SmartEvals LLC Security Policy

Risk Assessment

Version 1.0
September 1, 2022

Document Revision History

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

Table of Contents

1 Introduction 1

2 Purpose 1

3 Scope 1

4 Roles and Responsibilities 1

5 Management Commitment 2

6 Authority 3

7 Compliance 3

8 Policy Requirements 4

- 8.1 Risk Assessment Policies and Procedures 4
- 8.2 Security Categorization 4
- 8.3 Risk Assessment 4
- 8.4 Vulnerability Scanning 4

1 INTRODUCTION

SmartEvals LLC 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 LLC management and in compliance with the Access Control 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 access control requirements to ensure the confidentiality, integrity, and availability of SmartEvals LLC systems, 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 SmartEvals LLC employees, contractors, third parties, and others who have access to company and customer confidential information within SmartEvals LLC systems and facilities.

4 ROLES AND RESPONSIBILITIES

These policies apply to all SmartEvals LLC employees, contractors, business partners, third parties, and others who need or have access to SmartEvals LLC systems and our customer's confidential information.

Individual or Group	Role	Responsibility
Larry Piegza	President	Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program.
Security Control Team	Information Owner	Has statutory, management, or operational authority for SmartEvals information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal.

Individual or Group	Role	Responsibility
System Administrator	Authorizing Official	Responsible for operating information system at an acceptable level of risk to organizational operations and assets.
Security Control Team	Authorizing Official Designated Representative	Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process.
Security Control Team	Information Security Manager	Responsible for conducting information system security engineering activities. Responsible for providing for appropriate security, to include management, operational, and technical controls.
Security Control Team	Information Technology Manager	Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.
Security Control Team	Information System Security Officer	Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures.
Security Control Team	System Administrator	Responsible for conducting information system security Administration activities.
Management Team	Managers	Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures
Employees	Users	Responsible for understanding and complying with Policies and Procedures.

5 MANAGEMENT COMMITMENT

SmartEvals LLC and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the SmartEvals LLC system by implementing adequate security controls.

6 AUTHORITY

These policies and procedures are issued under the authority of the SmartEvals LLC Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
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 SmartEvals LLC policy 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 risk assessment requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the SmartEvals LLC information systems.

8.1 RISK ASSESSMENT POLICIES AND PROCEDURES

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

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

8.2 SECURITY CATEGORIZATION

Information is categorized in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance. All security categorization results (including supporting

rationale) are included in the security plan and all security categorization decisions are reviewed and approved by the Authorizing Official or authorizing official designated representative.

8.3 RISK ASSESSMENT

SmartEvals LLC will employ an internal assessor to conduct an assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and the information it processes, stores, or transmits

The assessor must document risk assessment results in the security assessment report and risk assessment results will be shared with the Information Owner, Information Security Manager, and Authorizing Official (AO).

An assessor must update the risk assessment at least every three (3) years or whenever there are significant changes to information or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system and SmartEvals LLC can review the risk assessment results at least every three (3) years or when a significant change occurs.

8.4 VULNERABILITY SCANNING

In order to protect its information system and the organizational infrastructure against vulnerabilities, SmartEvals LLC scans its information operating systems, infrastructure, web applications, and databases for vulnerabilities on a monthly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported.

SmartEvals LLC information security team shall use vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations
- Formatting and making transparent, checklists and test procedures
- Measuring vulnerability impact

In order to conduct the monthly and ad hoc vulnerability scans, the information security team must:

- Employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned
- Update the list of information vulnerabilities scanned continuously, before each scan, or when new vulnerabilities are identified and reported
- Employ vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (e.g., information system components scanned, and vulnerabilities checked)
- Use privileged access authorization and/or credentials to operating systems, infrastructure, databases, and web applications for all vulnerability scans to facilitate more thorough scanning
- Employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities

- ❖ Review historic audit logs to determine if a high vulnerability identified in the information system has been previously exploited

The information security team shall analyze vulnerability scan reports and results from security control assessment and must remediate legitimate high-risk vulnerabilities within thirty (30) days, moderate risk vulnerabilities within ninety (90) days, and low risk vulnerabilities within one hundred and eighty (180) days in accordance with an organizational assessment of risk.

Information obtained from the vulnerability scanning process and security control assessments must be shared with the ISM, Information Owner, and personnel designated by AO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

1.