

SECURITY AWARENESS AND TRAINING POLICY

Effective	Date	
Reviewed by	The	
next scheduled review date		
Supersedes		All previous similar policies
Approved by		
Date Approved		

1.1 Purpose

This policy aims to educate employees on cybersecurity best practices, attack vectors, and incident reporting procedures to minimise human error and insider threats.

1.2 Scope

This policy applies to all employees, contractors, and temporary staff with access to company systems and data.

2.0 Security Awareness and Training Policy

2.1 Initial Training

- All new employees must complete cybersecurity awareness training before accessing company systems.
- Training must cover phishing, password management, social engineering, data protection, and incident reporting procedures.

2.2 Ongoing Education

- All employees must participate in annual cybersecurity refresher courses and phishing simulations.
- Specialised training will be provided for departments with access to sensitive information, such as finance or human resources.

2.3 Tracking and Reporting

- The HR department will track training completion and issue reminders to employees who have not completed the required training.
- Quarterly reports on training participation and results will be submitted to the CISO for review.

3.0 Policy Compliance

3.1 Compliance Measurement

Employee participation will be monitored, and reports will be submitted to department heads.

3.2 Exceptions

Must be reviewed and approved by the HR and Infosec teams.

3.3 Non-Compliance

Failure to complete training may restrict access to sensitive systems or other disciplinary measures.