NEEA Website Security Policy

1. Overview

With the constantly changing and ever-increasing number of cyber-attacks targeting websites, it is imperative that NEEA takes steps to prevent and mitigate these risks.

2. Purpose

To define a set of requirements and guidelines to ensure our websites are safe and secure to preserve their integrity, availability, confidentiality, and authenticity.

3. Scope

Employees

When a program, product, brand, campaign, et al requires any type of *external facing* website, employees must adhere to these policies and consult with IT (in consultation with the Contracts Team) for guidance throughout the process of planning, developing, launching, updating, and maintaining said website.

Contractors

Companies or individuals, either contracted by NEEA or sub-contracted by NEEA contractors, to develop, design, maintain, or host our websites, must adhere to these policies.

Documentation

This website security policy will refer to related procedures, guidelines, and documentation which may be made available upon request.

4. Website Security Policies

Web Hosting Requirements

Web Hosting Providers, or Managed Service Providers for web hosting platforms, must provide to NEEA a security brief outlining the steps that are being taken to secure NEEA websites.

- Websites should be hosted on servers within the NEEA-owned Amazon Web Services (AWS) account
- Operating systems, applications, and plug-ins must be kept up to date with critical vulnerability patches
- Firewall rules must be set to only allow the necessary inbound and outbound traffic to and from trusted sources

- Websites must use HTTPS and any web requests to port 80 must redirect to port 443
- Web servers must follow best practices for Transport Layer Security (TLS) implementations
- All web servers must be monitored for uptime and performance by web hosting providers
- All web servers and database servers must be backed up daily with monthly retention
- Server vulnerability scans must be completed, at minimum, on an annual basis
- Real-time anti-virus and intrusion detection should be utilized on web servers
- Server logs must be retained for a period of one year

Web Development Requirements

Developers must provide a security brief outlining the steps taken to secure NEEA websites. NEEA may also request to review the developer's own internal security policies and procedures.

- Development environments may be hosted by developers so long as they are password protected
- Websites should have a test environment within NEEA's AWS account to be used for staging code deployments before pushing to production
- Content Management Systems and any installed plug-ins must be kept up to date with critical vulnerability patches
- All code must be maintained with version control in NEEA-owned code repositories
- All websites must be monitored for uptime and performance by developers
- All web forms must use reCAPTCHA, and should use additional CMS plug-in spam filtering
- Email generated from websites should use Amazon's Simple Email Service

NEEA IT Department Requirements

- NEEA must own all products and services related to websites (i.e., domain names, security certificates, software licenses, code repositories, and web hosting accounts), even when said products and services are managed on our behalf by contractors
- NEEA must have administrative access to all systems and services managed by contractors
- NEEA will manage all domain names and related Domain Name System (DNS) records
- NEEA will monitor the status of websites including, but not limited to, website uptime, website performance, domain name registrations, and SSL certificate expirations and security scores
- NEEA will develop and maintain an incident response plan for all websites
- NEEA will maintain an inventory of all website assets to be documented and kept up to date with yearly audits
- NEEA will run front-end website security scans quarterly
- NEEA will work with service providers to rotate AWS Identity and Access Management (IAM) access keys yearly
- NEEA will perform an annual audit of and document user accounts for server level access, CMS access, and code repository access

5. Compliance

Documentation and Records

- NEEA will maintain documentation and records of all the above
- NEEA, or a third-party, may audit all the above for compliance with this policy
- NEEA may request additional or updated information from contractors as needed
- NEEA may update, modify, or revise this document including all policies, procedures, or requirements therein and will notify contractors of any such changes

Exceptions

Any exceptions to these policies must receive written approval from NEEA's Senior Manager of Information Technology