**SECURITY AWARENESS AND TRAINING POLICY**

**PURPOSE:**

The Security Awareness and Training Policy for the company serve to educate and empower employees, contractors, and stakeholders in understanding and implementing effective security measures. By providing clear guidelines and training programs, the policy aims to enhance awareness and knowledge regarding cybersecurity threats, thereby reducing the risk of security breaches. Ultimately, the policy aims to create a culture of security consciousness throughout the organization, ensuring the protection of sensitive data and assets from potential threats.

**SCOPE:**

The Scope of our Security Awareness and Training Policy encompasses all employees, contractors, and stakeholders within the company. It aims to install a comprehensive understanding of cybersecurity threats and best practices, fostering a culture of vigilance and responsibility across the organization. This policy is applicable to all levels and departments, ensuring a unified and proactive approach to security awareness.

**AUTHORITY, RESPONSIBILITY AND DUTIES:**

Chief Information Security Officer (CISO) or Security Manager

**RESPONSIBILITY:**

* Develop and enforce security policies and procedures.
* Oversee the implementation of security awareness and training programs.
* Ensure compliance with industry regulations and standards.

**DUTIES:**

* Design and update the security awareness and training policy.
* Allocate resources and budget for security training programs.
* Identify and assess potential security risks.
* Establish metrics to measure the effectiveness of security awareness initiatives.

**Human Resources (HR) Department:**

**RESPONSIBILITY:**

* Support the implementation of security awareness programs.
* Collaborate with the security team to integrate training into onboarding processes.
* Manage employee awareness campaigns.

**DUTIES:**

* Incorporate security training modules into the employee onboarding process.
* Track employee participation in security training.
* Coordinate with department heads to ensure employees receive relevant and timely security information.
* Manage communication channels for security-related announcements.

**IT Department:**

**RESPONSIBILTY:**

* Implement technical aspects of security training (e.g., simulated phishing exercises).
* Ensure that employees are trained on the use of security tools and technologies.

**DUTIES:**

* Deploy and manage security training platforms and tools.
* Conduct simulated phishing campaigns and assess results.
* Collaborate with the security team to address technical vulnerabilities identified during training exercises.

**Department Heads/Managers:**

**RESPONSIBILITY:**

* Enforce security policies within their respective departments.
* Encourage and monitor employee participation in security training.

**DUTIES:**

* Emphasize the importance of security awareness to their teams.
* Collaborate with HR and the security team to address specific departmental training needs.

**Employees:**

**RESPONSIBILITY:**

* Participate actively in security awareness and training programs.
* Report security incidents promptly.

**DUTIES:**

* Attend and complete required security training modules.
* Stay informed about security best practices.
* Report any security incidents or concerns to the appropriate channels.

**ENFORCEMENT:**

* Employees violating this policy may face disciplinary action, including termination, and may incur civil or criminal penalties.
* Vendors, consultants, or contractors in violation may face sanctions, including the removal of access rights, termination of contract(s), and potential civil or criminal penalties.