Information Security 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 provide ABC Company with the resources needed to operate in an efficient and effective manner. Information systems must be protected from security-related threats.

# II. Purpose

This policy specifies security protocols and procedures to be followed by Staff and other users.

# III. Scope

This policy applies to all Staff that use ABC Company’s Information Systems.

# IV. Policy

A. Security Overview

The CSO shall ensure security safeguards and controls are implemented and maintained to achieve the desired security objectives of resource availability, information confidentiality, and data integrity. Per the Security Policy, security controls and safeguards shall be grouped into the following major categories:

* Administrative safeguards
* Technical safeguards
* Physical safeguards

B. Security Controls

Executive Management shall ensure job descriptions exist for all employees. Each job description shall identify the position title, purpose of the position, specific security duties and responsibilities, reporting relationships, position requirements, and related information.

All departments shall have appropriately supervised Staff sufficient to maintain information security. The staffing level should be appropriate to the environment, i.e. the amount and type of information for which they are responsible and the level of risk.

The Chief Security Officer (CSO) shall be responsible for implementing and maintaining security policies, procedures, plans, forms, and related documents. Policies and procedures shall manage the process of creating, monitoring, controlling, and removing of accounts. Refer to the Account Management Policy for more information.

All users, hosts, and data shall be classified per the Data Classification Policy.

Staff are a first line of defense and shall follow safe computing practices as outlined in the Acceptable Use Policy. Access to specific functions shall be restricted, never allowing Staff to request information, functions, or other resources for which they do not have access.

Staff shall ensure Sensitive Information remains secure by clearing their desks when they will be away from their office, positioning monitors to prohibit unauthorized viewing, etc. See the Clear Desk Policy for more information.

The CSO shall ensure that information is protected during its entire lifecycle. Information shall only be retained for the duration of its useful life. The disposal of hardware, software, and information requires special consideration. Refer to the Data Retention Policy, Disposal Policy, Encryption Policy, and Removable Media Policy for more information. ABC Company’s IT Department shall be responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). Please refer to the Software Development Policy for more information.

Prior to granting individuals physical or logical access to Information Resources, agreements with Staff, third-party users, and customers shall be in place and include responsibility for information security. Refer to the Third Party Service Providers Policy for more information.

For additional controls and safeguards please refer to the Security Policy.

D. Physical Safeguards

Physical safeguards shall ensure only authorized Staff have access to Information Systems, equipment, and operating environments. For more information see:

* Facility Security Plan
* Physical Access Policy
* Physical Security Policy

Physical security protection

* Only hardware or software acquired through ABC Company’s approved policies and procedures may be installed. Refer to the Acquisition and Procurement Policy.
* Media shall be handled according to the Removable Media Policy.
* Access to Information Resources shall be controlled and restricted as much as possible. Devices not in use for extended periods shall be turned off. Workstations and servers shall have appropriate and secure physical controls. Refer to the Physical Security Policy for more information.
* Staff shall be made be aware of the visibility of data on their computer or handheld device display screens. Staff shall position equipment or furniture to eliminate over-the-shoulder viewing.
* Staff shall minimize costly disruptions caused by data or hardware loss. Refer to the Physical Security Policy to reduce risks related to environmental threats and hazards and opportunities for unauthorized access.

# 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 Staff that use 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 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)

ISO 27001:2013 A.5, A.7.2.2, A8.1.3, A.8.2.1, A.9-14, A.16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8, PCI Software Security Framework