NHERI@UC SAN DIEGO EXPERIMENTAL FACILITY

LARGE HIGH PERFORMANCE OUTDOOR SHAKE TABLE – LHPOST6

CYBERSECURITY PLAN

1. REVISION HISTORY

REVISION	CHANGELOG	EDITOR	DATE
1	Original	KL	April 2021
1.1	Add/Edit	AH	Oct 2021
1.2	Add/Edit	AH	April 2022

Editor List:

KL: Koorosh Lotfizadeh

AH: Abdullah Hamid

Table of Contents

2. Cybersecurity Plan Summary

The NSF funded Natural Hazards Engineering Research Infrastructure (NHERI) Experimental Facility (EF) at the University of California, San Diego (NHERI@UCSD) provides the earthquake engineering community with a large, high performance, outdoor shake table (LHPOST) to support research in structural and geotechnical earthquake engineering. To ensure the security of the data, the hardware and networks at the EF, the NHERI@UCSD cybersecurity plan has been developed in alignment with requirements set forth by UC San Diego and the NHERI Cyberinfrastructure Awardee DesignSafe. Best practice policies and procedures will be maintained through participation in the annual NSF funded Cybersecurity Summit and DesignSafe cybersecurity activities.

3. Roles and Responsibilities

While cybersecurity is the responsibility of all stakeholders, specific duties and responsibilities of certain key individuals is made explicit here for the sake of clear accountability

3.1 Site Management Team

The site management team will oversee all aspect of cybersecurity at the site under the direction of lead PI:

Joel P. Conte
jpconte@ucsd.edu
858-822-4545

3.2 Site Security Contact

The site security contact is responsible for day-to-day operations related to IT and cybersecurity at the site:

Robert Beckley
(858) 534-6684
rbeckley@ucsd.edu

3.3 DesignSafe Chief Security Officer

The DesignSafe CSO Nathaniel Mendoza, also TACC's Information Security Officer, directs DesignSafe's day-to-day management of its security program, including maintaining a secure environment for the DesignSafe CI, providing security advice to the DesignSafe user community, conducting regular security audits, and coordinating all security related interactions among the various participating NHERI organizations as the leader of the Security Working Group.

3.4 Security Working Group

The DesignSafe CSO Nathaniel Mendoza, also TACC's Information Security Officer, directs DesignSafe's day-to-day management of its security program, including maintaining a secure environment for the DesignSafe CI, providing security advice to the DesignSafe user community, conducting regular security audits, and coordinating all security related interactions among the various participating NHERI organizations as the leader of the Security Working Group.

4. Administrative Safeguards

4.1 Risk Assessment

4.1.1. Risk Assessment Policy and Procedures

DesignSafe's risk assessment policy and procedures are developed, reviewed, updated and disseminated by the DesignSafe CSO. This is done annually, or as needed if urgent security information becomes available and new resources are brought online in the information system. Risk assessment identifies threats to and vulnerabilities of DesignSafe's information system.

4.1.2. Risk Assessment

DesignSafe risk assessment considers vulnerabilities, threat sources and security controls that are planned or in place to determine the resulting level of residual risk posed to DesignSafe's operations, assets or individuals based on the operation of the information system. Risk assessments are conducted, and results documented as threats are identified and addressed.

4.1.3. Audit

DesignSafe's comprehensive cybersecurity approach includes a security audit at each of the NHERI Awardees performed once a year. The audits use security best practices to verify that each server-class system operating at a NHERI Awardee site is operating in a manner to limit the potential for security incidents and breaches. Security incidents and data breaches could invalidate data being collected by scientists, damage experimental equipment, and spread the damage to the DesignSafe resources. No system can be perfectly secure, but regular audits of the system provide vital information for the regular upkeep and secure maintenance of the server systems.

4.1.4. Schedule for Audits

Each NHERI Awardee together with the DesignSafe CSO will determine an appropriate time schedule for performing the audit. This will be coordinated within 6 months after NSF awards are made with each NHERI Awardee. The audits will generally be done once a year and will be performed virtually. However, if a security incident occurs then further audits may be done. In all cases, the timing for the audit will be decided in consultation with the NHERI Awardee, such

that the site operations are minimally affected, and the resources of the site IT staff are optimally utilized.

4.1.5. Actions Following Audits

If there are audit findings, the DesignSafe CSO will recommend corrective actions for the NHERI Awardee to implement. A formal report will be generated once a year that summarizes the results of the audits for each NHERI Awardee. The report will identify the assets that were a part of the audit, where the audit did find vulnerabilities and security breaches, and remediation actions, both short term and long term. This report will not be for public disclosure, keeping in view the security sensitive nature of the information, but will be made available to the NSF.

5. Technical Safeguards

5.1 Proactive Security Monitoring and Detection

The expertise of the Administrative Computing and Telecommunications (ACT) office at UCSD is being leveraged for oversight of the NHERI@UCSD information technology and cybersecurity practices. ACT Support incorporates security leadership with the industry's best practices in compliance with university obligations into ACT Services and advocates secure practices for university systems and data. Services include secure network architecture and firewalls, computer incident response and investigation, system configuration management and anti-malware software, network vulnerability scanning and web application assessment. NHERI@UCSD will adhere to UC San Diego's Minimum Network Standards. Practices that are being followed include registering all devices, using complex passwords, patching software, maintaining host-based firewalls, using encrypted authentication, and following standards for logging all authentication successes and failures on all devices. This applies to computers at the site as well as mobile computing devices accessing the site network. Network access is restricted for all systems.

5.2 Vulnerability Scanning

Workstations are regularly scanned for viruses and malware.

5.3 Recommended Minimum Standards for Systems

5.3.1. Backups

- System administrators should establish and follow a procedure to carry out regular system backups.
- Backups must be verified on a regular schedule, either through automated verification, through customer restores, or through trial restores.

- Systems administrators must maintain documented restoration procedures for systems and the data on those systems.

5.3.2. Change Management

- A documented change control process should be in place for production systems.
- System changes should be evaluated prior to being applied in a production environment. Patches should be tested prior to installation in the production environment if a test environment is available. If a test environment is not available, the lack of patch testing should be communicated to users/customers, along with possible changes in the environment due to the patch, before the patch is applied.

5.3.3. Virus Prevention

- Anti-virus software must be installed, enabled, and updated regularly.
- Installing and enabling anti-spyware software is required on any computer if the machine is used by administrators to browse Web sites not specifically related to the administration of the machine.

5.3.4. System Hardening

- Systems should be initially set up in a protected network environment or by using a method that assures the system is not accessible via a potentially hostile network until it is secured.
- Operating system and application services security patches should be installed expediently and, in a manner, consistent with change management procedures. Strongly consider disabling products that no longer receive security updates from the vendor (e.g., unsupported).
- Services, applications, and user accounts that are not being utilized should be disabled or uninstalled.
- Apply the principle of least privilege to user, administrator, and system accounts.

5.3.5. Monitoring

- If the operating system comes with a means to log activity, enabling and testing of this function is required.
- Operating system and service log monitoring and analysis should be performed routinely. This process should be documented.
- The systems administrator must follow a documented backup strategy for security logs (for example, account management, access control, data integrity, etc.). Security logs should retain at least 14 days of relevant log information.

- All administrator or root access must be logged.

6. Policy and Procedures

6.1 Creating User Accounts

Authentication and authorization of all users of ESEC computer resources rely upon UC San Diego infrastructure. All users must acquire a campus account and be approved by campus designated responsible individuals before they are granted access to resources.

6.2 User Credentials

Single factor authentication is required with a strong unique password. Those passwords expire every 90 days. Administration access is granted only as required.

6.3 Inactive Account Expiration

Accounts that are inactive for 90 days will be deactivated and the user will need to request reactivation of the account.

7. Physical Safeguards

7.1 Physical Access Authorization

Systems with critical data or sensitive information are placed in secure server rooms with limited physical access, alarms, and video surveillance. Desktop computers with access to any sensitive data are required to utilize a passcode lock that is activated by user inactivity.

7.2 Access Control for Transmission Medium

Adequate physical protection is in place for wiring closets and communication demark areas to prevent accidental damage, disruption, or intentional physical tampering of transmission lines.

8. Awareness and Training

Awareness of the DesignSafe Cybersecurity Plan for NHERI Awardees will be achieved via the Security Working Group, and assurance of awareness and compliance is achieved via the aforementioned audits.

NHERI Awardees shall adhere to their local University cybersecurity policies and participate in their local University cybersecurity awareness and training.

Threat Detection and Identification (TDI) staff receive ongoing training on core infrastructure technologies and current security threats, ensuring they continue to be experts in their field

9. Incident Response and Notification Procedures

NHERI sites are expected to notify the DesignSafe CSO via email within 24 hours of detecting or suspecting an incident, as well as following their campus procedures for incident notification and response. Upon notification of a possible security incident, the DesignSafe CSO will lead a formal incident response. The DesignSafe Security Working Group will be informed that a response is being initiated, and the response team will be formed based upon the extent of the incident. It may be necessary to quickly suspend the suspected user account(s), services, or systems to prevent an escalation of the incident. The team will analyze all available information, interrogate any persons involved, determine corrective measures, and assure corrections are implemented and effective prior to allowing any accounts, services, or systems to be brought back online. An incident report will be generated and shared with the Security Working Group. Relevant information from the report will be shared with the Site Management Team and NSF as appropriate.

10. Non-Compliance and Exceptions

If any of the minimum standards contained within this document cannot be met on systems, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office, along with a plan for risk assessment and management.

11. Protected/Personally Identifiable Information

Primary data at NHERI sites should consist of technical information regarding experiments conducted at NHERI facilities, simulation output, source code, and reconnaissance data. It is expected that no site has data that would qualify under NIST standards as “Controlled Unclassified Information” (CUI), including but not limited to Protected Health Information (PHI), student records, financial information, and so on. If any CUI data is on NHERI-affiliated computing systems, the site administrators should contact the DesignSafe security officer to develop a more comprehensive security plan which complies with appropriate controls as set out in NIST 800.171 and NIST 800.53.

12. Related Institutional Policies and Procedures

UC San Diego documents, rules, and procedures

http://adminrecords.ucsd.edu/PPM/docs/135-3.HTML

UC San Diego Minimum Password Standards

https://blink.ucsd.edu/_files/technology-tab/network/password-standards.pdf