The Universities AT SHADY GROVE

Third Party Connection Policy
USG Policy 6 (4.00) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The policy is intended to provide guidelines for deploying and securing direct connections to third parties.

The scope of this policy covers all direct connections to USG's network from non-USG owned networks. This policy excludes connections which are already covered in USG's Remote Access Policy 6 (3.50).

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as "OIT." This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Access Control List (ACL):* a list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

B. *Demilitarized Zone (DMZ):* a perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

C. *Firewall*: a security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

D. *Third Party Connection*: a direct connection from a party external to USG. Examples of third-party connections include connections from vendors, partners, or suppliers.

III. Use of Third-Party Connections

A. Third party connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third-party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the OIT Director.

IV. Security of Third-Party Access

A. Third party connections require additional scrutiny. The following statements will govern these connections:

1. Connections to third parties must use a firewall or Access Control List (ACL) to separate USG's network from the third party's network.
2. Third parties will be provided only the minimum access necessary to perform the function requiring access.
3. Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.
4. If a third-party connection is deemed to be a serious security risk, the OIT Director will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the OIT Director.

V. Restricting Third Party Access

A. Best practices for a third-party connection require that the link be held to higher security standards than an intra-USG connection. As such, the third party must agree to:

1. Restrict access to USG's network to only those users that have a legitimate business need for access.
2. Provide USG with the names and any other requested information about individuals that will have access to the connection. USG reserves the right to approve or deny this access based on its risk assessment of the connection.
3. Supply USG with on-hours and off-hours contact information for the person or persons responsible for the connection.

VI. Auditing of Connections

A. In order to ensure that third-party connections are in compliance with this policy, they must be audited periodically.

VII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

VIII. Revision History

Date	Description	Revised By
11/28/2018	Initial Policy Creation	Russell Schlosburg

IX. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf