DATABASE SECURITY POLICY

Digital Personal Data Protection Act, 2023 (DPDPA)

SBS HR

Document Information

Document Title	Database Security Policy
Applicable Framework	Data Privacy Management System (DPMS)
Applicable Regulation	Digital Personal Data Protection Act, 2023
Organization	SBS HR
Version	1.0
Document Owner	Database Administration, Information Security & Compliance Department
Classification	Confidential

Table of Contents

1. Purpose

The purpose of this Database Security Policy is to establish standardized requirements, responsibilities, and controls for protection, configuration, access management, monitoring, backup, maintenance, and secure operation of databases used within SBS HR.

This policy supports compliance with the Digital Personal Data Protection Act, 2023 (DPDPA) and helps ensure confidentiality, integrity, availability, and protection of organizational and personal information stored in database environments.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

2. Scope

This policy applies to:

- Employees
- Consultants and contractors
- Relational and non-relational databases
- HRMS and payroll databases
- Cloud-hosted database environments
- Backup and archival repositories
- Database administration activities
- Third-party managed database systems

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

3. Objectives

The objectives of this policy are:

- Protect databases against unauthorized access or compromise
- Reduce cybersecurity and operational risks
- Ensure secure configuration and monitoring practices
- Support business continuity and resilience

• Meet compliance and audit obligations
• Improve governance and accountability

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

4. Database Security Principles

SBS HR shall ensure:
• Databases are securely configured before deployment
• Access is restricted based on business need
• Database activities are monitored appropriately
• Sensitive information is protected from unauthorized disclosure
• Security incidents are reported and addressed promptly

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

5. Secure Configuration Requirements

Databases shall:
• Use approved secure baseline configurations
• Disable unnecessary services and default accounts
• Restrict insecure settings or features
• Follow hardening and patch management requirements

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

6. Access Control Requirements

Access to databases shall:

- Follow least privilege principles
- Require formal authorization
- Use secure authentication mechanisms
- Be role-based where applicable
- Be periodically reviewed and monitored

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

7. Privileged Database Access

Administrative or privileged database access shall:

- Use enhanced authentication controls
- Support multi-factor authentication where applicable
- Restrict shared or generic administrative accounts
- Be monitored and logged appropriately

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

8. Data Protection & Encryption

Sensitive or personal information stored in databases shall:

- Use encryption where applicable
- Restrict unauthorized disclosure or extraction
- Support secure storage and transfer mechanisms
- Follow approved retention and disposal requirements

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

9. Backup & Recovery Requirements

Databases shall:

- Follow approved backup procedures
- Support restoration and recovery testing
- Protect confidentiality during recovery operations
- Maintain operational resilience

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

10. Patch & Vulnerability Management

The organization shall:

- Apply database security patches appropriately
- Conduct vulnerability assessments periodically
- Track remediation activities and unresolved risks
- Restrict unsupported or vulnerable database systems

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

11. Logging & Monitoring

The organization may monitor:

- Authentication and access activities
- Database queries and administrative actions
- Security events and anomalies
- Data modification and deletion activities
- Unauthorized access attempts

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

12. Network & Communication Security

Database communication activities shall:

- Use secure communication protocols
- Restrict unauthorized network exposure
- Follow approved firewall and segmentation controls
- Protect against unauthorized interception or access

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

13. Third-Party Database Management

Third parties managing organizational databases shall:

- Follow approved contractual obligations
- Maintain confidentiality and security safeguards
- Support audits and compliance reviews
- Report incidents promptly

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

14. Incident Reporting

Employees and stakeholders shall immediately report:

- Unauthorized database access attempts
- Data leakage or suspicious extraction activities

• Database vulnerabilities or misconfigurations
• Operational disruptions or outages
• Confidentiality breaches

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

15. Documentation Requirements

The organization shall maintain records related to:
• Database inventories and configurations
• Access and monitoring activities
• Backup and recovery operations
• Incident and audit records
• Corrective actions and exceptions

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

16. Employee Responsibilities

Employees shall:
• Follow approved database security procedures
• Avoid unauthorized access or modifications
• Protect confidentiality of organizational information
• Report incidents promptly
• Cooperate during reviews and audits

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

17. Database Administration Responsibilities

The Database Administration, Information Security, and Compliance Teams shall:

- Monitor database security compliance
- Conduct reviews and assessments
- Maintain related documentation
- Support audits and investigations
- Track corrective actions

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

18. Awareness & Training

Applicable personnel shall receive awareness training related to:

- Secure database administration practices
- Access control and encryption requirements
- Incident reporting procedures
- DPDPA compliance responsibilities

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

19. Audit & Compliance Monitoring

Compliance with this policy shall be monitored through:

- Internal audits
- Database security reviews
- Security assessments
- Compliance monitoring
- Corrective action tracking

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

20. Non-Compliance

Violation of this policy may result in:

- Disciplinary action
- Regulatory exposure
- Legal consequences
- Contractual penalties
- Restriction or suspension of administrative access

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

21. Continual Improvement

This policy shall be periodically reviewed and improved based on:

- Audit findings
- Incident and threat trends
- Regulatory updates
- Technology and operational changes
- Improvement opportunities

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

22. Approval

This Database Security Policy is approved by Top Management and shall be communicated to all applicable stakeholders.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

All database security activities shall be implemented in accordance with approved organizational procedures, privacy governance requirements, information security safeguards, operational controls, and DPDPA obligations.

Approval & Authorization

Prepared By	Reviewed By	Approved By	Date
Network Engineer	DPO	Director	April 1’st - 2026