**Database Security Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

**DATABASE SECURITY PROFILE 4**

**INFORMATION CLASSIFICATION 4**

**AUTHENTICATION AND IDENTIFICATION 4**

**ACCESS CONTROL** **5**

**CHANGE CONTROL 6**

**MONITORING AND REVIEW 7**

**DATABASE ADMINISTRATOR ROLES AND RESPONSIBILITIES 7 5**

***ENFORCEMENT 8***

**Description**: The purpose of this ***policy*** is to provide information necessary to implement compliance with the CompanyName security objectives which are confidentiality, integrity and availability.

1. **DATABASE SECURITY PROFILE**
	1. This ***policy*** is the property of CompanyName and is intended for internal use only. It should not be reproduced, partially or wholly, in whatever form.
	2. This database security ***policy*** applies to database platforms. If the role is outsourced to a vendor, the vendor must ensure compliance with the identified standards.
	3. Security controls should be implemented based on the level of confidentiality of the data determined by Data Owner.
	4. Database management system should provide accurate and reliable business data as well as preventing unauthorized data modification.
	5. CompanyName should ensure the roles and responsibilities of Database Administrator is established and formalized. Only authorized users are allowed to access business data.
	6. Referring to Application Access Matrix, database application is owned by data Owner and being authorized, approved by senior management. Changes shall be notified to the data Owner and relevant parties.
2. **INFORMATION CLASSIFICATION**

Data is classified to its sensitivity level. This sensitivity level is the level of risk to the Organization if the data is lost or disclosed to unauthorized parties.

1. **AUTHENTICATION AND IDENTIFICATION**
	1. **Username and Password**[[1]](#footnote-1)
		* 1. Access to the database system is controlled through identified, consistent naming convention IDs and password that should be in compliance with the CompanyName Password Management Guidelines.
			2. All naming convention, IDs and password as well as the usage of data should be complied in a data dictionary as a documentation reference.
	2. **Intrusion Avoidance**
		* 1. Account that has been inactive for 30 days should be disabled.
			2. Granting any access for guest account is prohibited.
	3. **Intrusion Countermeasures and Detection**

User’s accounts are to be locked after 3 repeated failed login attempts.

* 1. **Vendor Control**
		+ 1. Accounts created by vendors during the performance of their duties must be temporary and removed immediately upon completion of their work.
			2. All actions performed by vendor are to be logged and audited.
1. **ACCESS CONTROL**
	1. **Authorization, Access Rights and Privilege**
		* 1. All system installation and database files with directories must be protected to prevent unauthorized access.
			2. The respective System Owner shall authorize all user access to database.
			3. The database server and its network components shall be physically secured.
			4. SELECT privilege grants a user’s access on views and tables should be limited to authorized personnel.
			5. All users’ access privileges of database is based on the Application Access Matrix (according to duties segregation), owned by the Data Owner and endorsed by the senior management.
	2. **Audit Trails**
		* 1. Database audit data shall be archived according to the following requirements:-
				1. Daily Back-ups are retained for a minimum of 1 month,
				2. Monthly Back-ups are retained for every 7 years and
				3. Yearly Back-ups are retained for 7 years.
			2. All requests to link database should formally be approved by IT Security Department and relevant parties. Database maintenance utilities that bypass controls should be adequately restricted and monitored.
			3. ***Minimum Audit Information:-***

***The minimum audit trail for a database must be able to provide information on access to a database at any point of time.***

***The following scenarios will require minimum audit trails.***

1. ***Multi-site access (Connections from different IP or point of access) to a database is needed to be audited. The access is through a system (i.e. application server accessing a database server).***
	* ***Failed login***
	* ***Database exceptions***
2. ***Multi-user ID accessing a database. This connection is mainly by individual user (through database client i.e. SQL Plus, Toad or log on locally to the database server)***

***The following audits are suggested.***

* + ***Who logged into the database***
	+ ***Successful login and failed login (authorization failure/non existent users).***
	+ ***Where the connection was initiated from (source)***
	+ ***When the connection was made***
	+ ***What client was used to access the database***
	+ ***What was performed during the connection***
	1. **Availability, Backup**[[2]](#footnote-2) **and Recovery**
		+ 1. Database Administrator shall monitor the database periodically to ensure its availability and maintaining the performance.
			2. Data Administrator should determine the level of required backup and strategy being used (e.g. Full backup, incremental, online or offline backup) for different databases.
			3. Backup files for all databases must be sent to an offsite location for storage.
			4. The DBA shall backup the database periodically according to documented procedures.
			5. Where possible, the database redundancy should be implemented whereby the archive and redundancy are written to multiple physical locations for recovery purposes.
			6. Recovery testing of the off-site backup tapes shall be carrying out o a half yearly basis.

 (Attn: 4.3 (c) and 4.3 (f) is part of IT Security Department requirements)

* 1. **Database User Management**
		+ 1. Privileged Accounts
				1. Database Administrator (DBA) shall not have system administrator rights to the operating system for any server on which a database is installed.
			2. User Accounts
				1. Where possible, all database users should have a unique user account within the database
				2. The use of shared user accounts in the database application is not allowed.
				3. The Database Administrator (DBA) shall not transfer or share administrator account privileges with unauthorized users.
				4. Where possible, database session timeout for accounts should be implemented to mitigate the risk of unauthorized access when the terminal is left unattended.
				5. In the event of changes in job function of the user, the access rights of the user accounts shall be reviewed to ensure that minimum access rights are granted.
				6. All user accounts that have been inactive for 90 days shall be disabled.
			3. Default Accounts
				1. Default fault accounts shall be deleted disabled or removed from the production database management systems.
			4. Creation of Accounts
				1. Requests for creating user accounts and granting access privileges shall be approved by the respective Data Owner.
			5. Deletion of Accounts
				1. All user accounts should be deleted immediately after the user leaves the Organization, unless requested and approved otherwise.
			6. Application and System Development
				1. The database production and development environments shall be segregated.
				2. Developers shall not have an access to the production database.
			7. Operating System security
				1. The operating system where the database is installed shall be secured according to CompanyName platform-specific operating system technical control guideline.
			8. Data Confidentiality Controls
				1. Where possible, database passwords and other relevant authentication information should be appropriately encrypted.
				2. Where possible, “Classified” data (e.g. Customer PIN and Credit Card number) in the database should be stored in encrypted form.
				3. Where possible, database links or connection (e.g. Oracle SSL) should be encrypted.
1. **CHANGE CONTROL**
	1. **Database Change Requests**
		* 1. Any database changes shall be approved by the Data Owner and the relevant parties and a notification concerning about the changes will be sent to the IT Security Department for an updates on the changes made.
			2. Both outsourcer and CompanyName IT Security Department shall assess database changes that are not specific to business application.
			3. The changes specific to business application data (e.g. Database tables, data) shall be tested on the development system prior to implementation on the production system and shall be approved ahead of making any changes.
			4. Changes to the audit trail settings highlighted in this ***policy*** shall require assessment from both outsourcer and CompanyName IT Security Department.
2. **MONITORING AND REVIEW**
	1. **Access Control Matrix Review**

The Data Owner on a half yearly basis shall review the access control matrix. Updated access matrix should be forwarded to the outsourcer.

* 1. **Audit Trail Reviews**
		+ 1. The integrity of business data should be upheld by providing assurance of accuracy and reliability of the database management system as well as preventing unauthorised modification of data.
			2. For all databases, audit trail, error logs and access violation review shall be performed by the Database Administrator periodically and as needed in accordance with the standards.
			3. An independent party who does not have access to the same database shall review audit trails of Database Administrator and Database Security Officer Activities.
	2. **Security Patches**
		+ 1. The Database Administrator shall monitor the availability of database updates and patches releases by the vendors.
			2. Once done with the evaluation on impact on the database, database Administrator shall apply these database updates and prepare the impact analysis documentation to the Data Administrator for concurrence and acceptance.
1. **DATABASE ADMINISTRATOR ROLES AND RESPONSIBILITIES**
	* + 1. A database administrator is responsible for the usage, accuracy, efficiency, security, maintenance, administration and development of an organization's computerized database(s), providing support to some or all departments depending on the size of the organization.
			2. Typical responsibilities are likely to include:-
				1. Ensuring that the database(s) is updated accurately and regularly
				2. Controlling the access, performance monitoring and tuning
				3. Assisting development staff with application design
				4. Identifying and resolving user's problem
				5. Developing and implementing maintenance procedures
				6. Collaborating in the design and development of database to meet new user needs and respond to/anticipate technological innovations
				7. Facilitating and negotiating the increasing demand for access to data-increasingly via an organization's intranet or website
				8. Devising, developing and implementing disaster recovery and archiving procedures
				9. Supporting users by talking then through a search or by customizing the 'front ends' to incorporate new fields for data entry
				10. Capacity planning
				11. Working closely with IT project managers and database programmers
				12. Liaising with web developers to enable on-line database access and resolve associated problems
				13. Planning and coordinating database security measures
				14. Communicating regularly with internal technical, applications and operational staff to ensure the database integrity and security
				15. Commissioning and installing new applications.
2. **ENFORCEMENT**

# All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any CompanyName staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.

# Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.

* 1. CompanyName’s staff must ensure that CompanyName’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.
	2. Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.
1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)