Database Management

Policy Statement

Data stored within the Company's databases is critical and provides valuable information for management decisions. This Policy is aimed at ensuring the integrity, security, consistency and accuracy of the organizational databases by providing database management guidelines. The company should adopt methods to protect the data at rest in all possible ways.

Database should not be accessed via default admin accounts unless there is a business need to do so. Approval should be taken from the GH DT&SP before accessing the database from default admin account. Moreover, the database logs should be monitored and its logs should be protected.

Prerequisite

This procedure should be read in conjunction with:

- Information Security Policies, including
  - Access Control Policy
  - Change Management Policy

Responsibility

- Group Head Digital, Technology and Strategic Planning
- Database Administrator

Procedure

Step	Description	Responsibility
Installation		
1.	Database administrator shall provide database software that shall be approved by Head of IT before installation.	Group Head Digital, Technology and Strategic Planning
2.	All the default passwords of the system supplied accounts present in the database system shall be changed.	Database Administrator
3.	A separate ID with privileges shall be created for use. System supplied or "SYS", "System", "/ as SYSDBA" equivalent access accounts shall not be used for day to day operations.	Database Administrator
Configuration		
1.	Auditing shall be enabled for all sensitive and security related transactions. Moreover, key events like Failed Login and Successful Logins and sensitive table access related events will be logged at a minimum.	Database Administrator
2.	Any change in the database should be approved from team lead Data Management and properly logged as per the logging mechanism.	Manager Database Administrator
3.	Configuration database shall be created having all baselines settings. This database shall be updated upon all configuration changes.	Database Administrator
Operation		
1.	A list shall be maintained of roles and access rights of the authorized database accounts. This list shall be updated whenever required. The list shall include: • Database admin list with assign roles and network IDs • detailed audit logging should be enabled to all uses with "dba" rights. • Sys and system account should not be login or daily basis to perform normal tasks.	Database Administrator
Monitoring		
1.	On random basis, database logs shall be reviewed for any suspicious activity. Any anomaly noted shall be reported to Group Head Digital, Technology and Strategic Planning.	Database Administrator
2.	Logs of privileged user IDs (e.g. DBA) shall be reviewed periodically as per the user access policy.	Team Lead Database Administrator