DesignSafe CyberSecurity Plan

1. Overview

DesignSafe is an open CI that enables and supports leading-edge scientific discovery and promotes science and technology education. While it must be a widely accessible platform, a balanced approach to cybersecurity is required to support the confidentiality and integrity of the CI by architecting for security best practices, employing risk-based methodologies, and establishing a common project-wide approach to meet the needs of all NHERI awardees. As the NHERI-CI lead, we will establish and implement the NHERI-wide cybersecurity policy and procedure. Led by the DesignSafe Chief Security Officer (CSO) we will:

- Convene a Security Working Group comprised of members from each NHERI awardee, and establish incident response protocols including coordinating with the 24/7/365 operations center at the Texas Advanced Computing Center (TACC) at UT-Austin;
- Develop NHERI-wide cybersecurity policy and procedures for all awardees;
- Conduct an annual cybersecurity audit and provide an audit report to Council and NSF;
- Attend and participate in an annual NSF-supported Cybersecurity Summit, such as those provided by the Center for Trustworthy Scientific Cyberinfrastructure of which TACC attends regularly;
- Collaborate with cybersecurity teams of other major CI projects (iPlant, XSEDE, OSG, etc.) to ensure continued best practices are employed, and for awareness of incidents on those other CI projects that could impact DesignSafe.

DesignSafe implements cybersecurity based upon the federal standards in the Federal Information Security Management Act (FISMA) in NIST Special Publication 800-53 Revision 4. DesignSafe's authentication will be federated with InCommon, providing users single sign-on convenience. The DesignSafe web portal is actively monitored using TACC's Bro Network Security Monitor intrusion detection system that protects all information systems in the TACC datacenter.

2. 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.

2.1 DesignSafe Management Team

Ultimately, overall responsibility for the success of the DesignSafe CI lies with the management team comprised of the DesignSafe PI/Project Director Ellen Rathje, co-PI's Clint Dawson, Jamie Padgett, Jean-Paul Pinelli, and Dan Stanzione, Deputy Project Director Tim Cockerill, Project Manager Natalie Henriques and Portal Lead Steve Mock. This management team will be assisted by the DesignSafe CSO in the matter of the cybersecurity program and its overall goals, objectives, and priorities in order to support the overall mission of DesignSafe. The senior management team is also responsible for ensuring that adequate resources are applied to the security program to ensure its success.

2.2 DesignSafe Chief Security Officer

The DesignSafe CSO Nathaniel Mendoza, 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.

2.3 Experimental Facility Sites

To ensure that proper security measures are taken at each Experimental Facility (EF) site, local site security is ultimately the responsibility of the EF site Principal Investigator. Each EF will identify a main point of contact to participate in the NHERI-wide Security Working Group, coordinate with the DesignSafe CSO for security audits, and be a member of the incident response team.

2.4 Security Working Group

The DesignSafe CSO is the leader of this working group, and members are the local site security points of contact from each of the other NHERI awardees – one each from the seven EF's, one from the RAPID facility, one from the SimCenter, and one from the NCO. Communications will be maintained via a monthly Zoom virtual meeting and via an email list. The annual security audits will be done virtually as well.

3. Authentication and Authorization

The plan for Authentication and Authorization is utilizes TACC's well-established and proven infrastructure for a secure CI environment.

3.1 Access Control

Identification, authentication, and authorization are controls that facilitate access to and protect DesignSafe resources and data. Access to non-public resources will be achieved by unique user credentials and will require authentication.

DesignSafe will assign a username and password for identification and authentication purposes to each individual that has a need to access DesignSafe resources. In all cases, only the minimum privileges necessary to complete required tasks are assigned to that individual. Privileges assigned to each individual will be reviewed on a periodic basis and modified or revoked upon a change in status within the DesignSafe community. All DesignSafe resources must use only encrypted authentication and authorization mechanisms unless otherwise authorized by the CSO.

3.2 Creating User Accounts

DesignSafe user accounts will be created as TACC user accounts, and users will be required to provide identification information that enables TACC user services personnel to ensure we are compliant with University of Texas, state, and federal laws and regulations per standard TACC user policies. We will also federate account creation with InCommon, such that users can link their InCommon identity with a TACC identity and use their local institution credentials.

3.3 User Credentials

DesignSafe will initially use single-factor authentication via a user password. Multi-factor authentication is being phased into TACC's authentication infrastructure, and if deemed necessary will be applied to the DesignSafe CI. For multi-factor authentication, users would have a password and in addition a second mechanism of a short-lived access code provided by a fob or via mobile device app. The use of group accounts for administrative purposes and shared passwords for those accounts will be minimized where technically feasible. DesignSafe staff requiring privileged user access will be using RSASecurID fobs for controlling root access to resources.

Credentials may be used only by the authorized user. Passwords or accounts should never be shared with anyone. Account owners will be held responsible for any actions performed using their accounts. DesignSafe staff will never ask users to disclose their passwords in any manner. Passwords should never be written down and left in plain sight, or stored in plain text online.

3.4 Inactive Account Expiration

DesignSafe accounts that are inactive for 120 days will be deactivated, and the user will need to request reactivation of the account.

4. Proactive Security Monitoring and Detection

The DesignSafe resources are protected within the TACC datacenter by a firewall and a Bro Intrusion Detection system that monitors 100% of the network traffic and can automatically block IP's. Further automated analysis and detection is accomplished by ingesting logs from all datacenter resources into TACC's Splunk Operational Intelligence system. TACC's 24/7/365 Operations staff receive notifications from these monitoring systems and can take corrective action and notify the CSO which initiates the formal incident response. Additionally, users can report an incident via the DesignSafe Help system that will also notify TACC's Operations staff.

All connections to the DesignSafe CI, for example from EF site servers, must be encrypted and all data transport is encrypted e.g. using SSH, HTTPS, etc.

5. Incident 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 will 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 DesignSafe Management Team and NSF as appropriate.

6. Audit

DesignSafe's comprehensive cybersecurity approach includes a security audit at each of the Experimental Facility (EF) sites performed once a year. The audits use security best practices to verify that each server-class system operating at an EF 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.

6.1 Schedule for audits

Each EF site 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 constituent – EF, RAPID, NCO, and SimCenter. The audits will generally be done once a year, and will be performed virtually. However, in the event that 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 EF site, such that the site operations are minimally affected and the resources of the site

IT staff are optimally utilized.

6.2 Actions following the audit

If there are audit findings, the DesignSafe CSO will recommend corrective actions for the EF site to implement. A formal report will be generated once a year that summarizes the results of the audits for each EF site. 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.