NEES@Buffalo Cybersecurity Plan

Introduction

The NEES Cyberinfrastructure (CI) system is composed of fourteen equipment sites and one central IT facility, henceforth referred to as NEEScomm IT. With IT resources (hardware and software) spread across the system and connected together with internet protocols over the public internet, computer security is of prime concern. As a leading Cyberinfrastructure project, NEES has developed a comprehensive cybersecurity approach that includes best practice cybersecurity policies and mechanisms at NEESCentral and an annual security audit at each of the NEES sites.

NEES@Buffalo is one of the fourteen equipment sites within NEES. As such we have built our plan to rely havily and comply with NEEScomm CyberSecurity Plan (CSP)

Roles and Responsibilities

NEES CI security is the responsibility of everyone who can affect the security of NEES CI systems. However, since the specific duties and responsibilities of various individuals and organizational entities vary considerably, certain key responsibilities should be made explicit for the sake of clear accountability.

Laboratory Executive Commitee (ExCom)

The Laboratory Executive Commitee is responsible for the day-to-day operations of the NEES@Buffalo equipment site, including the supporting computer systems. Their responsibilities include enforcing appropriate security controls such as management, operational, and technical controls that comply with NEEScomm's CSP.

Cyberinfrastructure Security Management

The NEES@Buffalo IT Manager acts as site CSO (currently identified as Goran Josipovic). NEES@Buffalo IT Manger is ultimately responsible for the security of a site's IT systems. He is responsible for implementing technical security on computer systems and for being familiar with security technology that relates to all laboratory systems. He is also required to ensure the continued operation of IT services to meet the needs of NEES researchers, as well as analyze technical vulnerabilities in the systems and their security implications.

Authentication and Authorization Policy

Controlled access to IT resources is essential for NEES@Buffalo to fulfill its mission. This policy describes our plan for Authentication and Authorization that can support current needs for electronic access and accommodate future services and technologies by employing standardized mechanisms for Identification, Authentication, and Authorization.

Objective

This policy is guided by the following objectives:

1. To ensure that NEES@Bufflao can, without limitation, operate and maintain its IT resources;
2. To ensure that NEES@Buffalo can, without limitation, protect the security and functionality of its IT resources and the data stored on those resources;
3. To protect NEES@Buffalo's other property, rights, and resources;
4. To preserve the integrity and reputation of NEES@Buffalo;
5. To safeguard the privacy, property, rights, and data of users of NEES@Buffalo IT;
6. To comply with applicable existing NSF regulations; and
7. To comply with existing University at Buffalo policies, standards, guidelines, and procedures.
8. To comply with existing NEEScomm policies, standards, guidelines and procedures.

Policy Statement

Access Control

Identification, Authentication, and Authorization are controls that facilitate access to and protect NEES@Buffalo IT resources and data. Access to non-public IT resources will be achieved by unique User Credentials and will require Authentication.

NEES@Buffalo will assign a username and password for Identification and Authentication purposes to each individual that has a business, research, or educational need to access NEES@Buffalo IT 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 NEES community.

All NEES@Buffalo IT resources must use only encrypted Authentication and Authorization mechanisms unless otherwise authorized by the CSO.

User Credentials Standard

In general NEES@Buffalo will maintain closed operations in that it will allow only users with approved NEES projects that utilize NEES@Buffalo resources to become registered users.

User Credentials Standard

The password will be used as the primary user credential, to be used along with the username. A password may be used only by the authorized user. Passwords or accounts should never be shared with anyone, including trusted friends or family members. Account owners will be held responsible for any actions performed using their accounts. NEES@Buffalo IT 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.

Passwords for NEES@Buffalo IT resources must comply with the following standards:

- Passwords must contain at least 1 letter.
- Passwords must contain at least 1 number or punctuation mark.
- Passwords must be at least 8 characters long.
- Passwords must contain more than 4 unique characters.
- Passwords must not contain easily guessed words (e.g. Buffalo, Bills, UB).
- Passwords must not contain your name or your username.
- New passwords must be different than the previous password (re-use of the same password will not be allowed for one (1) year).

The use of group accounts for administrative purposes and shared passwords for those accounts should be minimized where technically feasible. In situations where group accounts for administrative purposes and shared passwords for those accounts is required (e.g. “Root” or “Administrator” accounts), the passwords used must also follow the standards stated above.

Password Expiration

All NEES@Buffalo IT resource passwords must be changed at least every one hundred eighty (180) days. Any group password must be changed every one hundred eighty (180) days and immediately upon any personnel change within the group.

Privacy Policy

The right to privacy is a deeply held conviction, especially within intellectual and academic communities. Privacy is critical to the intellectual freedom that forms the foundation of higher

education. While the right to individual privacy is highly valued in the University community, it must, however, be balanced with legal obligations and the larger needs of the community.

Although NEES@Buffalo seeks to create, maintain, and protect the privacy of electronic information on its IT resources, users should be aware that the use of NEES@Buffalo IT resources is not completely private. Except as provided in this policy, NEES@Buffalo does not routinely monitor the content of communications or transmissions using IT resources. The normal operation and maintenance of the NEES@Buffalo IT resources require the back up and caching of data, the logging of activity, the monitoring of general usage patterns, and other such activities. There are also special circumstances such as illness; death; violation of NEES@Buffalo policies, regulations procedures or rules; or illegal activity which may warrant intrusive or restrictive action within an individual's computer account and/or devices.

Audit Policy for NEES@Buffalo and NEEScomm IT Resources

NEEScomm's comprehensive cybersecurity approach includes a security audit at each of the NEES sites performed once a year. The audits use security best practices to verify that each server-class system operating at a NEES 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 NEES@Buffalo and NEEScomm IT resources. No system can be perfectly secure, to be sure. But regular audits of the system provide vital information for the regular upkeep and secure maintenance of the server systems. This section outlines the policies that will govern the audits of the site resources.

NEES@Buffalo computer resources are also constantly being monitored by University at Buffalo IT services that flag any misuse or odd behavior of all and any workstations and servers within NEES@Buffalo.

Objective

The objective of this policy section is to enable security audits with minimal impedance to the activities at NEES@Buffalo site and make the best possible use of the time and resources of IT personnel at the site and at NEEScomm. It also lays out certain minimal requirements for the security audit as well as preferred practices that go above and beyond the minimal

requirements. Yet another objective is to lay out the goals and the expected follow-on activities from a security audit.

Policy Statement

Schedule for the audit scans

NEES@Buffalo together with the NEEScomm CSO, or his designee, will work together to determine an appropriate time schedule for performing the audit. The audits will generally be done once a year. However, in the event that a security incident is suspected to have occurred or is anticipated, say due to the release of a dangerous malware that affects the IT systems at the site, then further audits will be done. In all cases, the timing for the audit will be decided in consultation with NEES@Buffalo, such that the site operations are minimally affected and the resources of the site IT staff are optimally utilized.

Running the audit scans

The set of scan software that will be a part of the audit will be provided by NEEScomm IT. Suite of audit software will be used, with one necessary requirement being that each software be actively maintained with updates to the vulnerability signatures. The entire audit will consist of multiple scans, each using a different software package. NEEScomm will seek to perform the scans at different layers of the software stack, from the network to the application level.

It is desirable that the audits be done in a manner that is as automated as possible. For this NEEScomm will generate, as far as practicable, scripts to run the audit scans automatically, collect the results, and perform a first-pass automated analysis of the scan results to identify any security vulnerabilities. The scan will be done in two modes -one where the source is a machine within the university that the site is a part of (to mimic attackers from inside the university) and the second where the source is from the general internet outside the university (to mimic external attackers). It is expected that for such technical reasons as well as operational reasons, the execution of the audit scans will be done with the participation of the SIM. The parties will determine which machines will be a part of the scan. This will be derived from the inventory of the site IT assets that will be done at the beginning of each project year. All the IT assets that are related to NEES activities, including, but not restricted to the following will be a part of the security audit ? local data repositories, and machines operated by the NEES network and used to access NEEScomm IT data and NEEScomm IT services.

Actions following the audit scans

Each piece of scan software automatically generates reports of what it found in the target systems and usually, classifies each observation in terms of severity. These reports will serve as the starting point for a more targeted and manual analysis of the report by the NEEScomm IT security staff. The objective of this is to identify vulnerabilities that are very difficult to be covered by any automated analysis script due to the evolving nature of the computer security threats. A second practical objective of the manual analysis is to remove incidences of false positives that have been observed in the automatically generated reports. Such false positives arise because it is difficult to document all the configuration details of the IT systems that affect the results of the security scans; even if a configuration detail is documented, it is often present in a form (such as, free text without any standardized structure) that cannot be parsed easily by the automated scan tools. If this manual analysis finds any vulnerability or evidence of a security breach, NEES@Buffalo will be immediately contacted and an incident report initiated.

A formal report will be generated once a year that summarizes the results of the audits for each 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. The report will be seen only by NEEScomm members, site IT members, and NSF.

Low intensity periodic scans

In addition to the annual audits by NEEScomm. NEES@Buffalo is also audited by University at Buffalo IT services that does continuous varying intensity audit scans. The goal of these periodic scans is to identify vulnerabilities as they come up and NEES@Buffalo is contacted immediately if such vulnerabilities do come up.

Conclusion

In this document, we have outlined the NEES@Buffalo Cyber Security plan that relies heavily and derives from NEES Cyberinfrastructure (NEES CI) security plan. This plan delineates the responsibilities, roles, and expected behavior of all individuals who access NEES@Buffalo IT services and the policies governing the security controls that will be used to minimize the risks of cybersecurity incidents. All site IT personnel should become familiar with this document. The security plan will be reviewed and updated at least annually, and further on an as-needed basis, to reflect enhancements to the NEES@Buffalo and NEEScomm IT services and to react to new security threats from the ever-changing computer security field.