Cybersecurity Framework 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

A Cybersecurity Framework is a set of industry standards and best practices that help organizations cost effectively manage cybersecurity risks.

# II. Purpose

Information Resources are critical to ABC Company’s business operations. This policy ensures a cybersecurity framework will be developed and implemented using business drivers to guide cybersecurity activities and protection mechanisms.

# III. Scope

This policy applies to all ABC Company Staff that have a responsibility to manage risks related to ABC Company’s Information Resources.

# IV. Policy

A. Cybersecurity Framework Functions

A cybersecurity framework allows communication of cybersecurity activities and outcomes across a wide range of ABC Company departments from Executive Management to operational departments. The following functions provide a strategic view of ABC Company’s lifecycle management of cybersecurity risk:

* Identify
* Protect
* Detect
* Respond
* Recover

Identify. ABC Company Staff shall understand and manage cybersecurity risk to systems, assets, data, and capabilities. Understanding business risk, resources that support critical functions, and the related cybersecurity risks enables ABC Company to focus and prioritize our efforts in a manner that is consistent with our risk management strategy and needs of the organization. Major categories to achieve these objectives include:

* Asset Management – Information Resources that enable ABC Company to achieve business purposes shall be identified and managed consistent with their relative importance to business objectives and risk strategy. For more information see the IT Management Policy and System Security Plan.
* Business Environment – ABC Company’s mission, objectives, stakeholders, and activities shall be communicated in an appropriate manner and prioritized. This information shall be used to make Staff aware of cybersecurity roles, responsibilities, and risk management decisions. For more information see the Business Impact Analysis, IT Governance Policy, and Securing Information Systems Policy.
* Governance – policies, procedures, and processes shall be used to implement, manage, and monitor ABC Company’s regulatory, legal, risk, environmental, and operational requirements. Requirements and cybersecurity risk shall be communicated to the appropriate Staff and Executive Management. For more information see the IT Governance Policy.
* Risk Assessment – Staff shall understand the cybersecurity risk to ABC Company operations, assets, and to Staff. For more information see the Risk Assessment Policy.
* Risk Management Strategy – ABC Company’s priorities, constraints, risk tolerances, and assumptions shall be established and used to support operational risk decisions. For more information see the Risk Management Policy.

Protect. ABC Company Staff shall develop and implement appropriate safeguards to limit or contain the impact of a potential cybersecurity event and ensure the delivery of critical services. Major categories include:

* Access Control – Access to assets and associated facilities shall be limited to authorized users, processes, or devices, and to authorized activities and transactions. For more information see the Identification and Authentication Policy, Logical Access Controls Policy, Network Access Policy, Password Policy, Remote Access Policy, User Privilege Policy, and Wireless Access Policy.
* Awareness and Training – ABC Company’s Staff shall be provided cybersecurity awareness education and adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. For more information see the Security Awareness and Training Policy and Security Awareness and Training Plan.
* Data Security – Information Resources shall be managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. For more information see the Account Management Policy, Asset Management Policy, Data Classification Policy, Electronic Disposal Policy, and Network Access Policy.
* Information Protection Processes and Procedures – Security policies, processes, and procedures shall be maintained and used to manage protection of Information Resources. For more information see the Security Policy and System Security Plan.
* Maintenance – Maintenance and repairs of Information Resources shall be performed consistent with ABC Company’s policies and procedures. For more information see the Hardware and Software Maintenance Policy.
* Protective Technology – technical security solutions shall be managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. For more information see the Anti-malware Policy, Electronic Data Retention Policy, Encryption Policy, Firewall Policy, Patch Management Policy, Quality Assurance Policy, Software Development Policy, System Update Policy, and VPN Policy.

Detect. ABC Company Staff shall develop and implement the appropriate activities to identify in a timely manner the occurrence of a cybersecurity event. Major categories include:

* Anomalies and Events – activity, and its potential impact, shall be detected in a timely manner. For more information see the Identity Theft Protection Policy, Incident Response Policy, and Logging Policy.
* Security Continuous Monitoring – Information Resources shall be monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. For more information see the Security Monitoring Policy.
* Detection Processes – detection processes and procedures shall be maintained and tested to ensure timely and adequate awareness of events. For more information see the Incident Response Policy.

Respond. ABC Company Staff shall develop and implement the appropriate activities to take action and contain the impact of a detected cybersecurity event.

* Response Planning – response processes and procedures shall ensure a timely response to detected cybersecurity events. For more information see the Security Monitoring Policy and Incident Response Plan.
* Communications – response activities shall be coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. For more information see the Incident Response Plan and Reporting Violations Policy.
* Analysis – analysis shall be conducted to ensure adequate response and support recovery activities. For more information see the Incident Response Policy and Incident Response Plan.
* Mitigation – Activities shall be performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. For more information see the Incident Response Policy and Incident Response Plan.
* Improvements – response activities shall be enhanced by incorporating lessons learned from current and previous detection/response activities. For more information see the Incident Response Policy and Incident Response Plan.

Recover. ABC Company Staff shall develop and implement the appropriate activities (e.g. redundancy, failover, etc.) to allow operations to continue and to restore any capabilities or services that were impaired due to a cybersecurity event. Timely recovery to normal operations reduces the impact of a cybersecurity event.

* Recovery Planning – recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. For more information see the Business Continuity Policy, Business Impact Analysis, Business Resumption Plan, Department Continuity of Operations Plan, and IS Disaster Recovery Plan.
* Improvements – recovery planning and processes shall be enhanced by incorporating lessons learned into future activities. For more information see the Business Continuity Policy
* Communications – restoration activities shall be coordinated with internal and external entities. Such entities to include Executive Management, resource owners, Internet Service Providers, etc. For more information see the Business Continuity Communications Plan, Business Continuity Plan, and Business Continuity Policy.

B. Cybersecurity Framework Implementation

On an annual basis the Chief Security Officer (CSO) shall evaluate how ABC Company views cybersecurity risk as well as the processes in place to manage that risk. The evaluation will include cybersecurity risk management practices and the extent to which cybersecurity risk management is integrated into an organization’s overall risk management practices.

Cybersecurity best practices have identified four cybersecurity framework implementation tiers:

1. Partial. Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad-hoc and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization may not have the processes in place to participate in coordination or collaboration with other entities.
2. Informed. There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis. The organization has not formalized its capabilities to interact and share information externally.
3. Repeatable. The organization’s risk management practices are formally approved and expressed as policies. Organizational cybersecurity practices are regularly updated based on the application of risk management processes, changes in business/mission requirements, and a changing threat and technology landscape. There is an organization-wide approach to manage cybersecurity risk. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization understands its dependencies and partners and receives information from these partners that enables collaboration and management decisions within the organization in response to events.
4. Adaptive. The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks. The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

The CSO’s evaluation should identify ABC Company’s current tier level as well as determine if a progression to a higher tier would cost effectively reduce cybersecurity risk.

C. Cybersecurity Framework Profile

The CSO shall implement and maintain a cybersecurity framework profile that aligns the functions and categories identified in with ABC Company’s business requirements, risk tolerance, and resources of the organization. The profile establishes a prioritized risk management roadmap that reduces cybersecurity risk, is aligned with ABC Company’s goals and objectives, helps meet compliance and regulatory requirements, and is aligned with cybersecurity best practices.

When possible, the CSO shall establish two cybersecurity framework profiles, one that describes the Current Profile state and another that defines the desired Target Profile state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. The CSO shall perform a comparison of the two profiles, the Current Profile and Target Profile, to reveal gaps to be addressed to meet cybersecurity risk management objectives. The CSO shall prepare a prioritized action plan to address these gaps.

# 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 all Staff members that have a responsibility to manage risks related to ABC Company’s Information Resources.

**Policy History**

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

**References:**

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 24, 25, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(i), 164.314(a)(2)(i)

ISO 27001 5.2, A.6.1

NIST SP 800-37 2.2, 3.4

NIST SP 800-53 CA-1, PL-1, RA-1, SI-1

NIST Cybersecurity Framework All sections ID.XX, PR.XX, DE.XX, RS.XX, RS.XX, RC.XX

PCI 12.1