RAZOR SHARP
CONSULTING

INFORMATION SECURITY AWARENESS PROGRAM

January 1, 2023

Abstract

The information security awareness program establishes a set of security guidelines and expectations for all employees to ensure a safe and protected work environment.

Mike Cottingham
mcottingham@razorsharpconsulting.com

Table of Contents

Revision History

Date	Revised By	Comment
January 1, 2023 (v1.0)	Mike Cottingham	Initial Document
June 22, 2023 (v1.1)	Mike Cottingham	Formatting

Introduction

At Razor Sharp Consulting, we prioritize the protection of sensitive information, both for our clients and our company. Information security is a collective responsibility, and every employee plays a crucial role in safeguarding our data assets. To ensure that all employees are equipped with the knowledge and skills necessary to maintain a secure environment, we have developed an Information Security Awareness Program. This program aims to raise awareness, promote best practices, and cultivate a culture of information security throughout the organization.

Program Objectives

Promote Understanding

The primary objective of our Information Security Awareness Program is to enhance employees' understanding of the importance of information security and the potential risks associated with data breaches and cyber threats. By fostering awareness, we aim to empower employees to make informed decisions and take appropriate actions to protect sensitive information.

Establish Best Practices

The program seeks to establish a set of best practices and guidelines for information security. These practices will cover areas such as password management, data classification, access control, phishing awareness, and safe internet browsing. By following these practices consistently, we can minimize the risk of security incidents and protect our data assets effectively.

Encourage Vigilance

Our program aims to cultivate a culture of vigilance among employees. This involves encouraging individuals to actively identify and report potential security threats, such as suspicious emails, unauthorized access attempts, or unusual system behaviors. By remaining vigilant and reporting incidents promptly, we can respond quickly and mitigate potential risks.

Compliance with Policies and Regulations

The program emphasizes compliance with relevant policies, procedures, and legal requirements related to information security. This includes adhering to our internal security policies, as well as external regulations, such as data protection and privacy laws. By ensuring compliance, we demonstrate our commitment to protecting confidential information and maintaining the trust of our clients and partners.

Program Components

Training Sessions

Regular training sessions will be conducted to educate employees on information security best practices, emerging threats, and company policies. These sessions will cover topics such as password hygiene, social engineering, phishing awareness, data handling, and incident reporting. We will provide interactive and engaging materials to enhance learning and retention.

Policy and Procedure Documentation

Comprehensive documentation will be provided to employees, outlining our information security policies, procedures, and guidelines. This documentation will serve as a reference for employees to understand their responsibilities and the actions they need to take to ensure information security.

Awareness Campaigns

We will launch awareness campaigns through various channels, such as email newsletters, intranet articles, posters, and digital signage. These campaigns will highlight current threats, promote best practices, and reinforce the importance of information security. Regular updates and reminders will be shared to keep information security top of mind for all employees.

Simulated Phishing Exercises

Periodic simulated phishing exercises will be conducted to test employees' ability to identify and respond to phishing attempts. These exercises will help raise awareness about the techniques used by attackers and provide targeted training to individuals who may require additional support.

Incident Reporting and Response

We will establish a clear process for reporting and responding to information security incidents. Employees will be educated on how to report incidents promptly and accurately, ensuring that the appropriate actions are taken to contain and mitigate any potential breaches.

Conclusion

Our Information Security Awareness Program aims to create a culture of information security within Razor Sharp Consulting. By promoting understanding, establishing best practices, and encouraging vigilance, we can collectively protect our valuable data assets. Through ongoing training, communication, and reinforcement, we will foster a strong and proactive approach to information security, ensuring the confidentiality, integrity, and availability of our information resources.

Remember, information security is everyone's responsibility. Let's work together to safeguard our data and maintain the trust of our clients and partners.