Access Control Procedure

|  |  |
| --- | --- |
| 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

This procedure provides detailed steps and actions to secure Information Systems per the Access Control Policy.

# II. Purpose

The purpose of this procedure is to formally document the steps, actions, and processes needed to meet the requirements specified in ABC Company's Access Control Policy.

# III. Scope

This procedure applies to all ABC Company Department Heads and IT Staff who administer access controls to Information Systems.

# IV. Procedure

On an annual basis, Department Heads review department Staff job descriptions to ensure they specify the appropriate level of access to Sensitive Information.

As needed, Configuration Items are added to the Configuration Management Database per the Configuration Management Plan. The Configuration Management Database includes relevant information about Configuration Items including a description, Resource Owner, attributes, baselines, relationships, changes, and other important information. Devices that contain Sensitive Information are specifically identified and inventoried as Configuration Items in the Configuration Management Database. For more information see the Configuration Management Plan for configuration controls and configuration management audits that review information in the Configuration Management Database to verify it is complete and error free.

On a quarterly basis, Department Heads review Information Systems Access Request Forms for appropriate approvals, changes to access rights, and termination of rights. ABC Company access permissions are validated by IT Staff to ensure Information System users, and processes acting on behalf of users or devices, are properly identified. IT Staff compare Information Systems Access Request Forms with system configurations to ensure Staff access rights agree with Access Request Forms. Any variations are brought to the attention of the appropriate Department Head for resolution.

On a quarterly basis, IT Staff review access rights from parent organizations and subsidiaries. IT Staff compare Information Systems Access Request Forms with system configurations to ensure Staff access rights agree with Access Request Forms. Any variations are brought to the attention of the appropriate Department Head for resolution.

On a quarterly basis, authentication controls for software applications, servers, workstations, firewalls, network devices, service providers, and related equipment are reviewed by IT Staff to verify they meet Password Policy requirements. Any variations are brought to the attention of the appropriate Department Head for resolution.

When new equipment is installed, and on a quarterly basis, IT Staff ensure that workstations with Sensitive Information are protected through the use of monitor positioning, privacy screens, password protected screen savers, session timeout, and auto logoff.

When new utility/audit programs are installed, and on a quarterly basis, IT Staff ensure that programs capable of overriding system and application controls are restricted and tightly controlled.

When new equipment is installed, and on a quarterly basis, IT Staff verify that passwords/phrases are changed according to the schedule identified in the Password Policy.

When new firewalls are installed, and on a quarterly basis, IT Staff ensure the firewall is placed in a physical location that restricts access to authorized individuals. Firewalls are hardened per the Firewall Hardening Procedure. Each firewall administrator uses their own unique administrator account when managing the firewall.

When new equipment is installed, and on a quarterly basis, IT Staff refer to manufacturer resources for updated guidance on hardening firewalls, servers, and security functionality.

# V. Enforcement

Any Staff member found to have violated this procedure may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This procedure is to be distributed to ABC Company Department Heads and IT Staff who administer access controls.

**Procedure History**

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