

Information Security Training Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

Version	Date	Author	Changes Made	Reviewed By	Approved By
1	22/03/2022	Gyan Singh	Initial creation of Information Security Training Policies and Procedures.	Mr.P Sahoo	Mr.Amit Sobti
1.1	23/03/2023	Gyan Singh	Updated mandatory training requirements and added role-specific training.	Mr.P Sahoo	Mr.Amit Sobti
1.2	23/04/2024	Gyan Singh	Revised assessment and feedback procedures to improve training evaluation.	Mr.P Sahoo	Mr.Amit Sobti

1. Purpose

The purpose of this **Information Security Training Policy** is to ensure that all employees, contractors, and third-party users are adequately trained on information security practices, data protection regulations, and the secure use of company resources. This policy aims to raise awareness about security risks and empower employees to take proactive steps to protect sensitive information and prevent security breaches.

2. Scope

This policy applies to:

- All employees, contractors, interns, and third-party users with access to company systems and data.
- All departments within the organization, including IT, HR, finance, and operational teams.
- All types of training, including onboarding, periodic refresher courses, and role-specific security training.

3. Definitions

- **Information Security Training:** Training provided to employees to ensure they understand the organization's security policies and procedures, and are equipped to handle sensitive information securely.
- **Sensitive Information:** Includes confidential data such as personal data, financial information, intellectual property, and business-critical information.

- **Security Awareness:** The knowledge and understanding of the importance of security in daily business operations and how individuals can contribute to securing company data.

4. Training Requirements

- **Mandatory Training:**
 - All new hires must complete the company's **Information Security Awareness Training** within their first [X] days of employment.
 - Employees must undergo **annual refresher training** on information security policies, data protection, and emerging security threats (e.g., phishing, malware).
- **Role-Specific Training:**
 - Employees in sensitive roles (e.g., IT, HR, finance, legal) must undergo **role-specific training** on handling sensitive data, access control, and system security.
 - This training may include more detailed topics such as encryption, secure data disposal, and secure remote work practices.
- **Training Delivery Methods:**
 - **Online Training Modules:** Available on the company's training platform.
 - **In-Person Workshops:** Conducted periodically for hands-on training and discussions.
 - **Simulated Attacks:** Phishing and other simulated attack exercises to test employee readiness and awareness.
- **Tracking and Compliance:**
 - Employee training completion will be tracked in the Learning Management System (LMS).
 - A training report will be generated for each department, ensuring that all employees have completed required training.

5. Training Content

The training programs will include, but not be limited to, the following topics:

- **Introduction to Information Security:** Basic principles of data protection, confidentiality, and integrity.
- **Password Management:** Best practices for creating and managing strong passwords.

- **Phishing and Social Engineering:** Recognizing and responding to phishing attempts and other social engineering tactics.
- **Data Protection Regulations:** Overview of relevant data protection laws (e.g., GDPR, CCPA) and their implications for handling sensitive information.
- **Incident Response:** What to do in case of a security breach or incident, including reporting procedures.
- **Access Control and Privilege Management:** Understanding and adhering to access control policies and ensuring that only authorized personnel access sensitive systems and data.

6. Training Evaluation and Effectiveness

- **Assessments:** Employees will be required to pass a knowledge assessment after each training session. The assessment will test the understanding of key concepts and ensure the effectiveness of the training.
- **Feedback Mechanisms:** Employees will have the opportunity to provide feedback on the training program. This feedback will be used to improve the training material and delivery methods.
- **Monitoring and Reporting:** Training records will be reviewed periodically to ensure that all employees are staying current with security training requirements. Reports will be generated and submitted to management to track progress.

7. Roles and Responsibilities

- **HR and Learning & Development:** Responsible for the development, delivery, and monitoring of the training programs.
- **IT Security Team:** Responsible for providing specialized security training for technical staff and supporting the development of training materials.
- **Department Heads/Managers:** Responsible for ensuring that employees within their department complete mandatory training and maintain compliance.
- **Employees:** Responsible for completing the required training and applying the knowledge to safeguard company information.

8. Training Frequency

- **Onboarding Training:** Completed by all new hires during the first 7 days of employment.

- **Annual Refresher Training:** Mandatory for all employees, reviewed and updated annually to ensure relevance.
- **Ad-Hoc or Specialized Training:** Conducted as necessary, such as when there are significant changes to security policies or the introduction of new technologies or regulatory requirements.

9. Exceptions

Any exceptions to this policy must be approved by the Chief Information Security Officer (CISO) and documented. For instance, exceptions might apply to employees who are unable to complete training due to special circumstances, such as medical leave.

10. Enforcement

- Non-compliance with the training requirements may result in disciplinary action, including access restrictions, performance reviews, or other measures to address the lack of compliance.
- The policy will be regularly reviewed to ensure that training remains up-to-date and effective in addressing emerging security threats.

11. Conclusion

The **Information Security Training Policy** is designed to ensure that employees are equipped with the knowledge and skills needed to protect sensitive information and comply with security best practices. Regular training and awareness programs will help foster a culture of security within the organization.