LECO Security Awareness Web Application

Acceptable Use Policy

Effective Date: 25.09.2024

1. Introduction

   The Security Awareness Web Application is designed to provide training, resources, and tools to ensure employees of Lanka Electricity Company (LECO) are aware of and adhere to security protocols. This policy outlines acceptable use practices for all users of the application to ensure it is used responsibly and securely.

   The LECO Security Awareness Web Application is an innovative tool created specifically to improve LECO's IT department's security awareness, training and education. The threat of cyber-attacks is constantly changing in today's digital environment; therefore it is essential for businesses like LECO to provide their employees with proactive training. By offering dynamic training modules covering important cyber security subjects, such as password management, incident response, social engineering, and phishing, this program offers a comprehensive solution.

   Furthermore, the platform provides staff with real-time policy updates so they are aware of the most recent security procedures, regulatory modifications, and compliance standards. This capacity guarantees that every team member continuously complies with business policies and fortifies LECO's defense against new cyber threats. The function that measures policy acknowledgements, employee training attendance, and adherence levels produces informative reports. This supports an ongoing culture of security practice improvement by assisting management in identifying possible knowledge gaps and taking appropriate corrective action.

   This Acceptable Use Policy (AUP) is ultimately intended to safeguard sensitive data and systems, encourage responsible application use, and support cyber security best practices in order to protect LECO and its personnel. Employees that utilize the platform in accordance

with its intended purpose help to establish a safe, dependable workplace where cyber hazards are successfully controlled and reduced.

2. Applicability

The following users of the Security Awareness Web Application are subject to this AUP:

- Registered employees of LECO IT Department

3. Prohibited Activities
   - Users must not try to disable or bypass the application's security measures.
   - It is completely forbidden to misuse the platform by trying to gain unauthorized access to administrative services, disclosing confidential material, or fabricating training records.
   - It is not permitted to use the application for activities that are not related to work or that go against business policies.

4. User Responsibilities

4.1 Access Control

- Users must log in using their unique credentials (employee ID and password).
- Users are responsible for maintaining the confidentiality of their login information and must not share their credentials with anyone.

4.2 Account Security

- A minimum of eight characters, comprising capital, lowercase, numeric, and special characters, should be included in passwords to comply with security criteria.
- The training platform password should not be the same as any other system password.
- Change your password immediately if you suspect unauthorized access to your account.

4.3 Training Modules

- Users must complete all assigned cyber security training modules in a timely manner.

- Each module goes over important security topics like phishing, managing passwords, and responding to security incidents. There may be quizzes and tasks based on situations in these modules.
- Users need to make sure they fully understand the information and do the quizzes.

4.4 Progress Tracking

- Users can view their training progress via the dashboard.

4.5 Phishing and Social Engineering

- Be cautious of fraudulent attempts. Inform the IT department of any suspicious emails or messages that are encountered during or outside of training.
- In order to safeguard both yourself and the organization, adhere to the instructions outlined in the phishing training modules.

4.6 Compliance

- Users must comply with all security policies, including data protection laws, physical security guidelines, and the organization's information security policies.
- Non-compliance may result in disciplinary action as per company policies.

5. Enforcement

LECO reserves the right to:

- The application will monitor user activities to ensure compliance with the AUP.
- Automated alerts will notify users of policy updates.
- Violations of this AUP may result in loss of access to the application or disciplinary actions based on company guidelines.

6. Reporting Violations

- Please notify Administrator of this training platform immediately if you suspect any violations of this Acceptable Use Policy. Disciplinary action or the loss of application access may be the consequence of violations.

7. Amendments

   This Acceptable Use Policy may be revised periodically to accommodate modifications in company policies or security protocols. Users will be informed of any significant updates or modifications to the policy.

8. Contact Information

   For any questions or concerns regarding this Acceptable Use Policy, please contact the following group:

   - Group ID: IE3072_24_011
   - Members:
     1. Piyarathna R.S. (IT22558114)
     2. Jayasekera H.D. (IT22000958)
     3. Ranwala R.M.C.D. (IT22604408)
     4. Thilakarathna S.T.D. (IT22578914)
     5. Siriwardhane H.H.D.V. (IT22291646)