The Universities AT SHADY GROVE

Network and Systems Security Policy
USG Policy 6 (3.30) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to outline controls necessary to secure USG's network and IT system infrastructure. The network security policy will provide the practical mechanisms to support USG's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

This policy covers all IT systems and devices that comprise the campus network or that are otherwise controlled by USG

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. *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. *Academic zone:* the section of the USG network intended to be accessed by students but not conference guests nor the general public.

C. *Antivirus Software:* an application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

D. *DMZ*: (Demilitarized zone) The section of the USG network which houses systems which are to be accessed by off-campus users/systems.

E. *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.

F. *Hybrid zone:* the section of the USG network which contains resources that must have access to or be accessed from both the Academic zone and the Trusted zone.

G. *IDS*: stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.

H. *IPS*: stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

I. *NTP*: stands for Network Time Protocol. A protocol used to synchronize the clocks on networked devices.

J. *Open zone:* the section of the USG network intended to provide services to all campus network segments. Few restrictions are places on access to this network zone so only minimal services are provided.

K. *Password*: a sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

L. *Public zone*: the section of the USG network intended to provide services to conference guests and to the general public. Few restrictions are places on access to this network zone so only minimal services are provided.

M. *RAID*: stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.

N. *Switch*: a network device that is used to connect devices together on a network, often supporting network separation via VLANs.

O. *Trusted zone*: the section of the USG network containing information not intended for access by students, conference guests, or the general public.

P. *VLAN*: stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.

Q. *Virus*: also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

III. Network and System Device Passwords

A. All USG owned and managed infrastructure equipment will comply with USG's Password Policy 6 (3.40).

IV. Logging

At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

A. Log Management
USG recommends that a log management application be considered.

B. Log Review
Log management applications can assist in highlighting important events. However, a member of USG's IT team should still review the logs as frequently as is reasonable.

C. Log Retention
Logs should be retained in accordance with USG's Data Retention Policy 6 (2.30). Unless otherwise determined by the USG OIT Director, logs should be considered operational data

V. Firewalls

Internet connections and other unsecured networks must be separated from USG network through the use of a firewall.

A. Configuration

The following statements apply to USG's implementation of firewall technology:

1. Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
2. No unnecessary services or applications should be enabled on firewalls. USG should use 'hardened' systems for firewall platforms, or appliances.
3. Clocks on firewalls should be synchronized with USG's other networking hardware using NTP or other means. Among other benefits, this will aid in problem resolution and security incident investigation.
4. The firewall ruleset must be documented and independently audited annually. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
5. For its own protection, the firewall ruleset should include a "stealth rule," which forbids connections to the firewall itself.
6. The firewall should log dropped or rejected packets.

B. Outbound Traffic Filtering

USG encourages outbound filtering if possible, but it is not required.

VI. Networking Hardware

A. Networking hardware, such as routers, switches, bridges, and access points, should be implemented in a consistent manner. The following statements apply to USG's implementation of networking hardware:

1. Networking hardware must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks or systems where management connections would be expected to originate.
2. Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
3. Access control lists should be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.
4. Unused services and ports should be disabled on networking hardware.

5. Service interfaces should be limited as per USG's Third-Party Connection Policy 6 (4.00).

VII. Servers and Centralized Systems

A. The following statements apply to USG's owned and operated server infrastructure:

1. Unnecessary files, services, and ports should be removed or blocked.

2. The following server-hardening guidelines are to be applied (unless these are legacy systems/devices):

- Operating system and applications must be supported, where applicable, by its manufacturer or a third-party vendor
- Operating system and applications must be updated with all critical and applicable patches in a timely manner
- Anti-malware and anti-virus must be updated with all applicable patches/definitions in a timely manner
- When applicable, all servers must follow the USG backup policy
- Manufacturers best practices are strongly encouraged

3. Servers and centralized systems, even those meant to accept public connections, must be protected by a network-based and host firewall or access control lists. Where available, application-based firewalls or access control lists must be applied.

4. If possible, a standard deployment process should be developed for USG's network and system servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

5. Clocks on network and system servers should be synchronized with USG's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

VIII. Intrusion Detection/Intrusion Prevention

A. USG requires host-based and/or network-based IDS/IPS to protect critical systems.

IX. Security Testing

The following sections detail USG's requirements for security testing.

A. Internal Security Testing

1. Internal security testing should be performed quarterly by members of USG's OIT staff as required by USG OIT Director. Internal testing should be used to assess the security of the network, systems, and USG supported applications. Internal security testing must only be performed by employees whose job functions are to assess security and only with permission of the USG OIT Director. Internal testing should have no measurable negative impact on USG's systems, network, or any application's performance.

B. External Security Testing

1. External security testing by a third-party entity should be conducted on an annual basis. The USG OIT Director must determine to what extent this testing should be performed, and what systems/network infrastructure and applications it should cover. External testing must not negatively affect USG's systems, network, or any application's performance during business hours or compromise USG's IT security at any time. In addition, if penetration testing is performed, it must not negatively impact USG's systems or data.

X. Disposal of Information Technology Assets

A. When USG owned and managed IT hardware assets are decommissioned, the following guidelines must be followed:

1. Any asset tags or stickers that identify USG must be removed before disposal.
2. Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
3. At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, USG must use methods that are in accordance with the NIST SP800-88 *Guidelines for Media Sanitization*. Alternatively, USG has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid-state memory).

XI. Network Compartmentalization

USG requires the following with regard to network compartmentalization:

A. Higher Risk Networks

1. Examples: USG Open zone, USG Public zone
2. Requirements: Segmentation of higher risk networks from USG's internal network is required, and must be enforced with a firewall or router that provides access controls.

B. Externally-Accessible Systems

1. Examples: USG DMZ zone, servers to which direct Internet access is permitted
2. Requirements: Segmentation of externally-accessible systems from USG's internal network is required, and must be enforced with a firewall or router that provides access controls.

C. Internal Networks

1. Examples: USG Academic zone, USG Hybrid zone, USG Trusted zone

2. Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. USG requires that networks be segmented to the fullest reasonable extent.

XII. Network and System Documentation

A. At a minimum, network and system documentation must include:

1. Network/System diagram(s)
2. System configurations
3. Firewall ruleset
4. IP Addresses
5. Access Control Lists

B. USG requires that network and system documentation be performed and updated on a yearly basis.

XIII. Antivirus/Anti-Malware

A. USG provides the following guidelines on the use of antivirus/anti-malware software:
   1. All USG-provided user workstations must have antivirus/anti-malware software installed.
   2. Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
   3. Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

XIV. Software Use Policy

A. All USG owned and managed devices must abide by the following requirements for the use of software applications:
   1. Only legally licensed and OIT approved software may be used.
   2. Open source and/or public domain software can only be used with the permission of the USG OIT Director.
   3. Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
   4. Vulnerability alerts should be monitored for all software products that are installed and managed on USG owned and managed devices. Patches that fix vulnerabilities or security holes must be installed in accordance with USG OIT's patch management process.

XV. Maintenance Windows and Scheduled Downtime

A. OIT Staff must perform service disrupting tasks at a time that minimizes user impact. Tasks that are deemed "emergency support," as determined by the USG OIT Director, can be performed at any time.

XVI. Change Management

A. OIT staff should make a reasonable effort to document hardware and/or configuration changes to network and systems devices. USG OIT staff is required follow the change management process established by USG OIT Security Team and approved the USG OIT Director.

XVII. Suspected Security Incidents

A. When a security incident is suspected that may impact a network or system device, the OIT Staff should refer to USG's Incident Response Policy 6 (1.20).

XVIII. Redundancy

A. Network, system, and application redundancy should be implemented as appropriate taking into consideration the criticality of the asset(s) and potential impact to the USG campus.

XIX. Manufacturer Support Contracts

A. USG should purchase a maintenance plan, support agreement, or software subscription when purchasing critical hardware or software. The plan should meet the following minimum requirements:
    1. Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time period, as determined by the USG OIT Director, as well as firmware or embedded software updates.
    2. Software: The arrangement must allow for updates, upgrades, and hotfixes for a specified period of time.

XX. Security Policy Compliance

A. Security Program Management
    1. An employee or team must be designated to manage USG's security program. Security management will be responsible for USG's compliance with this security policy and any applicable security regulations.
    Responsibilities include: A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on USG's information security program (as detailed below), D) any ongoing testing or analysis of USG's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

B. Security Training
    1. A training program must be implemented that will detail USG's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually.

C. Security Policy Review

1. USG's security policies should be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to USG's security policies. As part of this evaluation USG should review:
    - Any applicable regulations for changes that would affect USG's compliance or the effectiveness of any deployed security controls.
    - If USG's deployed security controls are still capable of performing their intended functions.
    - If technology or other changes may have an effect on USG's security strategy.
    - If any changes need to be made to accommodate future IT security needs.

XXI. Banner Requirement

A. For initial logon, banner text approved by Legal Counsel must be displayed for all switches, firewalls, and routers, when technically possible.

XXII. 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.

XXIII. Revision History

Date	Description	Revised By
03/07/2018	Initial Policy Creation	Russell Schlosburg
01/16/2020	Added Banner requirement, Requirement for host and/or network IDS/IPS , Added Service interface Agreement	Russell Schlosburg

XXIV. Related Documents

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

B. NIST SP 800-88 “Guidelines for Media Sanitization”
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819