Logical Access Controls 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

This policy controls logical, electronic access to information systems and applications.

# II. Purpose

The purpose of this policy is to define logical access controls as they relate to ABC Company Information Resources. Logical access controls are tools used for identification, authentication, authorization, and accountability in Information Resources. Logical access controls can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems.

# III. Scope

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

# IV. Policy

Without Logical access controls shall be established and documented for all ABC Company Information Resources. The access controls shall be implemented based upon the principle of least privilege.

A Risk Assessment shall be performed for the purpose of identifying Information Resources and sensitive data. A Risk Treatment Plan shall be prepared and updated annually that defines safeguards and controls to protect such Information Resources.

All access to Information Resources shall use an approved method of identification and authentication per the Identification and Authentication Policy. All third party service provider access to the ABC Company network and information systems must adhere to the same access restrictions as internal users.

Access rights shall be established, documented, and periodically reviewed based on business needs and external requirements. Access controls should consider:

* Security requirements given business needs, anticipated threats, and vulnerabilities.
* Relevant legislative and regulatory requirements.
* Contractual obligations and service level agreements.
* Consistency across ABC Company’s systems and networks.

Access control considerations include:

* The use of clearly stated rules and rights based on user profiles.
* Consistent management of access rights across Information Resources using an appropriate mix of logical (technical) and physical access controls.
* Segregation of access control roles including access request by the appropriate department, access authorization by the Data Owner, and access administration by the Network Administrator.
* Requirements for the formal authorization and timely removal of access rights.

All critical Information Resources must limit and enforce access to only the times identified as necessary for completion of ABC Company business processes. All access to these systems and applications at all other times shall be disabled or suspended.

All access to any database containing Sensitive Information (including access by applications, administrators, and all other users) shall be restricted as follows:

* All user access to, user queries of, and user actions on databases are through programmatic methods.
* Only database administrators have the ability to directly access or query databases.
* Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

Sessions that are inactive must be automatically terminated. The amount of time permitted before session termination must be aligned with the criticality of the information. Approved compensating controls, e.g. password protected screensavers or terminal locks, must be activated for information systems and applications that cannot automatically terminate sessions.

All critical information systems and applications must not allow users to have multiple concurrent sessions on the same system.

All information systems must have, or support, password management systems that are interactive and can ensure strong passwords to meet the requirements of the Security Policy.

All information systems must not transmit passwords in clear text and passwords must not be visibly displayed on the system when being entered.

Users given the opportunity to login to information systems must be presented with a login banner that includes a special notice informing the user that the system is to be used only by authorized users and that the use of the system constitutes consent to monitoring.

All Information Systems, databases, and applications that store authentication information such as a user ID and password must be encrypted with access restricted to only authorized personnel.

Utilities that are capable of overriding information system and application controls or performing low-level system maintenance must be approved with additional controls implemented to restrict their use.

# 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 Information Resource security Staff, System Administrators, Data Owners, and the Chief Security Officer.

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

ISO 27001 A.6.2.2, 7.2.1, A.8.1.2-3

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-1-3

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

PCI 7.1-3