# Network Operations Center and Security Overview

## NOC OVERVIEW

The Network Operations Center (NOC) is a state-of-the-art technical facility that houses servers and network equipment to ensure stable and reliable service for University enterprise systems. It is a centralized management center that is capable of identifying, notifying, and repairing problems when they occur and projecting when and where they might occur.

**Services:** The NOC is staffed 24x7 and systems are constantly monitored for problems. The Enterprise Monitoring and Enterprise Backup services are provided via this facility. NOC services include secure hosting and management of Enterprise technology services such as email, web services, enterprise network firewalls, and student and financial systems. Many University departments leverage the NOC's enterprise-caliber server hosting service for applications that require a high level of availability and security. The NOC also hosts the Center for Simulation and Modeling's high-performance computing cluster, as well as a FISMA-compliant environment for researchers working on projects that require special handling of sensitive data.

**Physical and Environmental Protections**: The NOC is secured by locked access points at all entrances. Physical access is restricted to designated Computing Services and Systems Development (CSSD) staff and approved guests. A list of personnel with authorized access to the NOC facility is maintained and reviewed on a monthly basis. Access to the NOC facility is controlled by an automated system, and all access is monitored by the University of Pittsburgh Police Department. University employees, facilities management, and vendors who do not work at the NOC are required to be pre-authorized as a guest to gain entry to the NOC. Once on site, they must electronically sign in and sign out each time they enter and leave the building, and are escorted while within the facility.

The NOC has redundant power sources along with uninterruptable power supplies and backup generators to prevent widespread system failure due to electrical outages. All cabling is routed under floors and in enclosed cabinets. Power is provided via waterproof, positive, locking connections. The NOC employs a fully monitored pre-action fire protection system, which would reduce the amount of damage that may occur in the event of a fire. The NOC is cooled by 11 monitored air conditioning units that are centrally controlled, in addition to an in row water cooling system for all research computing clusters.

**Help Desk:** The functions of the Technology Help Desk are co-located and closely integrated with the NOC to provide the best possible level of service to the University community.

## SECURITY OVERIVEW

As new security threats emerge and existing threats evolve, our task of protecting the University’s data and technology resources becomes more critical. The key to the University of Pittsburgh’s security strategy is the utilization of a layered approach.

No single technology or process is sufficient in itself to secure the University’s environment. Instead, Computing Services and Systems Development utilizes a “Defense in Depth” strategy that puts in place a series of security controls. A threat that manages to circumvent one control is likely to be thwarted by a control in another layer. The Defense in Depth strategy relies on multiple defensive mechanisms, at multiple layers, performing different tasks.

**Enterprise Network Firewalls:** Network firewalls are our first line of defense and provide the greatest level of protection from attacks originating on the Internet. More than 53,000 network ports across all five campuses are secured behind network firewalls.

**Network Monitoring:** The University’s Network Operations Center (NOC) is at the heart of our security monitoring efforts. The NOC monitors and manages critical University business and academic systems 24 hours a day, every day of the year. The NOC enables us to monitor specific areas of the network for anomalous network traffic, view attempts to breach the network, and identify high levels of network traffic coming from a single destination. Tools at the NOC also enable us to proactively detect and remediate attacks on our residential network.

**Secure Centralized Services**: Access to our network and enterprise systems is controlled by computing accounts that are centrally administered. This provides several security benefits:

• Ensures accounts are created only for authorized individuals

• Allows us to track and trace use of accounts

• Enables us to disable an account and restrict the resources it may access

• Permits us to identify which accounts accessed a system at specific times and locations

All University websites are required to be hosted on our Enterprise Web Infrastructure (EWI). We conduct a thorough security scan of each website on EWI to identify and remediate any potential security vulnerabilities before the website is launched.

**Spam and Virus Spam Filtering**: Our spam and virus filtering service scans all incoming University email. Messages containing viruses and those suspected of being spam are safely quarantined.

**Advanced Detection & Prevention:** We employ a number of advanced detection and prevention tools, and we are constantly adding to our monitoring capabilities. The Network Operations Center receives an alert when suspicious activity is detected, and our Security team follows up and investigates.

**Multi-factor Authentication:** Multi-factor authentication provides a more secure method of accessing University systems. It requires two forms of authentication: something you know (such as your University Computing Account password), and something that you have (such as a device that generates a separate, one-time password). We require multi-factor authentication for all CSSD staff, and we are in the process of making this service available to all individuals who regularly access sensitive data.

**Proactive Auditing:** We constantly audit the network traffic permitted through our firewalls to ensure that the firewalls are providing the proper protection. In addition, we routinely conduct external penetration testing, during which we use a variety of tools to examine our network from the perspective of a potential hacker. These auditing procedures help us to address potential weaknesses before attackers can attempt to exploit them.

**Secure Remote Access:** Part of our secure centralized services, Secure Remote Access encrypts traffic between an individual’s computer and Pitt’s network, making it possible to access restricted University resources while off campus.

**Risk Assessment, Security Planning, and Consulting:** As part of the University purchasing process, our Security team requires all vendors to complete a security questionnaire whenever the vendor will be using University data. The answers provided allow us to evaluate the vendor for risk. Depending on the results, we will either seek to mitigate any risks that are uncovered or decline working with the vendor.

**Compliance Management:** Two of the federal regulations for which our Security team helps to manage compliance are the Federal Information Security Management Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS). Our Network Operations Center provides a FISMA-compliant environment to researchers working on projects that require special handling of sensitive data. We work closely with the Office of Finance and the Electronic Resource Business Group to ensure eCommerce and PCI DSS compliance. Our network is segmented so that all point-of-sale devices are protected behind a firewall and are not able to access or be accessed from the Internet. In addition, these point-of-sale devices use anti-virus software that receives automatic updates through a special connection that we provide.

**Education and Awareness:** Educating students, faculty, and staff about security risks and what they can do to protect themselves is a key component of our layered security strategy. We emphasize good security practices at almost every opportunity, in addition to general and specialized Information Security Awareness Training programs.

**Incident Response:** In the event of a compromise, breach, or other security incident, CSSD Security will implement our incident response policy and coordinate with the department and/or unit.