Chameleon
Security

Security Awareness and Training Policy

1. Introduction

1.1 Overview

This security awareness and training policy outlines the guidelines and procedures that all employees in the Chameleon company must follow. This policy will ensure that our employees and company's information and resources are safely maintained and used. Since it is essential for all the employees to aware of potential security threats and risks related to cyber attacks and to manage a secure environment, the employees must follow this policy and ensure the confidentiality of our organization.

1.2 Purpose

The primary purpose of this document is to foster a culture of security awareness within Chameleon Company and ensure that all employees are aware of their responsibility in protecting confidential information. Security awareness training will enable employees to identify security threats, protect sensitive information, and enhance security awareness among all employees and stakeholders.

1.3 Scope

This policy applies to all employees, independent contractors, and third-party personnel who have access to the company's information systems and data. All individuals covered by this policy must undergo security awareness training as outlined in the ISO 27001 standard and related controls. Non-compliance with this policy may result in corrective actions as part of the organization's Information Security Management System (ISMS).

2. General Policy Statement

<u>This policy is applicable to all departments and users of IT resources and assets.</u>

1. All the employees under any department in Chameleon Company is committed to take security awareness training prior to using any system, when required by information system changes and annually thereafter.
2. The training will cover these topics.
    - Secure handling of sensitive information
    - Responsibility in handling company data
    - Email and Internet habits
    - Data protection regulations and compliance requirements
    - Phishing
    - Social media awareness
    - Social engineering awareness
    - Incident response and reporting procedures.
    - Practices for working remotely.
3. The training will encompass a range of security measures, including physical, personnel, and technical safeguards, to provide individuals with the necessary knowledge and skills to carry out their responsibilities and support the organization's information security

program. Contractors will also undergo role-specific security training to ensure their compliance with the organization's security standards.

4. All the employees must follow safety reporting procedures when they encounter any incidents or suspicious activities either inside or outside attacks. These reports will be the sources in improving the company safety practices.
5. Continuous monitoring, assessment, and improvement of security awareness training programs will be conducted to ensure alignment with industry standards, regulatory requirements, and organizational objectives.

3. Authority, Roles and Responsibilities

3.1 Management

The management team is responsible for

- Providing necessary resources for the training.
- Ensuring each and every employee has completed the security awareness training.
- Actively engage with employees and set clear expectations regarding information security responsibilities and communicate according to their level of expertise, roles and responsibilities.
- Monitoring and recording all employees training process and retained for a period as defined in company retention policy.

3.2 Information Security Officer

- Develop, implement and evaluate the security awareness training and maintain records of training for entire program in accordance with ISO 27001 requirements.
- Coordinates, monitors and tracks the completion of the Security Awareness Training.
- Ensure updated training contents according to the changes in systems.

3.3 Employees

- New starters are required to start taking training within a short period of time.
- All employees must complete security awareness training monthly or every time changes in systems happen.
- Employees must agree and understand security policies and procedures and report any incidents promptly.
- Employees are required to adhere to this policy and reduce the risks of security in the workplace.

4. Training Policy

4.1 Training Approaches

- Firstly, new employees will be given a questionnaire that tests their current knowledge regarding information security.

- Employees will receive cloud based security training modules that include materials based on the knowledge and roles of employees within the organization to ensure understanding and relevance.

4.2 Training Process

- All employees are required to complete the training upon hire and maximum within 15 working days.
- Training courses and interactive workshops will be launched or emailed to all employees monthly.
- System changes shall alert employees to take training upon using it.
- Continuous training with up-to-date contents of security awareness principles is essential.

5. Compliance

Compliance with this policy is mandatory for all employees, and non-compliance may result in disciplinary actions in accordance with the organization's disciplinary procedures.

6. Evaluation and Revision

This Security Awareness and Training Policy will be reviewed regularly to ensure its alignment with ISO 27001 standards, industry best practices, and organizational objectives.

Updates to the policy will be communicated to employees, and training materials will be revised accordingly to address evolving information security threats and requirements.