Security Controls Review 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 controls and safeguards are part of ABC Company’s Risk Treatment Plan to mitigate, eliminate, and transfer risks that can impact business operations.

# II. Purpose

Risk is the potential that a threat will exploit one or more asset vulnerabilities and result in a loss or failure to achieve an objective. At ABC Company, risk management is the process of identifying, analyzing, and the use of safeguards and controls to treat risks. This policy establishes a formal and periodic review of security control and safeguards.

# III. Scope

This policy applies to the Risk Management Officer and ABC Company Department Heads.

# IV. Policy

ABC Company’s Risk Management Officer shall be responsible for reviewing safeguards and controls on an annual basis. The purpose of the review will be to ensure the controls are sufficient, appropriate, and effective at managing and reducing risks to acceptable levels.

Per the Risk Management Policy, on an annual basis each ABC Company Department Head will prepare and provide to the Risk Management Officer, a Risk Assessment, Risk Analysis, and a Risk Treatment Plan. Collectively, these documents specify specific security controls and safeguards.

The Risk Management Officer will review the security controls to ensure they are aligned with the needs of the organization. The Risk Management Officer may choose to have security controls independently reviewed by a Certified Information Systems Auditor (certified by the Information Systems Audit and Control Association) to ensure they are sufficient, appropriate, and effective at managing and reducing risks.

As necessary, the Risk Management Officer will recommend to the appropriate Department Heads changes or enhancements to security controls and safeguards. This process helps ensure each department’s approach to managing risk is properly aligned with the needs of the organization.

Security controls can be classified according to their approach to security incidents:

* Preventive controls – These safeguards prevent security incidents. Examples include passwords, encrypting laptop hard drives, cards that permit physical access to data centers, etc.
* Detective controls – During an event, detective controls identify and characterize an incident in progress. Examples include anti-virus software, alarms and notifications, etc.
* Corrective controls – Limit the extent of damage caused by the incident and assist in resuming normal business operations.

Security controls may also be classified according to their nature, for example:

* Administrative controls – Safeguards include formal and informal policies, procedures, and security training.
* Physical controls – Protection mechanisms that protect physical assets (e.g. access cards, data center server racks, locking cabinets).
* Technical controls – Technical safeguards (e.g. logical access controls, passwords, patch management, security assessments)

# V. Enforcement

Any Staff 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, Department Heads, IT Director, Risk Management Officer, and Chief Security Officer.

**Policy History**

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

**References:**

COBIT APO01.11, APO03.06, APO11.09, APO12.02, APO12.07, DSS05.07, MEA04.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(i), 164.308(a)(8), 164.308(a)(2)

ISO 27001:2013 9.3, A.5.1.2, A.9.1.1, A.18.2

NIST SP 800-37 3.5, 3.7

NIST SP 800-53 All XX-1 controls, CA-2, CA-7

NIST Cybersecurity Framework ID.RM-1, PR.PT-1, DE.CM-8, DE.DP-5

PCI 6.7, 7.3, 8.1, 8.8, 12.5, 12.8