IFIN GLOBAL

Security Awareness Training Policy

1. Purpose

The purpose of this Security Awareness Training Policy is to provide a framework for educating employees about the importance of information security, the threats facing the organization, and the best practices for protecting sensitive information and systems. This policy is designed to reduce the risk of security breaches caused by human error or negligence.

2. Scope

This policy applies to all employees, contractors, and temporary staff who have access to company information systems and data. It covers training on both technical and non-technical aspects of security awareness.

3. Policy Statement

[Company Name] is committed to ensuring that all employees receive security awareness training that is both timely and relevant to the security needs of the organization. Employees are expected to understand and comply with security policies, recognize common security threats, and be proactive in safeguarding the organization's information resources.

4. Responsibilities

- **IT Security Team**:
  - Design, develop, and implement security awareness training programs.
  - Maintain training materials and ensure they are up to date with the latest security threats and best practices.
  - Conduct periodic risk assessments to identify training needs.
- **Employees**:
  - Actively participate in all mandatory security awareness training sessions.
  - Follow the security policies, procedures, and practices outlined during training.
  - Report any suspicious activities or security incidents immediately.
- **Managers**:
  - Ensure that their team members complete training as required.
  - Reinforce the importance of security awareness within their teams.
  - Monitor compliance with training and address any issues.

5. Training Requirements

- **Frequency**:
  - All employees must complete an initial security awareness training session during onboarding.

    - Employees must participate in annual refresher courses to stay current on emerging security threats and policies.
    - Additional training may be required based on specific roles, such as those involving access to sensitive or classified data.

- **Content**: The training will cover, but is not limited to, the following topics:
    - **Data Protection and Privacy**: Guidelines on handling sensitive information and personal data.
    - **Phishing and Social Engineering**: How to recognize and respond to phishing emails and other social engineering tactics.
    - **Password Management**: Best practices for creating strong passwords and securing accounts.
    - **Physical Security**: Protecting devices and physical access to secure areas.
    - **Incident Reporting**: How to report security incidents or suspicious activities.
    - **Mobile Device and Remote Work Security**: Guidelines for securing mobile devices, laptops, and remote work setups.
    - **Compliance**: Understanding legal and regulatory requirements related to information security.

6. Evaluation and Monitoring

- **Knowledge Assessments**: Periodic quizzes and assessments will be conducted to evaluate employee understanding of security principles and the effectiveness of the training.
- **Compliance Tracking**: Completion of security awareness training will be tracked in the company's learning management system (LMS). Employees must achieve a minimum score to pass the training.
- **Incident Analysis**: Security incidents will be analyzed to determine if insufficient training contributed to the event. If training gaps are identified, additional or revised training will be implemented.

7. Consequences of Non-Compliance

Failure to complete security awareness training or follow security protocols can result in disciplinary action, up to and including termination of employment. The consequences may vary depending on the severity of the infraction and whether the employee's actions were intentional or due to negligence.

8. Policy Review and Updates

This policy will be reviewed annually or whenever there are significant changes to security threats, legal requirements, or organizational structure. Updates to the policy will be communicated to all employees.

9. Acknowledgment

All employees must sign an acknowledgment form to confirm that they have read, understood, and agreed to comply with the Security Awareness Training Policy.

Conclusion

This policy is crucial to fostering a security-conscious culture and ensuring the safety of the organization's information and assets. By regularly educating employees about security threats and practices ,IFINGLOBAL GROUP aims to mitigate risks and ensure compliance with legal and regulatory requirements