NETWORK SECURITY POLICY

Table of Contents

1. Introduction

1.1 Purpose

Howard University (HU) resources, such as Internet/Intranet/Extranet-related systems, are to be used for Howard business purposes in serving the interests of the University.

The participation and support of every student, faculty, employee and affiliate who deals with information and/or information systems is necessary to achieve effective security. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to delineate acceptable use of HU technology resources. These rules are in place to protect the user of these resources and the University. Inappropriate use exposes HU to risks including virus attacks, compromise of network systems and services, and legal issues.

1.2 Scope

This policy applies to all Howard University networks, both the perimeter and the infrastructure, and the parties with which we do businesses.

1.3 Maintenance

This Policy will be reviewed by the University's Information Security Office annually or as deemed appropriate based on changes in technology or regulatory requirements.

1.4 Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to University-owned Information Systems. Additional administrative sanctions may apply; up to and including termination of employment or contractor status with the University, or expulsion of student workers. Civil, criminal and equitable remedies may also apply.

1.5 Exceptions

Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the University's Provost, or Chief Operations Officer. All exceptions will be formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

2. Policy

The data network is a shared resource used by the entire University community and its affiliates in support of the business processes and academic missions. Business units and community members must cooperate to protect the network by securing computers and network devices in order to secure access. In addition, they must certify that the devices connecting to the business unit's network are in compliance with the policies and procedures as established by Enterprise Technology Services (ETS).

Concurrently, academic, administrative and support units are responsible for the efficient, effective and secure operation of their local networks. This policy is designed to help protect the University's central and distributed telecommunications and computing environment from accidental, or intentional damage, and from alteration or theft of data while preserving appropriate access and use.

This policy is established under the provisions of Howard University's Information Security Policy Program.

The following rules define the ETS's policy regarding access to the University network:

1. Only authorized people can gain access to Howard University's networks. Positive identification is required for system usage. All users must have their identities positively identified with user-IDs and secure passwords--or by other means that provide equal or greater security--prior to being permitted to use Howard University-owned computers.

2. User-IDs must each uniquely identify a single user. Each computer user-ID must uniquely identify only one user, so as to ensure individual accountability in system logs. Shared or group user-IDs are not permitted.

3. Use of service accounts for local log-ins by any individual is prohibited. This rule is designed to prevent unauthorized changes to production data by accounts that allow groups of users to employ the same password. In cases where users require authorities inherent in service accounts, the user's manager must obtain approval from ETS. Those privileges may be assigned to individual users on as-needed basis and must be revoked when they are no longer necessary.

4. Access controls required for remote systems connecting to production systems. All computers that have remote real-time dialogs with Howard University's IT production systems must run an access control package approved by ETS.

5. Multiple simultaneous remote external network connections prohibited. Unless special permission has been granted by the Director of Information

Security, (CIO/CISO/ISM), computer systems must not allow any user to conduct multiple simultaneous remote network connections.

6. All log-in banners must include security notice. Every log-in screen for multi-user computers must include a special notice. This notice must state: (1) the system may only be accessed by authorized users, (2) users who log-in represent that they are authorized to do so, (3) unauthorized system usage or abuse is subject to penalties, and (4) system usage will be monitored and logged.

7. Security notice in log-in banner must not disclose system information. All log-in banners on network-connected Howard University computer systems must simply ask the user to log-in, providing terse prompts only where essential. Identifying information about the organization, operating system, system configuration, or other internal matters must not be provided until a user's identity has been successfully authenticated.

8. Users must log off before leaving sensitive systems unattended. If the computer system to which users are connected or which they are currently using contains sensitive information, and especially if they have special access rights, such as domain admin or system administrator privileges, users must not leave their computer, workstation, or terminal unattended without first logging-out, locking the workstation, or invoking a password-protected screen saver.

9. Academic, Administrative, and Supporting Enterprise Technology Services' staff must:

   a. Follow policies and procedures, as established by ETS, to validate firewall activation, operating system installation, application software security patches and virus protection updates for all devices in the unit's areas of physical or administrative control that are to be, or are configured to utilize network resources that are controlled and managed by ETS.

   b. Follow policies and procedures, as established by ETS, for using automated tools to test devices connected to the business unit's local wired or wireless data network for compliance. Noncompliant devices are to be disconnected, disabled or quarantined until the device is brought into compliance. When devices are not compliant, operating units, or individuals and their information technology staff must employ compensating controls. Units must document compensating controls and/or any exceptions. These must be reviewed, tested, and approved by Information Security.

   The operating business unit or individual must retain the approved documentation for audits as long as the device is in operation. Any connection to the Internet, or to a national or regional network from a private network operated by an academic, administrative, or support unit, must be made via University network resources. The Executive Director of Enterprise Technology Services must approve any exceptions to this requirement.

10. All network access attempts (success or failure) must be logged and retained for auditing.

11. Server

Howard University embraces an open information technology environment to encourage the use of technology in pursuit of the University’s teaching, learning, and research missions and supporting administrative functions. However, within this open environment, the University must also preserve and safeguard its electronic information resources and comply with applicable laws and regulations, while facilitating activities the support the University’s missions. In a highly distributed technological environment, operation and management of electronic information resources is broadly distributed.

This policy applies to all servers that Howard University ETS is responsible to manage. This explicitly includes any system for which Howard University ETS has an obligation to administer. This also includes all server systems setup for internal use by HU regardless of whether ETS retains administrative obligation or not.

Policy

Howard University ETS operational group responsible for system administration and must manage all internal servers. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by ETS. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by ETS.

11.1 Servers must be registered within the Enterprise Management System. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- Information in the Enterprise Management System must be kept up-to-date.

11.2 Each device must meet the following minimum standards prior to, and after connecting to the data network or support infrastructure:

- The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic.

- Current operating system and application software with current security patches must be installed.

- The device must be protected against malicious or undesired software such as viruses, spyware, or adware.

- Access to the device must require appropriate authentication controls such as account identifiers and robust passwords.

- The device must be certified and registered by ETS as equipment that has met all security criteria, prior to connecting to the network.

11.3 SERVER GENERAL CONFIGURATION GUIDELINES

The following items serve as provisioning configuration guidelines for the servers that are managed by ETS staff:

- Operating System configuration should be in accordance with ETS-approved guidelines.

- Services and applications that will not be used must be disabled where practical.

- Access to services should be logged and/or protected through access-control methods such as Transmission Control Protocol (TCP) Wrappers.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is available.

- Do not use root account when a non-privileged account can performed the task.

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).

- Servers should be physically located in an access-controlled environment.

- Servers are specifically prohibited from being operated in uncontrolled cubicle areas.

11.4 Internal network addresses must not be publicly released.

The internal system addresses, configurations, and related system design information systems and users outside the ETS internal network cannot access this information.

11.5 All Internet Web servers must be firewall protected.

All connections between Howard University's internal networks and the Internet (or any other publicly-accessible computer network) must be protected by a router, firewall, or related access controls approved by ETS.

11.6 Public servers on Internet must be placed on separate subnets.

Public Internet servers must be placed on subnets separate from internal ETS networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

12. MALWARE PROTECTION

Howard University ETS is entrusted with the responsibility to provide professional management of the university's servers as outlined in this policy. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

This policy applies to all servers that Howard University ETS is responsible to manage. This explicitly includes any system for which ETS has an obligation to administer. This also includes all server systems setup for internal use by Howard University, regardless of whether ETS retains administrative obligation or not.

Policy

Howard University ETS operations staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

12.1. ANTI-VIRUS

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server

- NBT/Microsoft Share access is open to the server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet
- Other “risky” protocols/applications are available to this system from the Internet at the discretion of the Howard University IT Security Administration

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Outbound web access is available from the system

12.2 MAIL SERVER ANTI-VIRUS

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

12.3 ANTI-SPYWARE

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

12.4 NOTABLE EXCEPTIONS

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions applies to this system:

- The system is a SQL server
- The system is used as a dedicated mail server
- The system is not a Windows based platform

12.5 Enforcement:

The responsibility for implementing this policy belongs to all operational staff at Howard University. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the Howard University ETS Information Security Officer. Any employee, student, faculty, guest, or contractors found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

13. ROUTER

This policy describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Howard University ETS.

All routers and switches connected to Howard University IT production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the Internet DMZ Equipment Policy.

Policy

13.1. All routers within Howard University IT Enterprise must meet the following configuration standards:

No local user accounts are configured on routers. Routers must use TACACS+ for all user authentications.

The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization

13.2. All routers within Howard University IT Enterprise must disallow the following:

- IP directed broadcast

Incoming packets at the router sourced with invalid addresses such as RFC1918 address

- TCP small services
- UDP small services
- All source routing
- All web services running on router

13.3. Any external network connections, inbound or outbound, must be authenticated or secured via approved standards.

Before dial-up users reach a log-in banner, all inbound dial-up lines connected to Howard University IT internal networks and/or computer systems must pass through an additional access control point, such as a firewall, which has been approved by ETS. Unless ETS has first approved the action in writing, Howard University staff must not enable any trusted host relationships between computers connected to the Howard University internal network.

13.4. Use Enterprise standardized SNMP (Simple Network Management Protocol).

Routers must be included in the Enterprise Management System with a designated point of contact. Users must have explicit permission by ETS to access or configure any router. All activities performed on these devices may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on these devices.

13.5 Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

14. FIREWALL

The firewall policy dictates how the firewall should handle application traffic such as web, email, or telnet. The policy describes how the firewall is to be managed and updated.

14.1 Real-time external network connections require firewalls.

Before reaching a log-in banner, all in-bound real-time external connections to Howard University IT internal networks and/or multi-user computer systems must pass through an additional access control point such as a firewall, gateway, or access server.

- The functionality of firewalls will be setup to ensure secure Internet connections and the connections to other networks.
- Firewall rule-sets must be created for implementing security controls as they pertain to the handling of applications traffic such as web, email and other business processing.
- Users, who are at remote locations, must verify that firewall appliances are in place to secure their connections to the Internet and Internet Service Providers before establishing the connection with the University network.

14.2 Firewall configuration change requires ETS permission.

Firewall configuration rules and permissible service rules established by IT Security and Disaster Recovery have been reached after evaluation. These rules must not be changed without first obtaining the permission of ETS Information Security Management.

- The University must monitor incident response team reports and security websites for information about current attacks and vulnerabilities.
- The firewall policy should be updated as necessary.
- A formal process must be used for managing the addition and deletion of firewall rules.
- The University must ensure that administrators receive regular training in order to stay current with threats and vulnerabilities.

15. INTERNET DMZ EQUIPMENT

This Policy defines the standards to be met by all equipment owned and/or operated by Howard University ETS that is located outside the University's Internet firewalls (the demilitarized zone or DMZ). These standards are designed to minimize the potential exposure to Howard University from the loss of sensitive or University confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of IT resources.

Devices that are Internet facing and outside the University’s firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the university’s firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

All equipment or devices deployed in a DMZ owned and/or operated by Howard University (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Howard University must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "howard.edu" domain or appears to be owned by Howard University.

All new equipment that falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from ETS. All existing and future equipment deployed on Howard University's un-trusted networks must comply with this policy.

Policy

Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by Information Security for DMZ systems, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the University-wide enterprise management system. At a minimum, the following information is required:
  - Host contacts and location.
  - Hardware and operating system/version.

    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the University wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of Information Security upon demand, per the Audit Policy.
- Changes to existing equipment and deployment of new equipment must follow and University change management processes/procedures.

To verify compliance with this policy, Information Security team will periodically audit DMZ equipment per the Audit Policy.

16. General Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by ETS as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot-fixes recommended by equipment vendor and ETS must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by ETS.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by ETS) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to ETS approved logs. Security-related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- ETS will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

17. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the DMZ Equipment Deployment Process.
- Configuration changes must follow the University Change Management (CM) Procedures.
- ETS must be invited to perform system/application audits prior to the deployment of new services.
- ETS must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

18. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

19. Network Management/ Access Requirements

- All networks on the Howard University campus are installed and maintained by Enterprise Technology Services.
- To assure the integrity and availability of network services, no other network communications (with the exception of commercial cellular telephony networks) shall be permitted on University facilities.
- No networking equipment (routers, managed switches, DHCP servers, DNS servers, WINS servers, VPN servers, remote access dial-in servers/RADIUS, wireless access points, hardware firewalls – shall be permitted without a written exception from ETS (ETS Infrastructure group).
- All devices connected to HU networks shall be registered with ETS when initially attached to the network. This applies to printers, computing systems, laboratory equipment, and communications devices that use TCP/IP network protocols. The registrant must be a current faculty, staff, student, or affiliate account user with a valid and active Network ID. Information on how to register a network device can be obtained by contacting the ETS Help Desk. Unregistered devices are subject to disconnection from the HU Network, without notice, whether or not they are disrupting network service.
- Currently devices connected to the HU Guest (HU-Visitors) wireless network are unregistered. As wireless registration services become available, all university-purchased or owned hosts shall be registered in a similar manner to wired network registration. HU users accessing the Howard IT resources via wireless networking may assure the privacy of the network communications by using the HU VPN software.

- No device or program that has the potential to disrupt network service to others is permitted on the HU Network without prior arrangement with ETS.

20. Protocol Standards

The management of network protocols shall be performed by information systems administrators and network administrators to assure the efficiency, availability, and security of the common resources, in accordance with the governing HU Acceptable Use Policy.

Simple Mail Transfer Protocol (SMTP):

- All email protocol traffic shall utilize the centralized mail gateways (smtp.howard.edu). Inbound mail traffic with destination addresses for servers other than those operated by ETS shall utilize a DNS MX record to relay that traffic through the centralized mail gateways. All outbound traffic shall utilize the SMTP gateway.
- The use SSL or TLS based communication standards for email client to email server communication is preferred such that the authentication session is the protected transaction.

Domain Name Services Protocol (DNS):

- All hosts on HU networks shall utilize the Howard DNS systems. All hosts connected to HU networks receive a howard.edu domain name extension. No host connected to Howard networks shall be addressable by any DNS name other than that provided by Howard.
- No host with a howard.edu domain name (and an IP address within the Howard network spaces) will use an IP address outside the University's registered name space without a written exemption from Enterprise Technology Services.

Dynamic Host Configuration Protocol (DHCP):

- All hosts on Howard networks shall either obtain and use a static IP address or use the Howard DHCP service to obtain an assigned IP address. Users shall not use a self-assigned IP address, or operate a DHCP server. The use of bootstrap (BOOTP) shall be governed in the same manner as DCHP.

Banned Protocols:

- Enterprise Technology Services keeps a listing of banned protocols which have shown to interfere with the architecture and management of the HU network environment.

21. Remote Access

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private key with strong pass-phrases.
- At no time should any employee provide his or her login or email password to anyone, not even family members.
- Employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to the enterprise network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Employees, contractors and students with remote access privileges to the enterprise network must not use non-University email accounts or other external resources to conduct University business.
- Routers for dedicated Integrated Services Digital Network (ISDN) lines configured for access to the University's network must meet minimum authentication requirements of Challenge-Handshake Authentication Protocol (CHAP).
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time
- Frame relay must meet minimum authentication requirements of Data Link Connection Identifier (DLCI) standards.
- All hosts that are connected to the University's internal network via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.
- Third party connections must comply with requirements as stated in the Third Party Agreement.
- Personal equipment that is used to connect to the network must meet the requirements of University-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from ETS.
- Direct network connections with outside organizations must be approved. The establishment of a direct connection between the University's systems and computers at external organizations, via the Internet or any other public network, is prohibited unless this connection has first been approved by the ETS Department.
- Inventory of connections to external networks must be maintained. ETS must maintain a current inventory of all connections to external networks including telephone networks, EDI networks, extranets, the Internet.

VPN

Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefit of VPN, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy.

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.
- When actively connected to the enterprise network, the VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by ETS.
- All computers connected to the internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the enterprise standard, this includes personal computer.
- VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- Users of computers that are not owned by the University must configure the equipment to comply with VPN and Network policies.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the network, and as such are subject to the same rules and regulations that apply to the University's owned equipment, i.e., their machines must be configured to comply with ETS's Security Policies.

3. Appendix A – Definitions

- *Server*: For purposes of this policy, a server is any computer system residing in the physically secured data center owned and operated by Howard University ETS. In addition, this includes any system running an operating system specifically intended for server usage as defined by the ETS Manager that has access to internal secure networks. This includes, but is not limited to, Microsoft Servers and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to.

- *Malware*: Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

- *Spyware*: Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

- *Anti-virus Software:* Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

- *Production Network*: The "production network" is the network used in the daily business of Howard University ETS. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to Howard University employees or affiliates, or impact their ability to do work.

- *Lab Network:* A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, research, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to Howard University nor affect the production network.

- *DMZ (de-militarized zone)*: Any un-trusted network connected to, but separated from, Howard University's IT network by a firewall, used for external (Internet/partner, etc.) access from within Howard University, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.

- *Secure Channel:* Out-of-band console management or channels using strong encryption. Non-encrypted channels must use strong user authentication (one-time passwords).

- *Un-Trusted Network*: Any network firewalled off from the University network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

- *Cable Modem*: Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

- *CHAP*: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.

- *DLCI*: Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

- *Dial-in Modem*: A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

- *Dual Homing*: Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a HU provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Howard University and an ISP, depending on packet destination.

- *DSL*: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
- Frame Relay: A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

- *ISDN:* There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

- *MX record:* An MX record or Mail exchanger record is a type of resource record in the Domain Name System (DNS) specifying how Internet e-mail should be routed. MX records point to the servers that should receive an e-mail, and their priority relative to each other.

- *SSL:* secure sockets layer, an encryption method for communication between the mail client and mail server.

- *TLS:* transport layer security, an encryption method for communication between a mail client and a mail server, or between mail servers.

- *TCP/IP:* transmission control protocol and internet protocol, which define how communications are currently implemented in the Howard network infrastructure.

- *IP address*: Internet protocol address, an essential networking element which permits traffic to be routed to a specific host.

- *Cloud services*: Software and/or systems that are hosted in off-campus data centers that rely on network communications to permit access for users in the Howard network environment.

- *CHAP*: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.

- *DLCI:* Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

- *Dial-in Modem:* A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

- *DSL*: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

- *Electronic data interchange (EDI*): is a method for transferring data between different computer systems or computer networks Frame Relay A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

- *ISDN*: There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

- *Remote Access*: Any access to a Howard University IT network through a non-IT controlled network, device, or medium.

- *Split-tunneling*: Simultaneous direct access to a non-Howard University network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Howard University's IT network via a VPN tunnel.

- *VPN*: Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

- *IPsec Concentrator*: A device in which VPN connections are terminated.

- *L2TP:* Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.