Cybersecurity 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

Since all Information Systems rely on operating systems and networks to function, those areas are often targeted for attack and are the main sources of many security vulnerabilities.

# II. Purpose

Cybersecurity is the use of various technologies and processes to protect networks, computers, programs, and data. Cybersecurity ensures that ABC Company’s Information Systems are protected by security measures that prevent attacks, damage, or unauthorized access.

# III. Scope

This policy applies to all ABC Company Staff responsible for the security of ABC Company’s Information Resources.

# IV. Policy

Cybersecurity helps to maintain an environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, and privacy.

The Chief Security Officer (CSO) shall establish a risk-based framework core consisting of cybersecurity activities, outcomes, and references that provide guidance for developing individual organizational profiles. The CSO shall:

* Prioritize and scope. Identify organization objectives and priorities and determine the scope of systems and assets that support the selected business line or process.
* Orient. Identify Information Systems and assets, regulatory requirements, and overall risk approach, identify threats to, and vulnerabilities of, those systems and assets.
* Current Profile. Identify categories, subcategories, and outcomes achieved.
* Risk assessment. Identify the likelihood of a cybersecurity event and the impact on the organization. Consider emerging risks.
* Target Profile. Create a Target Profile focusing on categories, subcategories, and desired cybersecurity outcomes.
* Determine, Analyze, and Prioritize Gaps. Compare the Current Profile and the Target Profile to determine gaps and create a prioritized action plan to address those gaps.
* Implement Action Plan. Determine actions to take and monitor against the Target Profile.

The CSO shall consider how the cybersecurity program might incorporate privacy principles such as:

* Individual consent to the use of personal information
* Collecting the minimum amount of personal information
* Controls over the use and disclosure of personal information
* Use and retention of personal information related to a cybersecurity incident
* Transparency for certain cybersecurity activities
* Accountability and auditing

A. Functions

The CSO shall identify five concurrent and continuous functions:

* Identify. To better align security with the organization, the CSO shall understand the business, resources, and cybersecurity risks. Major categories (e.g. Asset Management, Governance, and Risk Management) shall be identified to assist in this effort.
* Protect. The CSO shall ensure that appropriate safeguards are implemented. Major categories (e.g. Access Control, Security Awareness and Training, Data Security, and Maintenance) shall be identified to protect ABC Company’s Information Systems.
* Detect. The CSO shall identify cybersecurity events. Major categories shall include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.
* Respond. The CSO shall identify actions regarding a detected event. Major categories include Response Planning, Communications, Analysis, Mitigation, and Improvements.
* Recover. The CSO shall ensure ABC Company’s Information Systems maintain resilience and restore capabilities. Major categories include Recovery Planning, Improvements, and Communications. See the Resilience Policy for more information.

B. Implementation Tiers

The CSO shall identify how ABC Company views cybersecurity risk and the processes in place to manage that risk. The CSO shall identify implementation tiers that vary from Partial (Tier 1) to Adaptive (Tier 4). The CSO shall identify ABC Company’s current implementation tier according to the following criteria:

* Tier 1: Partial implementation. Examples of partial implementation include risk management is not formalized, ad-hoc approach to security, limited awareness of cybersecurity risk, and no collaboration with other entities regarding cybersecurity events.
* Tier 2: Risk Informed. Examples of risk informed include management approves risk management, no wide management of cybersecurity risk, and no capabilities to share info externally.
* Tier 3: Repeatable. Examples of a repeatable implementation include risk management policies, organization-wide management of cybersecurity risk, and ABC Company receives information from partners that enables risk-based decisions.
* Tier 4: Adaptive. Examples of an adaptive implementation include the ability to adapt security based on lessons learned, predictive indicators, risk management is part of the organization’s culture, information is shared by and with other entities before an event occurs, and continuous awareness of activities on systems/networks.

C. Profiles

A Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables ABC Company to establish a roadmap for reducing cybersecurity risk that is aligned with organizational goals, considers legal/regulatory requirements, industry best practices, and reflects risk management priorities.

Profiles help ABC Company align its cybersecurity activities with its business requirements, risk tolerances, and resources. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile with a “Target” Profile.

The CSO shall compare the Current Profile with a proposed Target Profile to identify gaps to be addressed to meet cybersecurity risk management objectives.

D. Cybersecurity Framework

The CSO shall develop a comprehensive framework that includes Functions (Identify, Protect, Detect, Respond, and Recover), appropriate categories, subcategories, and applicable informative references. See the Cybersecurity Framework Policy for more information. The following table helps illustrate the relationship of Functions, Categories, Subcategories, and references. Additional examples are available in National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function** | **Category** | **Subcategory** | **References** |
| Identify | Asset Management | An inventory exists of the physical devices and systems.  Software platforms and applications are inventoried.  Communications and data flows are mapped.  External information systems are identified and documented.  Information Systems are prioritized based upon their classification, criticality, and business value | ISO 27001 A.8.1.1-2  NIST SP 800-53 CM-8  ISO 27001 A.8.1.1-2  NIST SP 800-53 CM-8  ISO 27001 A.13.2.1  NIST SP 800-53 AC-4, CA-3, CA-9  ISO 27001 A.8.2.1  NIST SP 800-53 AC-20, SA-9  ISO 27001 A.8.2.1  NIST SP 800-53 CP-2, RA-2, SA-14 |

E. Policies

The CSO and Chief Risk Officer (CRO) shall ensure that ABC Company’s risks are properly managed and mitigated to the extent possible. The CSO and CRO shall oversee the implementation and maintenance of formal policies that govern Information Resources.

|  |  |
| --- | --- |
| **Control Category** | **Policy/Plan/Procedure** |
| Governance  Leadership Context | Context and Alignment Policy  Ethics Policy  Health Safety Policy  IT Governance Policy  Mergers and Acquisitions Policy  Standard Operating Procedure Policy  Terms and Definitions Policy |
| Information Security | Information Security Policy  Privacy Policy  Securing Information Systems Policy  Security Controls Review Policy |
| Planning  Risk Management | Business Impact Analysis  Cybersecurity Policy  Cybersecurity Framework Policy  Risk Assessment Policy  Risk Management Policy |
| Policies and Procedures | Security Policy  Security Policy Introduction  System Security Plan |
| Organization | Audit Policy  IT Management Policy  Non-Disclosure Agreement  Outsourcing Policy  Staffing Policy  Security Self Assessment Policy |
| Asset Management | Access Control Policy  Access Control Procedure  Asset Management Policy  Configuration Management Plan  Configuration Management Policy  Configuration Management Procedure  Data Classification Policy  Software Licensing Policy |
| Human Resources  Communication | Acceptable Use Policy  Audit Policy  Security Awareness and Training Plan  Security Awareness and Training Policy  Staffing Policy  Social Networking Policy  Third Party Service Providers Policy |
| Physical  Environmental | Facility Security Plan  Personnel Security Policy  Physical Access Policy  Physical Security Policy |
| Operation  Support | Account Management Policy  Anti-Malware Policy  Anti-Malware Procedure  Backup Plan  Backup Policy  Backup Procedure  Bluetooth Policy  Capacity and Utilization Policy  Data Analytics Policy  Data Integrity Policy  Data Marking Policy  Data Privacy Policy  Disposal Policy  Documentation Policy  Domain Controller Policy  Domain Name System Policy  E-commerce Policy  E-mail Policy  Firewall Policy  Firewall Procedure  Guess Access Policy  Internet Connection Policy  Intrusion Detection Policy  Logging Policy  Logging Procedure  Mass Communication Policy  Network Address Policy  Network Configuration Policy  Network Documentation Policy  Network Security Policy  Problem Management Policy  Problem Management Procedure  Ransomware Policy  Removable Media Policy  Router Security Policy  Security Monitoring Policy  Server Hardening Policy  Vendor Access Policy  Workstation Hardening Policy  Workstation Security Policy |
| Access Control | Access Control Policy  Admin Special Access Policy  Bring Your Own Device Policy and Technology  Guest Access Policy  Identification and Authentication  Logical Access Controls Policy  Mobile Device Policy  Password Policy  Portable Computing Policy  Remote Access Policy  Securing Information Systems Policy  Securing Sensitive Information Policy  Smartphone Policy  System Update Policy  User Privilege Policy  Wearable Computing Device Policy  Web Policy  Wireless Access Policy |
| Acquisition  Development  Maintenance | Acquisition and Procurement Policy  Application Implementation Policy  Approved Application Policy  Audit Trails Policy  Change Management Policy  Change Management Procedure  Encryption Policy  Green Computing Policy  Hardware and Software Maintenance Policy  Hardware and Software Maintenance Procedure  Patch Management Policy  Patch Management Procedure  Production Input Output Controls Policy  Quality Assurance Policy  Secure Development Lifecycle Policy  Server Certificates Policy  Software Development Policy  VPN Policy  Web Site Policy |
| Incident Management | Identity Theft Protection Policy  Incident Response Policy  Incident Response Plan  Reporting Violations Policy |
| Business Continuity  Disaster Recovery | Business Continuity Plan  Business Continuity Policy  Business Resumption Plan  Continuity Communications Plan  Department Continuity of Operations Plan  IS Disaster Recovery Plan  Resilience Policy |
| Compliance  Performance Evaluation | Business Associates Agreement  Certification and Accreditation Policy  Compliance Policy  Data Retention Policy  GDPR EU Privacy and Data Protection Policy  HIPAA and HITECH Policy  HITRUST Policy  PCI Policy  Security Controls Review Policy  Software Licensing Policy  System and Organization Controls SOC2 Policy  Vulnerability and Penetration Testing Policy |

# 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 all ABC Company Department Heads and those responsible for information and physical security.

**Policy History**

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

**References:**

COBIT APO11.01-02, APO11.04-05, BAI02.04, BAI03.06, BAI03.08, BAI07.03, BAI07.05

GDPR Article 25

HIPAA 164.308(a)(2)

ISO 27001 A.8.1.1-2, A.8.2.1, A.13.2.1

NIST SP 800-37 3.1

NIST SP 800-53 AC-4, AC-20, CA-3, CA-9, CM-8, CP-2, RA-2, SA-9, SA-14

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

PCI A3.2.3, PCI Software Security Framework