**Cybersecurity Awareness Training Policy**

Last Updated: 11/28/2023

**1. Purpose**

This Cybersecurity Awareness Training Policy outlines the requirements and expectations for all employees to undergo regular cybersecurity awareness training at our company. The objective is to enhance the overall security posture of the organization and empower employees to recognize and respond to cybersecurity threats effectively.

**2. Training Program Overview**

**a. Frequency**

* All employees are required to complete cybersecurity awareness training annually.
* New employees must complete the training within the first 6 months of their employment.

**b. Training Content**

* The training program covers essential topics, including but not limited to:
  + Password security and management.
  + Phishing and social engineering awareness.
  + Safe internet and email usage.
  + Mobile device security.
  + Data protection and confidentiality.
  + Physical security measures.
  + Reporting security incidents.

**c. Training Delivery**

* The cybersecurity awareness training will be delivered through ESET [https://www.eset.com/us/business/cybertraining], which employees can access remotely or during designated training sessions.

**3. Employee Responsibilities**

**a. Mandatory Participation**

* Participation in the cybersecurity awareness training program is mandatory for all employees.
* Failure to complete the training within the specified timeframe may result in disciplinary action.

**b. Reporting Suspicious Activities**

* Employees are encouraged to report any suspicious activities or potential security threats promptly to the IT department.

**c. Continuous Learning**

* Employees should actively engage in continuous learning opportunities related to cybersecurity through additional resources provided by the company.

**4. IT Department Support**

**a. Assistance**

* The IT department is available to provide assistance and answer questions related to the cybersecurity awareness training program.

**b. Reporting Incidents**

* The IT department is responsible for receiving and responding to reports of potential security incidents submitted by employees.

**5. Compliance**

* Adherence to this policy is mandatory for all employees.
* Violations of this policy may result in disciplinary action, up to and including termination of employment.

**6. Review and Updates**

* This Cybersecurity Awareness Training Policy is subject to periodic review and updates.
* Employees will be notified of any changes to the policy.

**7. Contact Information**

If you have questions or concerns regarding the cybersecurity awareness training program, please contact the IT department at [ITSupport@email.com](mailto:ITSupport@email.com).

By accepting employment at [Company Name], employees agree to comply with the terms outlined in this policy.

[Company Name]  
[Company Address]  
[San Antonio, TX. 78216]  
[[contact@email.com](mailto:contact@email.com)]