CHAMELEON

FOR OUR SMARTER WORLD

Security Awareness Policy

Security Awareness Policy

Protecting Our Company's Information Assets

1. Introduction

In today's increasingly interconnected world, information security has become paramount for every organization. Cyber threats, such as phishing, malware, ransomware, and social engineering tactics, are constantly evolving and pose significant risks to companies' data and reputation. It is crucial for all employees to be aware of these threats and take proactive measures to safeguard our company's sensitive information assets. This Security Awareness Policy outlines the company's expectations for employee behaviour and provides comprehensive guidance on how to remain vigilant and protect our data in the digital realm.

2. Purpose

The overarching purpose of this policy is to:

- Enhance awareness of prevalent cybersecurity threats
- Equip employees with the knowledge and skills to protect company information assets
- Proactively reduce the likelihood of cybersecurity incidents
- Ensure compliance with ISO 27001 information security standards

3. Scope

This policy encompasses all employees, contractors, and any individuals who have access to company information assets.

4. Policy Statement

The company is steadfastly committed to safeguarding its information assets from unauthorized access, use, disclosure, disruption, modification, or destruction. Every employee bears the responsibility to protect company information assets and adhere to this policy.

5. Policy Requirements

All employees must:

a. Be Aware of Cybersecurity Threats

- Familiarize themselves with common cybersecurity threats, including phishing, malware, ransomware, and social engineering tactics
- Understand the potential risks associated with these threats
- Develop the ability to identify and promptly report suspicious activity

b. Protect Company Passwords

- Craft strong and unique passwords for all company accounts
- Refrain from sharing passwords with anyone, even colleagues
- Regularly change passwords to maintain security
- Never store passwords in unencrypted formats, such as plain text documents

c. Exercise Caution When Clicking on Links

- Refrain from clicking on links or opening attachments from unknown senders
- Approach emails with caution, especially those containing urgent requests or enticing rewards
- Before clicking, hover over links to preview the actual destination URL

d. Safeguard Company Devices

- Abstain from installing unauthorized software on company devices
- Maintain company devices up-to-date with the latest security patches
- Never leave company devices unattended or accessible to unauthorized individuals

e. Report Cybersecurity Incidents

- In the event of suspected cybersecurity incidents, promptly report them to the IT department without delay

6. Consequences of Non-Compliance

Failure to adhere to this policy may result in disciplinary action, potentially leading to termination of employment.

7. Training and Awareness

The company will provide comprehensive cybersecurity training to all employees annually. Additionally, ongoing communication and awareness campaigns will be implemented to keep employees informed about the latest cybersecurity threats and emerging trends.

8. Review and Revision

This policy will be thoroughly reviewed and revised annually or as needed to adapt to changes in the company's information security landscape.

9. ISO 27001 Alignment

This policy aligns with ISO 27001, the internationally recognized standard for information security management systems. ISO 27001 provides a structured framework for organizations to identify, assess, and effectively manage information security risks.

10. Conclusion

Cybersecurity is a collective responsibility that requires the concerted efforts of all employees. By following the guidelines outlined in this policy, we can collectively protect our company's information assets, safeguard our data, and maintain our reputation as a secure and trustworthy organization.