SOP - Security Awareness Training

1. Purpose

This SOP outlines the procedure for conducting **Security Awareness Training** for employees to ensure that all personnel are equipped with the knowledge and skills to recognize, prevent, and report security threats, particularly those targeting financial environments.

2. Scope

This SOP applies to all internal employees and staff, who have access to the organization's digital systems, financial data, or internal resources. The focus is on raising security awareness internally to reduce human-related risks and ensure a secure operational environment within the finance corporation.

3. Objective

To protect the organization from cyber threats such as phishing, social engineering, insider threats, and data breaches by:

- Increasing staff awareness of common attack vectors
- Building a security-first mindset
- Reducing the risk of human error
- Meeting regulatory compliance

4. Timing

- **New Employee Onboarding**: Within the first 7 days of joining
- **Annual Training**: Mandatory refresher course for all staff
- **Quarterly Updates**: Micro-trainings or newsletters to cover emerging threats
- **After Incidents**: Ad-hoc training sessions following security incidents

5. Methodology

Security Awareness Training will be delivered using the following methods:

- **E-Learning Modules** (Trainual)

- **Phishing Simulations**
- **Security Newsletters**
- **Policy Acknowledgment Forms** for accountability

Training completion will be tracked, with reminders and escalation procedures for non-compliance.

6. Key Topics to Include in Training

Category	Topics
Cybersecurity Basics	Importance of security, confidentiality, availability, and integrity
Phishing & Email Security	Identifying malicious emails, URLs, and attachments
Social Engineering	Tactics used by attackers and how to resist manipulation
Password Security	Creating strong passwords, password managers, MFA
Data Handling	Secure storage, transfer, and disposal of sensitive financial data
Remote Work Security	Safe use of VPNs, BYOD policies, home network security
Insider Threats	Awareness of internal risks and behavioral red flags
Incident Reporting	How and where to report suspicious activity
Compliance Requirements	Overview of financial regulations
Physical Security	Tailgating, secure desk policy, device protection

7. Roles and Responsibilities

Role	Responsibility
IT Security Team	Design, deliver, and update the training program
HR Department	Coordinate scheduling, track completion, and escalate non-compliance

Department Heads	Ensure team participation and compliance
All Employees	Complete training and apply security best practices daily

8. Review and Updates

This SOP and training content must be reviewed **annually** or following:

- A significant security incident
- Changes in regulatory requirements
- Organizational restructuring or new tools/platforms being adopted

Date: 06/06/2025