Information Security Awareness Training Policy

Conforms to ISO 27001:2013

Document Ref.	**Doc**
Current Version:	**1**
Previous Version:	**-**
Dated:	**1st February, 2022**
Document Author:	**ISMS Manager**
Document Owner:	**ISMS Manager**

Table of Contents

1. Introduction

1.1 Purpose

This document establishes the Information Security Awareness Training Policy for the TrusTrace. This policy ensures security awareness and training controls that protect the confidentiality, integrity, and availability of the TrusTrace's Information Resources.

1.2 Scope

This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of TrusTrace. All TrusTrace-related employees with access to TrusTrace Information or computers and systems operated or maintained on behalf of the TrusTrace are responsible for adhering to this policy.

1.3 The Issue Status

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this document.

When any part of this document is amended, a record is made in the Amendment Log shown below. The Manual can be fully revised and re-issued at the discretion of the Management Team. Please note that this Manual is only valid on the day of printing.

Issue	Amendment	Date	Initials	Authorized
1	Initial Issue	02/01/2022		ISMS Manager

2. Information Security Awareness & Training

2.1 Policy

HR Manager on behalf of TrusTrace, shall define and ensure the implementation of an information security awareness training program to increase Users' awareness of their information security responsibilities in protecting the confidentiality, integrity, and availability of TrusTrace's Information Resources.

2.2 Definitions

Information System
A major application or general support system for storing, processing, or transmitting TrusTrace Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics; the same security needs and reside in the same general operating environment.

Information System Owner
The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the TrusTrace and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

2.3 Employee and Consultants Security Awareness Training

All TrusTrace employees (full-time, part-time, contractual, interns) and consultants must complete security awareness training within the first 30 days from the date of hire. Information Security Refresher Training must be completed annually, within 60 days of the anniversary of the previous instance of such training.

2.4 Role-Based Security Awareness Training

Additional role-based security awareness training shall be required for employees and consultants whose responsibilities require additional Access, including access to Regulated or Confidential Information, as defined in the TrusTrace's Information and Classification Handling Document and related Information Systems. Role-based training must be completed on an annual or periodic basis, as required by the relevant regulatory or contractual compliance programs.

2.5 Compliance

Tracking, Measuring, and Reporting
HR Manager shall initiate mechanisms for tracking compliance with this policy and shall produce reports representing these measures to support TrusTrace decision making.

Recourse for Noncompliance
HR Manager/IT Manager is authorized to limit network access for individuals or Units not in compliance with information security policies (including this one) and related procedures. In cases where TrusTrace resources are actively threatened, the HR Manager shall act in the best interest of TrusTrace by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the HR is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, TrusTrace may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

Exceptions
Requests for exceptions to information security policies (including this one) may be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the HR for review and approval pursuant to the exception procedures published by the HR.

Frequency of Policy Review
The HR Manager shall review information security policies and procedures annually, at a minimum. This policy is subject to revision based upon findings of these reviews.

2.6 Responsibilities

TrusTrace-related employees (full-time, part-time, contractual, intern) & consultants
All TrusTrace-related employees (full-time, part-time, contractual, intern) & consultants are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.

Information Owners and Information System Owners
Information Owners and Information System Owners are also responsible for implementing processes and procedures designed to provide assurance of compliance with the minimum standards, as defined by the HR Manager, and for enabling and participating in validation efforts, as appropriate.

Regulatory and Contractual Compliance Programs
Regulatory and Contractual Compliance Programs that are responsible for ensuring appropriate treatment of Regulated or Confidential Information shall establish additional role-based security awareness training modules specific to their program, along with accompanying periodicity requirements.