Cyber Security Awareness Assessment Policy

Purpose

This policy establishes guidelines and procedures for conducting Cyber Security Awareness Assessments to evaluate and enhance employees' awareness of cyber threats and best practices. It aims to ensure that all employees, contractors, agency partners, and third-party individuals are well-informed and capable of safeguarding CONFIRE's assets from potential cyber threats.

Scope

This policy applies to all employees, contractors, agency partners, and third-party individuals with access to CONFIRE information systems and data.

Cyber Security Awareness Assessment Process:

a. **Frequency:** Cyber Security Awareness Assessments will be conducted monthly and quarterly instructional email and test. Additional assessments may be scheduled in response to significant security incidents or changes in the threat landscape.

b. **Assessment Components:** The assessment will cover phishing, social engineering, password management, data handling, and general cybersecurity best practices. The assessment may include simulated phishing attacks, quizzes, and interactive training modules.

c. **Simulated Phishing Attacks:** Simulated phishing attacks will be periodically conducted to evaluate employees' ability to recognize and report phishing attempts. - Results of simulated phishing exercises will be used for individual training and organizational awareness improvement.

d. **Training Modules:** Cybersecurity training modules covering essential topics will be provided to employees. (Completion of training modules will be mandatory for all employees).

Reporting and Analysis:

a. **Individual Results:** Individual assessment results will be confidentially shared with each employee. (Employees who perform exceptionally well may be recognized).

b. **Organizational Analysis:** Aggregated results will be analyzed to identify common weaknesses and areas for improvement. (The analysis will inform the development of targeted awareness campaigns and training initiatives).

Remediation:

a. **Individual Training Plans:** Employees who demonstrate weaknesses in specific areas will be required to undergo targeted training. (Training plans will be developed based on individual assessment results).

b. **Continuous Improvement:** CONFIRE MIS will regularly review and update the Cyber Security Awareness Assessment Policy to adapt to evolving threats and technologies.

c. **Enforcement:** Each agency partner is responsible for determining remedial actions and disciplinary measures based on their policies.

d. **Non-Compliance:** Failure to participate in or complete mandatory cybersecurity awareness assessments may result in disciplinary action, up to and including termination, depending on the severity and frequency of non-compliance.

e. Each agency partner maintains final authority regarding personnel decisions and will adhere to their policy.

Policy Details:

a. **Frequency of Meetings:** Periodic meetings will be scheduled between CONFIRE MIS and CONFIRE Division leads and agency partners to review Cyber Security Awareness performance. The frequency of these meetings shall be determined based on division and agency partner needs and priorities.

b. **Evaluation Process:** During these meetings, the overall performance of Cyber Security Awareness within each division and agency partner will be assessed. This evaluation will include an analysis of user engagement levels, feedback mechanisms, and any emerging trends or challenges related to cyber security awareness.

c. **Feedback Gathering:** Division leads, and agency partners will be able to provide feedback on current Cyber Security Awareness initiatives, including successes, areas for improvement, and specific challenges their respective teams face.

d. **Guidance and Advisement:** CONFIRE MIS will guide and advise division leads and agency partners on strategies to increase user engagement and awareness regarding cyber security. This may include recommendations for tailored training programs, awareness campaigns, or technological solutions to address identified gaps.

e. **Reporting:** CONFIRE Division leads, and agency partners will receive monthly reports on Cyber Security Awareness performance from CONFIRE MIS.

Policy Implementation:

This policy shall be implemented immediately upon approval by the CONFIRE Administrative Committee. MIS will coordinate and facilitate the periodic meetings outlined in this policy, in consultation with CONFIRE Division leads and participating agency partners.

a. **Review and Approval:** This policy shall be periodically reviewed and evaluated to ensure its effectiveness and relevance to CONFIRE needs. Any necessary revisions or updates will be made in consultation with CONFIRE MIS leadership and relevant stakeholders and communicated to all CONFIRE personnel and agency partners.

b. **Enforcement:** CONFIRE MIS is responsible for enforcing compliance with this policy, which is mandatory for all CONFIRE employees and agency partners.