Resilience 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

Information Systems are critical to ABC Company’s business operations. Controls prevent disruption as well as provide the ability for ABC Company to quickly restore services if they are disrupted. Resiliency is an important component of ABC Company’s risk management program.

# II. Purpose

The purpose of this policy is to ensure appropriate controls are designed and implemented to provide ABC Company with the ability to protect and recover quickly when an Information System is not able to provide service.

# III. Scope

This policy applies to the Chief Security Officer (CSO) and Risk Management Officer (RMO).

# IV. Policy Working together, the CSO and RMO shall:

* Focus on capabilities supporting organizational missions or business functions.
* Identify processes that provide and maintain an acceptable level of service considering the threats and challenges to Information Systems.
* Ensure resilience includes the ability to withstand and recover from deliberate attacks, accidents, or events that occur naturally.

A resilient lifecycle shall be developed and maintained:

* Concept - Prioritize and tailor objectives, design principles, and limit the set of techniques and approaches to be used in solutions.
* Development - Use techniques and approaches to define alternative solutions, apply design principles to refine and analyze alternative solutions, develop capabilities to achieve the objectives.
* Production - Implement and evaluate the effectiveness of resiliency solutions, provide resources, or ensure that resources will be provided, to achieve the objective.
* Utilization - Monitor the effectiveness of cyber resiliency solutions, using capabilities to achieve objectives, reprioritize and tailor objectives as needed, and adapt mission, business, and/or security processes to address environmental changes.
* Support – Re-visit the prioritization and tailoring of objectives, use the results of monitoring to identify new or modified requirements, re-visit constraints on techniques and approaches, and modify or upgrade capabilities.
* Retirement - Prioritize and tailor objectives for the environment of operation, ensure that disposal processes enable those objectives to be achieved including modifying or upgrading capabilities of other systems as necessary.

The CSO and RMO should ensure that risks are properly identified per the Risk Management Policy. Risk management is an on-going process by which ABC Company Staff manage risks through a three-step process:

* Risk Assessment – Identify assets, threats to the assets, and vulnerabilities that exist as a result of the threats.
* Risk Analysis – For each risk, identify the likelihood and impact on our organization.
* Risk Treatment Plan – Develop controls and other safeguards designed to mitigate, eliminate, or transfer risks.

Executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. A summary of the departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans shall be reviewed by Executive Management on an annual basis to ensure that controls are sufficient and effective at treating risks.

ABC Company’s RMO shall ensure a formal and document Risk Management Framework has been established to manage risks related to Information Systems. The Risk Management Framework shall include:

* Categorize Information Systems
* Select security controls
* Implement security controls
* Assess security controls
* Authorize security controls
* Monitor security controls

The CSO shall ensure:

* The Risk Assessment identifies scenarios that may result in a disruption to services.
* Security measures with preventive, detective, and corrective controls are implemented to ensure services are resistant to disruptions.
* Business continuity and disaster recovery processes restore operations within identified recovery point objectives and recovery time objectives.

When appropriate, the CSO shall prepare and document an uncertainty analysis for the RMO. The uncertainly analysis shall consider a lack of sufficient information to determine the exact value of the elements of the risk model, including the threat frequency, safeguard effectiveness, or consequences.

# 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 the Chief Security Officer (CSO), Risk Management Officer (RMO), and executive management.

**Policy History**

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

**References:**

COBIT EDM03.02, APO09.05, BAI04.05, BAI04.07, DSS01.05, DSS03.05, MEA01.05

GDPR Article 32(b)

HIPAA 164.308(a)(1)(i)

ISO 27001:2013 9.3, 10.2, A.16.1, A.17

NIST 800-53 CP-2, 800-193 §2.3.1

NIST Cybersecurity Framework ID.BE-5, PR.IP-9-10, DE.DP-2, RS.RP-1, RC.RP-1

PCI 6.1