Access Control 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

ABC Company’s Information Systems are provided as a central resource for ABC Company Staff. It is important that the network infrastructure, which includes cabling and associated devices continues to develop with sufficient flexibility to meet ABC Company demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

# II. Purpose

The purpose of this policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of ABC Company information.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company’s Information Resources.

# IV. Policy

Users are permitted to access and use only approved Information Resources. Users inside the ABC Company firewall may not connect to the ABC Company network if they are using a wireless connection to connect to an external network.

Non-IT Staff shall not:

* Extend or re-transmit network services by installing a router, switch, hub, or wireless access point to the ABC Company network
* Install network hardware or software that provides network services
* Alter network hardware in any way
* Download, install, or run security programs or utilities that reveal weaknesses in the security of a system
* Run password cracking programs, packet sniffers, network mapping tools, or port scanners

The Chief Security Officer shall ensure:

* The organization has implemented procedures for the authorization and/or supervision of employees who work with Sensitive Information or in locations where it might be accessed.
* Detailed job descriptions determine the appropriate level of access to Sensitive Information.
* Access to Information Systems is limited to authorized users and processes. Access to Information Systems is limited to the types of transactions and functions that authorized users are permitted to access. Users, processes, and devices are authenticated before allowing access to Information Systems. Controls shall be implemented and maintained to ensure Information System users, and processes acting on behalf of users or devices, are properly identified.
* A process exists to establish and maintain access to Sensitive Information. Similar processes exist to control access to paper records.
* Procedures exist to ensure the access of an employee to Sensitive Information is appropriate and the procedures are used consistently.
* Procedures protect Sensitive Information from parent organizations and subsidiaries. Technical safeguards exist to separate Sensitive Information used by ABC Company to protect against unauthorized access by other organizations.
* Procedures grant access to Sensitive Information through access to a workstation, device, transaction, program, or process. Procedures specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of a specific device that can access Sensitive Information.
* Procedures identify devices that access Sensitive Information and those that do not. Procedures specify where to place and position workstations to only allow viewing by authorized individuals. Procedures specify the use of additional security measures (e.g. privacy screens, password protected screen savers, auto logoff, etc.) to protect workstations with Sensitive Information.
* Procedures address device use for users that access Sensitive Information from remote locations.
* Procedures specify that electronic sessions be terminated after a specified period of inactivity. Automatic logoff is implemented on all devices that have access to Sensitive Information. Refer to the Securing Information Systems Policy for more information.
* The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
* Controls are implemented and maintained on connections to external Information Systems. Controls are implemented on information that is posted or processed on publically accessible Information Systems. Processes are implemented to ensure controls are sufficient and effective.
* Passwords/phrases are changed on a regular basis according to a schedule identified in the Password Policy.

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

# 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.

**Policy History**

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

**References:**

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)

ISO 27001 A.7.2.1, A.8.1.2-3

NIST SP 800-37 3.3

NIST SP 800-53 AC-1-3

NIST Cybersecurity Framework PR.AC1-7, DE.CM-1-3, DE.DP-2, RS.RP-1

PCI 7.1-3, PCI Software Security Framework