Identification and Authentication 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

By establishing user accountability and rules for access, ABC Company mitigates the risks related to unauthorized access to electronically stored information.

# II. Purpose

This policy defines the security requirements for establishing accounts, enabling access to Information Resources, and ensures the user is properly authenticated to access the information.

# III. Scope

This policy applies to Information Resources data owners and security Staff that implement controls to govern access to Information Resources.

# IV. Policy

The Chief Security Officer (CSO) shall ensure that Information Resources are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access controls on Information Resources.

Data Owners for each information system shall be responsible for ensuring that authorization and account management processes exist for their specific application and that the appropriate people have been assigned the responsibility of creating and maintaining the authorization records. The design and development of the authorization and account management processes shall comply with CSO security standards.

Department Heads shall submit user access requests to the appropriate Data Owners. As appropriate, Data Owners shall approve or deny such requests for user access privileges.

System Administrators have the responsibility of periodically reviewing user access privileges and notifying the appropriate Data Owners of any access concerns.

The request for Information Resource Authorization shall adhere to the following requirements:

* Access shall be limited to the Information Resources described on the request.
* The Information Resources shall only be used for the purpose stated on the request.
* A new request will be submitted if there are any changes to the stated conditions of access
* The authorization request must be signed by the applicant and approved by the Department Head.

Access to Information Resources is generally established or reviewed under the following conditions:

* A new Staff member requires access to Information Resources.
* A Staff member has a change in job functions.
* A Staff member is terminated or no longer needs access to certain Information Resources.
* A Staff member requires additional access rights.

Requests for a change in access rights (e.g., to grant or disallow access) shall be accomplished by submitting a new request

When a Staff member is transferred or terminated, the Staff member’s access to Information Resources must be terminated. The Staff member’s records and data, stored locally or in network directories, must be preserved. It is the responsibility of the direct supervisor or manager to contact the Data Owner and the System Administrator when a Staff member is transferred or terminated.

The Data Owner for each information system shall ensure that all user accounts are reviewed and access rights evaluated at least once per year.

User identification and authentication is an access control methodology. At a minimum, ABC Company uses two-factor authentication with an ID and password to determine a user’s identity, ensure it is correct, and establish accountability. User login IDs shall be unique and shall not be shared by Staff members unless special permission is authorized by Executive Management. User selected passwords are required to authenticate the user and grant access to ABC Company Information Resources.

The Chief Security Officer (CSO) shall ensure:

* Sensitive authentication data shall not be stored after authorization even if it is encrypted.
* If sensitive authentication data is received, processes shall render all data irretrievable upon completion of the authorization process.
* Processes permit storing of sensitive authentication data if there is a business justification and the data is stored securely.

Access controls shall be implemented to protect Information Resources. Only IT Department approved access control software shall be used to restrict access to Information Resources. Access to security protection systems shall be limited to security administrators and authorized personnel.

Logical access controls may be implemented on applications and databases. These controls shall have the effect of limiting access to data based upon the principle of least privilege.

The number of consecutive attempts to enter an incorrect password shall be limited to prevent password guessing attacks. After a given number of unsuccessful attempts to enter a password, the ID shall be suspended until reset by a system administrator. Please refer to the Securing Information Systems Policy for more information.

If there has been no activity for a given period of time, the system must automatically either blank the screen or use a screen saver, and restrict access. Re-establishment of access may occur after the user has logged back on to the system. Please refer to the Securing Information Systems Policy for more information.

# 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 Information Resources data owners and security Staff that implement controls to govern access to Information Resources.

**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

GDPR Article 25, 32

HIPAA 64.308(a)(4)(ii)(B-C), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B-C)

ISO 27001:2013 A.6.2.2, A.7.3, A.9

NIST SP 800-37 3.2, 3.6

NIST SP 800-53 AC-1-2, IA-2, IA-4, IA-5, IA-8

NIST Cybersecurity Framework PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-7, DE.DP-2

PCI 6.3, 6.5.8, 8.1-2, 8.8.2