Database 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

Databases and the data that they contain must have proper security controls that protect against loss of data or unauthorized access or alteration.

# II. Purpose

The purpose of this policy is to establish the rules for the access and protection of databases. These rules are necessary to preserve the integrity, availability and confidentiality of ABC Company’s databases and data.

# III. Scope

This policy applies to ABC Company Staff who perform network administration, database administration (DBA), or web development duties.

# IV. Policy

A. Access

The Chief Security Officer (CSO) shall ensure Staff must receive prior written authorization before they are permitted to access databases and data.

B. Security Protection

The CSO shall ensure that appropriate security mechanisms are implemented to protect databases from unauthorized access or alteration. Examples of such security mechanisms include:

* Access control policies including password policies
* Information Systems Access Request Form
* Network segmentation
* Network firewalls and web application firewalls
* Router Access Control Lists (ACL)

Software applications that access ABC Company databases must use proper coding and security techniques:

* Database user names and passwords (credentials) shall only be accessible by authorized persons, programs, and processes.
* Credentials must adhere to specifications listed in ABC Company’s Password Policy.
* Access to databases shall be granted only after authentication of proper credentials.
* Database access credentials must not be stored in readable clear text format.
* To reduce the likelihood of unauthorized access, source code credentials must be stored in a separate source file. The credentials file may contain user names, passwords, and any code needed to access the credentials.
* Credentials stored in an external file shall be read from the file immediately prior to use and, immediately after authentication, the memory containing the credentials shall be cleared or released.
* Database authentication may occur programmatically as part of the user authentication process on an authentication server.

# 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 the CSO, Network Administrators, Database Administrators (DBAs), and web developers.

**Policy History**

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

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 32

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

ISO 27001 A.8.1.3, A.9

NIST SP 800-37 3.4

NIST SP 800-53 AC-3, AC-24

NIST Cybersecurity Framework PR.AC-5, PR.AC-7, PR.DS-1, DE.DP-2

PCI 1.1.3, 2.2