SECURITY AWARENESS & TRAINING POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Security Training Frequency 4

2.2 SAT Relevance 4

2.3 SAT Course / Presentation 4

2.4 Additional SAT Material (optional) 4

3. Policy Compliance & Enforcement 5

3.1 Compliance Measures 5

3.2 Enforcement 5

4. Exception Process / Glossary 6

4.1 Exception Process 6

4.2 Glossary / Acronyms 6

5. Document Management 7

5.1 Document Revision Log 7

5.2 Document Ownership 7

5.3 Document Coordinator 7

5.4 Document Approvers 7

5.5 Document Distribution 7

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, seeXXXX-POL-ALL-001 *- Information Security Policy Framework*.

## Objective

The objective of this Policy is to provide information security requirements to provide effective security awareness and training (SAT) processes for all XXXX (XXXX) employees and contractors (where relevant).

SAT provides the single most effective method of increasing the security posture of any organisation and is the primary catalyst for instilling a culture of security and individual responsibility

## Scope

### Applicability to Employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-PRC-ALL-012 - Security Awareness & Training Procedure*

# Policy Statements

## Security Training Frequency

Security Awareness Training will be provided prior to start for all new employees and at least annually thereafter. For any consultant or sub-contractor, security awareness training may be provided, and the content will be evaluated on a case-by-case basis depending on the contracted function.

All SAT recipients will acknowledge in writing that they have taken and understood the training.

## SAT Relevance

All employees will receive or ‘security basics’ training upon hire, which will evolve along with the current threat landscape. Specific trainings will be provided on an as-needed basis in order to maintain appropriate levels of competence.

## SAT Course / Presentation

The current training is available by request from IT or HR department.

## Additional SAT Material (optional)

Where feasible, or appropriate, additional methods of SAT communication may be provided on a situational basis (e.g. on-going phishing attacks).

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review security awareness training tools and techniques throughout the XXXX environment. | * Interview with various staff members * Review personnel files * Attendance and participation lists on security trainings * Online Security training and tests completed |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in XXXX-POL-ALL-001 *- Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| PCI | Payment Card Industry |
| Phishing | An attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication |
| SAT | Security Awareness Training |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff
* Approved third parties