Area of Responsibility:	Information Technology
Responsible Contact:	Chief Information Officer
Policy Identification:	Network Security Policy
Effective: Date	07/01/2021
Last Revised:	04/26/2022

POLICY

This policy provides general security requirements for Virginia Union University networks and network devices consisting of routers, switches, wireless controllers, wireless access points, and other embedded network devices providing network infrastructure services to the Virginia Union University environment, authorizes access, and controls information flows from and to networks. Access requirements for Virginia Union University networks are included in the policy.

This policy applies to all users of Virginia Union University Information Resources. The Information Technology team is responsible for implementing systems that conform to this policy to ensure the protection of data, assets, and information that are stored on the devices residing on the network, and the information flowing through the network.

PROCEDURES

Network Architecture
The Virginia Union University network architecture must meet the key security related architecture requirements described in the following sections.

Network Segmentation
The Virginia Union University network is separated into different functional zones to protect critical assets and provide business required access. There are five primary network zones, specifically:

- Internet
- DMZ
- Intranet
- Application specific networks (e.g., Labs or Security Cameras)

Proper controls, normally firewalls or access control lists (ACLs), are required to ensure only authorized network traffic passes between the different zones. Additionally, packet inspection and logging are required between the internet, DMZ, and intranet.
The IPS shall be capable of inspecting TLS encrypted traffic without notifying the users that the inspection is occurring. Virginia Union University will not inspect the content of traffic to or from known financial or health providers.

Network Security Devices
Network security devices including firewalls and intrusion prevention systems (IPS) are required between the

following network zones as shown in Figure 1:

- Internet
- DMZ
- Intranet

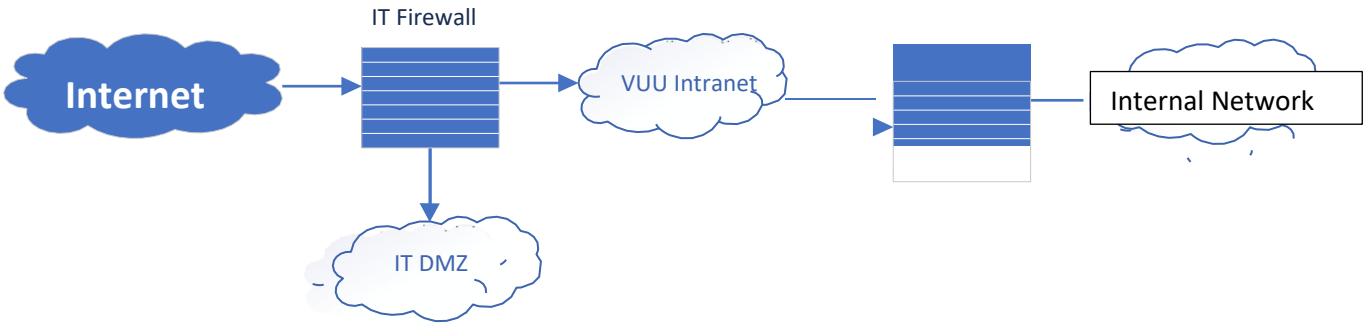

Figure 1: Network Zones

Network Device requirements

Network[1] devices must conform to the following requirements:

- Have a support contract from the manufacturer including security updates
- Configured to industry best practices including following the manufacturer's hardening guide where applicable.
- Appropriate system logging is enabled including, at a minimum, successful and failed logins.
- Send logs to a central logging facility
- Configuration backups are maintained
- All devices must be inventoried and maintained in the HELPDESK SYSTEM
- Security related patches and updates are evaluated within seven (7) days
- Security patches and updates are applied within twenty-eight (28) days, unless the evaluation indicates the patching must be done sooner

IP Addresses

Virginia Union University shall use either Public IP address allocated to Virginia Union University or private IP addresses. Public IP addresses used by Virginia Union University systems hosted in cloud providers are allocated to Virginia Union University by the cloud provider.

Domain Names

Virginia Union University shall only use DNS domains registered to Virginia Union University or its subsidiaries for Virginia Union University systems including servers and laptops. Vendor hosted domains including those for software-as-a- service vendors may use vendor provided DNS domains.

Network Map

The IT organization will ensure network maps, diagrams and configuration documentation of routers, switches, etc., exist. Network maps will be reviewed for completeness and accuracy at least annually. Network changes

1 Network devices include both physical and virtual devices that process or protect network traffic. Examples of network devices include routers, switches, firewalls and universal threat management (UTM) devices.

including new devices[2], changes in IP ranges, or new external connections must be documented within fifteen (15) days of the change. Updated electronic drawings must be approved in 30 days.

Network Access
Ensuring only authorized machines and users can access a network is critical to securing Virginia Union University.

Onsite Access
Three types of onsite access, described in the following sections, are supported when implemented securely.

Physical
Only authorized devices may be attached to the physical network. Unused ports on network devices must be administratively disabled. Wherever possible technical controls including 802.1x should be implemented to secure physical network access.
Only Virginia Union University managed systems are authorized to connect to the corporate physical network.

Wireless
Only authorized devices may connect to Virginia Union University wireless networks. Access to the Enterprise Wireless network requires 802.1x or other access controls that ensure the user and device is authorized to access the Enterprise Wireless network.
Wireless networks used primarily for machine communication may use MAC filtering with a shared password if other controls are not practical. Except for the Guest Wireless Access.

Guest Wireless Access
Guest wireless access is primarily provided for guests of Virginia Union University. A unique username and password should be used for guest access. If a shared password must be used, the shared password shall be changed quarterly.

Guest Physical Access
When third-party devices cannot use Guest Wireless Access, a dedicated physical connection can be approved by the Senior IT Director or the Cyber Security Leader. This physical network connection must be isolated from the Virginia Union University networks at Layer 2.

Remote Access
User Remote Access – VPN
Remote connections by users to Virginia Union University networks require the use of approved VPN software or hardware. Multifactor authentication, as defined in the Identity and Access Management Policy, is required for all VPN connections.[3]
Only Virginia Union University managed devices are allowed unrestricted VPN access. That is, Virginia Union University devices when connected to the VPN will have the same access as if connected to the Virginia Union University physical network.

Non-Virginia Union University managed devices may be granted limited remote network access with documented approval from the Cyber Security Leader or Senior IT Director.

---

2 This applies to network devices, not servers or personal computers

System Remote Access

Site-to-Site VPN

Vendors and customers that need to communicate with Virginia Union University internal systems may connect using a site-to-site VPN. Access to individual systems is based on business requirements. Site-to- site VPNs require approval from the Cyber Security Leader or Senior IT Director.

System to System Remote Access

In many cases vendors and customers need to access a single system inside Virginia Union University. This can be accomplished using a reverse proxy. All inbound connections must terminate at the network firewall, load balancer or reverse proxy and then a new connection shall be established to the internal system. Only specific source IP address that are registered to the vendor or customer may be used.

System to System remote access requires documented approval from the Cyber Security Leader or Senior IT Director.

Inbound Internet Access

Virginia Union University needs to provide public access to business information. Any inbound internet increases the risk of a successful attack against Virginia Union University information resources. Whenever possible a third- party company should be used to host an extract of the business information in an environment that is separated from Virginia Union University networks.

Inbound internet access must use a two or three tier structure with the first, web, tier existing in a DMZ. Machines in the DMZ must be standalone and not joined to the Virginia Union University active directory domain. Inbound access to webservers must be protected by a Web Application Firewall (WAF).
Inbound internet access requires documented approval from the Cyber Security Leader or Senior IT Director.

Encryption

All sensitive data transmitted across Virginia Union University network shall be encrypted at the application or transport layer using TLS1.2 or higher.

Device and Change Management

The Information Technology team(s) are responsible for implementing a network change management procedure that incorporates cyber security. The Information Technology team(s) are responsible for ensuring only authorized individuals perform administrative duties on network equipment.

SUPPORTING DOCUMENTS (if applicable)

GLOSSARY

Documented Approvers:

_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**
_____	_____
Name, Title	**Date**