Cybersecurity Plan

The NHERI Lehigh RTMD Equipment Facility (Lehigh EF) at Lehigh University's ATLSS Engineering Research Center is an awardee of the NSF-funded NHERI program. DesignSafe is the cyber-infrastructure for NHERI and is located at the Texas Advanced Computing Center (TACC). The NHERI Lehigh EF is an integrated member of the DesignSafe team. Cybersecurity protocols are enforced at both the TACC site and the NHERI Lehigh EF to meet NSF requirements. TACC, as the NHERI-CI lead, establishes and implements the NHERI-wide cybersecurity policy and procedure to which the NHERI Lehigh EF adheres.

Roles and Responsibilities

Library and Technology Services (LTS) at Lehigh University is charged with developing and maintaining a secure, fault-tolerant, high-performance campus technology infrastructure to support instruction, research, administrative activities and university communication and outreach. Under this broad mandate, LTS is responsible to develop and promulgate standards which will ensure that the centrally-supported technology infrastructure is secure and operational.

Lehigh University's Information Security Officer is responsible for the enforcement and implementation of the campus-wide cybersecurity policy noted above. The NHERI Lehigh EF falls under the umbrella of the University's cybersecurity plan. The NHERI Lehigh IT Manager is responsible for enforcing the cybersecurity policies and protocols at the NHERI Lehigh EF. The responsibilities include, but are not limited to:

- Operating system integrity
- Malware and virus analysis
- Off-site data backup risk mitigation in case of breach
- Securing physical systems under key lock and ID card access
- Credential administration for facility, staff and students at the Lehigh EF for NHERI related system usage
- Coordinate with LTS for updated University cybersecurity policies
- Coordinate annual security audits with TACC

In the absence of the NHERI Lehigh IT Manager, the ATLSS IT Manager assumes all roles and responsibilities at the NHERI Lehigh EF.

Risk Assessment

LTS reserves the right to scan network-connected hosts to understand what resources are connected to the network and the associated vulnerability of each. LTS will provide advanced notification to the NHERI Lehigh EF prior to initiating such activities. LTS will perform an ongoing assessment of the performance,

utilization, and security of the core network and network subnets. Sub-nets or network-attached devices that pose a risk to the broader network community will be considered for removal from the network until the risk is reduced or eliminated. Action taken will depend on the severity of the discrepancies and the associated vulnerability of the network. To that end, LTS will take all reasonable steps, consistent with the risk posed, to help the NHERI Lehigh EF resolve the non-compliance issue.

For all Lehigh EF Linux-based servers, Linux Malware Detect software is run weekly to investigate for any potential intrusions. Windows-based systems utilize Microsoft Security Essentials for potential intrusions or viruses.

Each NHERI awardee will participate in a NHERI security group with appropriate members from each site. This security group will ensure that best practices are flowed on Incident Response (IR), best practices, and security awareness. In addition, a yearly audit of all NHERI resources will take place and a gap analysis will be created. Any findings in the gap analyses will be reviewed by the NHERI CISO and recommendations made for resolution of those gaps.

Technical Safeguards

Lehigh University's network contains multiple levels of firewalls designed to limit the ability of intruders to access the computers beyond those firewalls. Lehigh University has installed a border firewall system between the campus network and the Internet. These firewalls operate in a "default deny" environment wherein all connections from off campus computers are denied unless specifically allowed through the firewall. The border firewalls are stateful firewalls which keep track of the state of any network connections passing through them. In this regard, any network protocol which exits Lehigh University's network utilizing one network port, but replies to Lehigh on another port, will operate without the need of a firewall exception.

Outside users are recommended to utilize VPN to connect a single off-campus computer to the Lehigh University network. Exceptions for inherently insecure protocols such as telnet (port 23) or ftp (port 21) will not be granted. All requests must include the Lehigh University faculty or staff member responsible for maintaining the security of the computer corresponding to the IP address for which the exception is requested.

Local server and workstation firewalls are enabled at the NHERI Lehigh EF to ensure any malicious activity on the Local Area Network does not affect the NHERI-related systems.

Administrative and Physical Safeguards

Usage of any NHERI Lehigh EF system requires a Lehigh University authenticated username and password. Rooms containing NHERI related equipment are restricted by ID card and key access. Lehigh University user account passwords expire every 180 days.

Policy and Procedures

LTS has developed, published and maintains a set of standards which ensures that network segments and connections can interact appropriately with the campus-wide network, that network security is maintained, and that network hardware and software is maintained. Standards include but are not limited to such issues as:

- Electronic interface
- Cable plant used within the subnet
- Internal configuration
- Security practices
- Use of appropriate network monitoring procedures
- Up-to-date network diagrams
- Appropriate server security facilities in place (including anti-virus and software patch levels)
- Currency of operating system release levels
- Backup procedures are in place and adequate
- Hardware maintenance and/or support is in place
- Software maintenance and/or support is in place
- Departmental contact is assigned and available on-call
- Appropriate technical documentation is available
- All applicable software has been appropriately licensed

All devices connecting to the Lehigh University network, including the NHERI Lehigh EF, must be capable of complying with LTS-selected standard network protocols.

Awareness and Training

LTS has the responsibility to disconnect from the network any network subnet, wireless access point, server, computer, or any other network-connected device that has been identified as being the source of any action which:

- Violates applicable "conditions of use" policies
- Violates local, state, federal or international laws
- Is determined to be a nuisance or potential nuisance

- Is determined to be compromised or is likely to be compromised
- Is interfering with the security or performance of the broader infrastructure

LTS will notify the appropriate departmental contact of the nature of the “violation” and assist the departmental contact to cure the violation.