connection	Technical details regarding the third-party interconnections will be documented; this shall include, at a minimum: ▪ Description of the purpose of the connection; ▪ Updates to SUIT logical and physical topology diagrams to account for the connection (or a supplementary diagram); ▪ Allowed protocols; ▪ Allowed network addresses or address ranges; ▪ Allowed TCP/UDP ports if applicable; ▪ Allowed data types; and Authorized users (with specific names or user groups)
F	Monitoring Activation	Third party interconnections shall not be authorized until security monitoring of that connection has been enabled in accordance with the SU Continuous Monitoring Policy.
G	Least Privilege	New third party interconnections will: ▪ Grant the minimum connectivity into the agency required to meet the objectives of the connection Grant the minimum access privilege required to meet the objectives of the connection
H	No Full Network Access	Unfiltered network connections (WAN, LAN, WLAN, VPN, etc.) between the agency and any third parties other than SUIT itself, will not be authorized or allowed. NOTE: Connectivity to a University LAN by a third party-owned or supplied computer system constitutes FULL NETWORK ACCESS

		without compensating controls, and thus is disallowed by default. Alternatives to connecting to a University LAN include: ▪ Provisioning a guest network for third party Internet access from a University facility ▪ Provisioning University-owned workstations for use by third party staff who require access to University systems. EXCEPTION: Vendors providing penetration testing services may be granted additional elevated privileges under the conditions established within the scope of the evaluation.
I	Third Party Contact Information	▪ The third party will be required to provide contact information to SUIT for the appropriate groups or individuals who can fulfill agency requests for cyber security monitoring and incident handling ▪ Contact information will include emergency contact information for off-hours requests SUIT will maintain this contact information so that it is immediately accessible to staff as needed

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
Third Party	Any entity or computing environment that is not the University complying with this policy.
Third Party Interconnection	Any IT connection to a third party that enables the transfer of data between the University and the third party, or the sharing of computing resources. This includes, but is not limited to: ▪ Direct network connection (Local Area Network, Wide Area Network, etc.); ▪ Virtual Private Network (VPN) connection; ▪ Shared computing platforms. For example, a University virtual machine hosted on a server or cluster that also hosts non-University virtual machines would constitute a third party connection; or ▪ Known usage of external storage media to move data between the agency and the third party.

8. ENFORCEMENT

SUIT is responsible for ensuring the security of third-party connections 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.