Network Security Policy

Purpose
The purpose of this policy is to ensure secure and reliable network access and performance for the University community. Internet access to University resources and University access to Internet resources are an important part of education and business today. This policy is intended to protect the integrity of the campus network and to mitigate the risks and losses associated with security threats to the campus network and information systems.

Like many university campuses, Villanova University is experiencing an increase in unauthorized access or attempts to access its data network and computer systems. In addition, computer systems on campus have been used as platforms to launch similar attacks on systems on the Internet at large.

The purpose of this security policy is to:

- Provide a reliable campus network and Internet connection to conduct the University's business.
- Provide only authorized access to institutional, research or personal data and information.
- Protect computer system and network integrity at Villanova University.

Specifically, this policy will protect University computing resources from:

- Unauthorized access to resources and/or information
- Unintended and/or unauthorized Disclosure of information
- Denial of Service attacks.

How likely are the threats?

The University network is scanned every day from the Internet. Much of this scanning is done to determine the number and location of potentially vulnerable systems on the campus network. Villanova University computer systems have been compromised, and have been used to attack other systems on the Internet. Denial of Service (DOS) attacks from the Internet have occurred in the past, and will most likely be attempted again in the future against University systems.

Risks to our academic mission are most apparent. The loss or corruption of data or unauthorized disclosure of information in research and instructional computers, student records, and financial systems is unacceptable. The campus also has a legal responsibility to secure its computers and networks from misuse. This policy will allow the University to handle network security responsibly.

The University considers any violation of acceptable use principles or guidelines to be a serious offense, and reserves the right to test and monitor security, including copy and examine any files or information resident on university computer systems allegedly related to unacceptable use. It is the responsibility of the Office for University Information Technologies to ensure a reliable network.

Scope

This policy applies to any existing or future connection(s) to the University's data network.

Policy

Addressing and Domain Services

1. Individuals, academic colleges/departments or administrative departments at Villanova may not create nor support an Internet domain, hosted from the University’s network without prior approval of the Office for University Information Technologies (UNIT).

2. UNIT will administer the Villanova University IP address space.
will also administer the villanova.edu and vill.edu domains. UNIT will manage any additional domains that support the mission of the University. (UNIT will also administer all other network addressing systems at Villanova, e.g., Novell NetWare and AppleTalk.)

3. Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to computers. UNIT will give prior notice to affected users before making any changes.

**Network Connections**

1. Villanova University departments, faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system to the University’s data networks without the prior review and approval of UNIT.

2. Colleges or departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the University must get prior approval from UNIT.

3. All devices placed on the University’s network must be registered with UNIT. All authorized University network users (faculty, staff or students) must be assigned a physical network port and network address by UNIT. Network connections at public access ports are restricted to authorized members of the University community.

4. Physical access to University networking equipment (routers, switches, hubs, etc.) is not permitted without the prior approval of UNIT.

5. UNIT will provide a general method for network authentication to University systems.

**External Services and Requests**

1. UNIT will take action to prevent source network address forgery (spoofing) of internal network addresses from the Internet. UNIT will also take action to protect external Internet sites from source address forgery from the University’s network.

2. The University’s external Internet firewall policy is to deny all external Internet traffic to the University’s network unless explicitly permitted. Access and service restrictions may be enforced by IP address and/or port number. Proxy services may be used in conjunction with the firewall to restrict usage to authenticated individuals. This policy is designed to protect University network users from attacks launched from the Internet.

3. The University must identify which systems will offer Internet services, to better protect them. To facilitate this, academic colleges/departments and other administrative departments must register with UNIT systems that require access from the Internet. These systems must also be protected by access control software, e.g., TCP Wrappers.

4. The University’s internal Internet firewall policy is to deny all internal IP traffic outbound to the Internet unless explicitly permitted. This policy is designed to protect others on the Internet from attacks launched from the University’s network.
5. Some network services through standard ports is supported. (See Internet Services list for supported services.) However, services may be restricted to a limited number of subnets or hosts. For example, electronic mail (SMTP, Port 25) may only be sent and received by authorized mail servers on campus. User access to the mail accounts (POP3, Port 110 and IMAP, Port 143) on these servers will be permitted from off-campus through the firewall.

6. Most network services through non-standard ports are not supported. (See Internet Services list for exceptions.) Services through non-standard ports may be restricted to a limited number of subnets or hosts. For example, WWW access via the standard HTTP port (Port 80) will be permitted, but to some other arbitrary port number may not be permitted.

7. Limited encrypted tunnels for passing through the firewall to internal resources, such as X-Windows, is permitted with the prior approval of UNIT. The recommended method is to use Secure Shell (SSH). IP Multicast tunneling is not permitted.

8. All modem connections that allow someone from outside to access to the University’s network must be registered with UNIT. The University reserves the right to block any modem connections, or disconnect any computer system, that allows unauthorized access to the network.

**Network Security**

1. UNIT shall identify the appropriate network security level for University systems, in collaboration with academic and administrative departments. These levels should be divided into the following categories, from highest to lowest: Mission-critical, Important, Normal and Low. Efforts shall be made to protect these systems at the appropriate level. UNIT will determine the security status of University computer systems and review it periodically.

2. UNIT will investigate any unauthorized access of University computer systems. UNIT will work with administrative departments and law enforcement when appropriate.

3. Systems on the network must have adequate security installed and maintained. All systems connecting to the University network must be configured and maintained in such a manner as to prohibit unauthorized access or misuse. For example, a guest account must have a secure password.

4. If security problems are observed, it is the responsibility of all Villanova University network users to report problems to the appropriate system administrators or UNIT for investigation.

5. Network usage judged appropriate by the University is permitted. Some activities deemed inappropriate include, but are not limited to:

   - Establishing unauthorized network devices, including router, gateway or remote dial-in access server; or a computer set up to act like such a device.
   - Engaging in network packet sniffing or snooping.
   - Operating network servers of any sort in violation of UNIT guidelines.
   - Setting up a system to appear like another authorized system on the network (Trojan).
   - Other unauthorized use prohibited by the University’s acceptable use or other UNIT policies.
**Enforcement**

1. Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network in any way is subject to immediate disconnection from the University’s network. The Data Network Services Department or other UNIT department may require specific security improvements where potential security problems are identified.

2. Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.

**Monitoring and Auditing**

1. UNIT will maintain traffic logs of the firewall for security auditing purposes.

2. UNIT reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a University policy violation, criminal activity, monitoring required by law or at management request. Reasonable cause may be provided by a complaint of a policy violation or crime or as incidentally noticed while carrying out the normal duties of the Data Network Services Department.

3. UNIT may perform a security audit of any computer system attached to the University’s network with the permission of the system administrator or his superior. UNIT will provide a report after the audit is completed.

**Status**

1. This document will be reviewed on a regular basis. Changes to be made to this document must be approved by the University’s IT governing bodies.

2. UNIT will report on a regular basis to UCIT on the status of network security at Villanova University.

3. UNIT will create procedures to execute this policy, and to inform the University community of its existence and importance.

4. A Security Policy Committee will be created to review this policy and ensure fair enforcement. This committee will provide a mechanism for members of the University community to propose changes to procedures and firewall restrictions.