Network Management and Security Standard

Standard Type: Administrative
Responsible Office: Office of Technology Services
Initial Standard Approved: 05/14/2012
Current Revision Approved: 05/25/2017

Standard Statement and Purpose

The Network Management and Security Standard defines the minimum set of security and management controls that must be applied to VCU networks. These controls address those network services and activities that are either the most sensitive or have the broadest impact, as well as general management principles applied to the management of the VCU network. All activities related to the management and / or security of the VCU network are governed by this document.

This document is not considered an exhaustive list of possible network management and security controls. Any network services or activities not specifically covered by this policy or corresponding procedures are not automatically authorized; Guidance from the VCU Network Services or VCU Information Security team is needed for any services or activities not covered in this document, these services and activities will be reviewed on an as-needed basis.

Access to and use of the VCU Network is subject to the VCU Computer and Network Resource Use Policy, the VCU Information Security Policy, and any related University policies and procedures. Refer to the Related Documents section below.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Policy

All individuals using VCU network resources are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

Definitions

Default Deny Rule
A default deny rule in firewall management refers to the default blocking of all network services, where only selected, approved, and trusted services are allowed through the firewall with the implementation of an Access Control List.

Domain Name System (DNS)
The Domain Name System allows the translation between a friendly name of an asset with an associated IP address of an asset and vice versa.

Dynamic Host Configuration Protocol (DHCP) services
The DHCP services allows the automatic assignment of an IP address to an asset connected to a network. Modern routers and some modern switches possess this capability.

Internet Facing Services
Internet Facing Services refer to network based services or protocols that can be accessed directly from the Internet without the use of any VPN services. Examples of such services may include but are not limited to: website access to the VCU homepage or website access to the course registration page.

Intrusion Attempt
An intrusion attempt is the attempted bypass of security controls. Intrusion attempts may include but are not limited to: hacking, exploitation of system vulnerabilities, guessing of passwords, tricking people into providing sensitive information, and picking of locked doors to secure areas.

Legacy Network
Legacy networks are network segments that are or are being retired or replaced.

Network Infrastructure Devices
Network Infrastructure devices are devices that are used to transmit and / or manipulate network traffic from source computing devices to destination computing devices. Network infrastructure devices may include but are not limited to devices that function as routers, switches, wireless access points, hubs, network repeaters, network hardware firewalls.

Network Routing Controls

Network Routing Controls refer to the technical controls that can be applied to network infrastructure devices that will restrict the communications between a source device and a destination device. An example of a network routing control is an Access Control List that only allows a group of computers to access a specific website, while rejecting access attempts from all other computers.

Principle of Least Privilege

Principle of Least Privilege refers to the provision of only the necessary amount of privileges and rights for a resource to function. The implementation of this principle helps to limit the amount of damage a resource can cause if it is compromised.

Secure Link

Secure Links refer to trusted connections such as site-to-site VPN tunnels between an external network and an internal trusted networks. These secure links allow simple exchange of data between the two networks, often bypassing many security controls placed between an external network and the internal trusted network. An external network with an established secure link is considered a Trusted External Network.

Security Incident

A security incident is a successful intrusion attempt that caused harm to the organization.

Server or Server like device

A server or a "server-like device" is any device that makes resources available to multiple users via a network connection. Desktop and laptop computers that permit remote support / management by IT staff and network printers are not classified as servers or server like devices for purposes of this statement, so long as they do not permit remote access by anyone other than authorized administrators.

Trusted External Network

Trusted external networks are external networks managed by appropriately assessed business partners of VCU and with a secure link established with VCU internal trusted networks

Trusted Internal Network

Trusted internal networks are VCU managed internal private network segments designated for the use of academic, research, or administrative purposes.

Untrusted External Network

Untrusted external networks are external networks that were not assessed by VCU. Generally, the majority of the Internet is considered an untrusted external network.

Untrusted Internal Network

Untrusted internal networks includes the VCU RESNet for student residence, VCU public facing networks, and any VCU guest networks are not considered untrusted internal networks

VCU Network

VCU Network refers to the network and all associated segments used by Virginia Commonwealth University to conduct its academic, research, and administrative operations. The VCU network is directly managed and controlled by VCU Network Services.

Virtual Private Network (VPN)
Virtual Private Network (VPN) is a technology that allows the secure remote access to internal VCU resource from external and / or untrusted networks.

Contacts

The VCU Information Security Office officially interprets this policy. The VCU Information Security Office is responsible for obtaining approval for any revisions through the appropriate governance structures. Questions about this Standard should be directed to the VCU Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The following sections contain the requirements of this Standard.

A. General Requirements and Requirements for Category III Data/Information.
These requirements apply to all networking services and to all systems and services handling Category III data/information.

1. **All network infrastructure devices, including but not limited to devices that function as routers, switches, hubs, and wireless access points, connecting to VCU networks must be approved, installed, managed, and decommissioned by VCU Network Services.** If such devices are found to be connected to the VCU network without proper authorization, they may be confiscated at the discretion of VCU Network Services. Any service found to interfere with the proper functioning of the VCU Network, or any segment thereof, may be disabled, disconnected and/or confiscated at the discretion of VCU Network Services. (J17)

2. **VCU Network Services shall exclusively operate all DNS (Domain Name System) services, IP addressing management, network segment management, and DHCP (Dynamic Host Configuration Protocol) services within VCU.** Except Microsoft DNS, where it is required for the proper functioning of an enterprise Active Directory Domain and is managed by VCU Technology Services in accordance with any configuration guidance provided by VCU Network Services.

3. **Management practices of the VCU Network and all associated network infrastructure devices must follow all documented and applicable management procedures and baselines.**

4. **VCU Network Services shall periodically review and securely maintain up-to-date configuration files for VCU network equipment, and ensure configuration are synchronized across devices when applicable.** (J18, J19, J20)

5. **Unauthorized use of any networking tools for the purpose of hacking, network scanning, and vulnerability scanning is prohibited. These tools include but are not limited to, key loggers, password crackers, network sniffers, and vulnerability scanners. Use of such tools on the network must be approved by VCU Network Services and VCU Information Security Office.**

6. **No new devices will be added to any legacy network segments, as defined in the Network Configuration and Management baseline.**

B. Category I Data/Information Requirements

The requirements delineated in this section are applicable to systems having VCU information/data that are classified as Category I. In addition to the requirements from the Category II Information/Data Requirements section, systems having Category I information/data must also adhere to the following requirements:

1. **Logs for all network infrastructure devices in the VCU Network must be centrally stored and monitored to enable the recording of security relevant actions.** (J6)

2. **VCU Network Services in collaboration with VCU Information Security Office shall classify and document network segments as trusted internal network, trusted external network, untrusted internal network, untrusted external network, or legacy network.** VCU Network Services shall securely maintain up-to-date network diagrams showing the Internal network segments, interconnections, secure links, and the relationships between these networks and the Internet. (J21, N23)

3. **All network infrastructure devices will be housed in exclusive physical space, where physical access to the space is restricted to authorized network services staff only.** When not occupied, these spaces shall be physically secured from unauthorized entry. (J19)

4. **Network access control to systems and applications must follow the principle of least privilege where appropriate and most restrictive network access controls will be applied to facilitate individuals' access to systems and information.** (G9, Partial mapping to J8)

5. **Virtual Private Network (VPN) access to internal assets from external and internal untrusted networks shall be governed by specific VPN access groups and related VPN access procedures.** In order to protect VCU's systems and data against attacks originating from external or untrusted networks, Virtual Private Network (VPN) must be used to access any high risk ingress services, as defined in the Network Configuration and Management baseline, from the Internet,

On-campus Residential Network (ResNet), any VCU guest networks, and all untrusted internal or external networks. (J2, J15, J21, J23)

6. **Formal interconnection security agreements are needed for the establishment of any secure links between internal trusted networks and external networks.** (J16)

7. **Session Initiation Protocol (SIP) may not be used to transmit messages to or from the Internet, except where this is required for the normal functioning of authorized and dedicated teleconferencing systems that are placed on a dedicated and segregated network designed for these systems.** (J22, Q5)

8. **Servers will not be made accessible from the Internet unless they have been properly registered with the server inventory, provisioned and are hosted or housed on designated server network segments.** (J2)

9. **All network segments except untrusted internal networks shall be governed by a default deny rule on their corresponding firewalls.** Traffic into those segments will be blocked unless a specific rule exists to permit it. (G9, J4, J5, J15)

10. **Access of data over wireless network requires authentication and authorization.** Wireless network with access to data requires proper authentication and authorization. (J7)

C. Special Requirements

The following requirements apply to systems used to handle specific data types; all data types listed in this section are considered Category I Information/Data and must also adhere to the requirements listed in the Category I Information/Data Requirements Section.

1. **VCU Network Services will ensure the performance of semi-annual review of configuration file for VCU network equipment.** Required by PCI-DSS. (J18)

2. **In order to prevent data theft, connections to the high risk egress services, as defined in the Network Configuration and Management baseline, with devices on the Internet and internal or external untrusted networks are restricted.** Required by PCI-DSS and CUI. (J3)

3. **Direct access to high risk ingress services, as defined in the Network configuration and Management baseline, is prohibited.** Required by FISMA (mod) and CUI. (J15)

4. **No split-tunnel remote access is allowed.** VPN into networks containing the following data types must direct all user traffic through the VPN tunnel, including both traffic intended for the assets residing on internal network, as well as assets residing on other networks, including but not limited to the Internet. Required by CUI, FISMA (mod) and CJI. (J26)

5. **Must use separated/dedicated network to access data.** Dedicated network segments with at a minimum logical firewall separation must be used to handle this data. Physical network separation is preferred.Required by PCI-DSS and CUI. (J1).

6. **Terminate network session following 30 minutes of inactivity**. Required by PCI-DSS, FISMA (mod) and CUI. (J12)

7. **Actively detect and remove rogue wireless access points from the network.** Required by PCI-DSS, CJI, FISMA (mod) and CUI. (J17)

8. **Ensure firewalls are installed to separate wireless network from network containing data.** Required by PCI-DSS and CUI. (J24)

Forms

1. VCU Information Security Policy Exception Form

Related Documents

The VCU Information Technology Policy Framework contains VCU Information Technology policies, standards and baseline requirements, all of which must be followed in conjunction with this Standard. The framework also includes information technology guidelines as recommendations and best practices.

Baseline documents can be found in the VCU University Computer Center IT Professionals Intranet under Security Baselines. Access to the IT Professionals Intranet requires approval. Requests for access can be made via email to uccnoc@vcu.edu.

1. **Computer Network and Resources Use Policy**
2. **Information Security Policy**
3. **Exposure and Breach of Information Policy**
4. **Data Classification Standard**
5. **Information Technology Policy Framework**
6. **ISO / IEC 27001 and ISO / IEC 27002 standards**

7. VCU Network Configuration and Security Baseline

Revision History

This policy supersedes the following archived policies:

5/14/2012	VCU Network Security Standards
02/02/2015	Network Management and Security (Formerly called VCU Network Security Standards)
08/10/2015	Network Management and Security
05/25/2017	Network Management Security (now revised as a Standard)

FAQs

1. What must occur when handling a network security incident?

When a network intrusion attempt is confirmed to be a security incident, the following procedures are performed, and may impact network connectivity and / or system availability for affected IT systems.

- Upon the discovery of the security incident, VCU Information Security Office and / or VCU Network Services will contact designated IT support personnel responsible for the affected asset. If immediate threat to VCU assets or data is perceived, VCU Information Security Office in collaboration with VCU Network Services will disable the network access for the affected asset with immediate notification to designated IT support personnel for the affected asset.

- For incidents with non-immediate threats, designated IT support personnel responsible for the affected asset will have up to 24 hours to respond, acknowledge and triage the incident in collaboration with the VCU Information Security Office. If no adequate response is received within the first 24 hours, VCU Information Security Office or VCU Network Services will disable the network access for the affected asset.

- If network access to an affected asset is disabled due to immediate threat or inadequate response, network access will only be restored when the threat is effectively eliminated, and the elimination of the threat is verified by the VCU Information Security Office. Digital forensic data maybe collected by the VCU Information Security Office from the affected assets if additional analysis is needed.

2. What are the requirements and the process associated with network access provisioning?

The following procedure will be followed for the provisioning of network access, which includes static IP address request, network change request, IP address request for servers, and port change requests. Typical connection of desktop or laptop workstations to the network without the need of static IP addresses or special network or port configurations does not need to go through this process.

- A network access provisioning request must be submitted through the Technology Services request ticketing system at https://servicedesk.vcu.edu or through the HelpIT center at (804) 828-2227. The request must include the request details, contact information for the requester, and budget code to be charged if hardware installation is needed.
- Following the request, the requester will complete a system security plan for the asset that needs network access. The system security plan can be accessed from http://go.vcu.edu/serverassessment .

- Once the system security plan is reviewed and approved by the VCU Information Security Office, the VCU Network Services team will then be cleared to provision the necessary network access for the asset.

- If the asset is a server or server-like device hosted or housed outside of the University Computer Center, the requester is responsible for coordinating the registration of the asset on the Server inventory in the VCU IT Professionals Intranet (http://go.vcu.edu/itpros). If the asset is hosted or housed within the University Computer Center, then the University Computer Center staff will coordinate with the requester to register the asset in the Server inventory.