Security Self Assessment Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Security self assessments are part of ABC Company’s controls and safeguards designed to identify, mitigate, eliminate, and transfer risks that can impact business operations.

# II. Purpose

Security self assessments help ensure ABC Company's security controls and safeguards adequately protect Information Resources. By knowing the current status of information systems and information security programs, ABC Company can determine the appropriate risk treatment option.

# III. Scope

This policy applies to ABC Company Executive Management, Chief Security Officer, Risk Management Officer, and ABC Company Department Heads.

# IV. Policy

Per the Risk Management Policy, executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization.

Security self assessments help manage and reduce risks to ABC Company’s Information Resources. The Chief Security Officer (CSO), with assistance from the Risk Management Officer (RMO), shall oversee the security self assessment. Security self assessments shall be performed on an annual basis or more frequently if major changes occur to Information Resources.

The CSO shall:

* Resources – identify internal resources to perform the security self assessment.
* Scope – define the scope of the security self assessment.
* Security Requirements – prepare a list of any requirements that are relevant to the security self assessment.
* Description – Describe the Information Resources to be assessed including mission description, system identification, and criticality. Describe the environment including facilities, physical security, maintenance, etc. Identify the system architecture, interfaces, data flow, etc. Describe the system security requirements.

The CSO shall identify the security safeguards to be included in the security self assessment project scope:

* Administrative safeguards – identify if administrative safeguards are to be included in the scope. Administrative safeguards include security policies, procedures, job descriptions, agreements with service providers, security training and awareness plans, incident response plans, business continuity plans, cyber security insurance policies, and other written security controls.
* Technical safeguards – identify the technical safeguards to be included in the project scope. Technical safeguards include access controls (passwords, account lock, inactivity timeout), security protection measures (firewalls, anti-malware, encryption), management (patch management, system utilization, backups), logging and monitoring systems, system configurations and hardening, and related security controls.
* Physical safeguards – identify the physical safeguards to be included in the project scope. Physical safeguards include secure areas are protected by appropriate entry controls, only authorized personnel are allowed access, cameras record activities in sensitive areas with appropriate retention of images, procedures identify visitor controls such as visitor sign-in, wearing of visitor badges, escorting by authorized personnel, etc.

Once the scope has been identified, the CSO shall:

* Vulnerabilities – establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”).
* Evaluating – identify methods for evaluating vulnerabilities and assigning risk ratings based on an organization’s environment and risk assessment strategy.
* Tools – ensure access to security assessment tools is controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. Security self assessment requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

The security self assessment report shall include the project scope, findings, and recommendations to enhance security. The CSO shall:

* Review the report to confirm the findings and verify the security recommendations are appropriate and sufficient.
* Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The Risk Management Officer shall provide necessary reporting to ABC Company Executive Management.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to ABC Company Executive Management, Chief Security Officer, Risk Management Officer, and ABC Company Department Heads.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM03.07, APO11.09, APO13.07, BAI04.05, BAI10.07, DSS05.08, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(D), 164.308(a)(8)

ISO 27001:2013 8.3, 9.2, 9.3, A.12.7, A.15.2.1

NIST SP 800-37 3.5, 3.7

NIST SP 800-53 3.3, AU-1, AU-6

NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-1-4

PCI Self-assessment Questionnaires (SAQs), A3.1.2