



Security Policy

Awareness & Training

Version 1.0
September 1, 2022

Proprietary and Confidential
For Authorized Use Only

Document Revision History

Date	Version	Description	Author
9/1/2022	1.0	Published AT Policy	Security Control Team

Table of Contents

Introduction	4
Purpose	4
Scope	4
Roles and Responsibilities	4
Management Commitment	5
Authority	5
Compliance	6
Policy Requirements	7
Security Awareness and Training Policies and Procedures	7
Security Awareness Training	7
Role-Based Security Training	7
Security Training Records	7

1 INTRODUCTION

[REDACTED] has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by SmartEvals management and in compliance with the Awareness & Training family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

2 PURPOSE

The purpose of these policies is to establish Awareness & Training requirements to ensure the confidentiality, integrity, and availability [REDACTED] facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

3 SCOPE

The provisions of these policies pertain to all [REDACTED] employees, contractors, third parties, and others who have access to company and customer confidential information within SmartEvals systems and facilities.

4 ROLES AND RESPONSIBILITIES

These policies apply to all [REDACTED] employees, contractors, business partners, third parties, and others who need or have access to [REDACTED] customer's confidential information.

Individual or Group	Role	Responsibility
[REDACTED]		

7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

7 COMPLIANCE

Compliance with these policies is mandatory. It is [REDACTED] that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed as needed by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team's recommendations.

8 POLICY REQUIREMENTS

The following security awareness requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the SmartEvals information systems.

8.1 SECURITY AWARENESS AND TRAINING POLICIES AND PROCEDURES

This document is intended to serve as the *Security Awareness and Training Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Security Awareness and Training Policy* and related physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Security Awareness and Training Policy* every three (3) years and the procedure(s) any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with the organization's overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Security Awareness and Training Policy* and/or procedure(s) must be sent to the Information Owner.

8.2 SECURITY AWARENESS TRAINING

[REDACTED] must provide basic security awareness training to all employees including managers, senior executives, and contractors as part of initial training for new users and at least annually thereafter or when required by system changes. The security awareness training must include recognizing and reporting potential indicators of insider threats.

8.3 ROLE-BASED SECURITY TRAINING

[REDACTED] must provide role-based security-related training before authorizing access to the system or performing assigned duties and at least annually thereafter or when required by system changes.

8.4 SECURITY TRAINING RECORDS

[REDACTED] must document and monitor individual information system security training activities including basic security awareness training and specific information system security training and retain individual training records for at least one (1) year.