Database Security Policy

V1.0

TLP: CLEAR

THE TRAFFIC LIGHT PROTOCOL (TLP)

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). The protocol includes four colors (traffic lights), which are detailed as follows:

Red- Not for disclosure, restricted to participants only:
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed

Amber- Limited disclosure, restricted to participants' organizations:
Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Green- Limited disclosure, restricted to the community:
Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Clear- Disclosure is not limited:
Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP:CLEAR information may be distributed without restriction.

TABLE OF CONTENTS

POLICY REVISION HISTORY

AUTHOR	DESCRIPTION	VERSION	DATE
(EG-CERT)	RELEASE DATE	1.0	
(EG-CERT)	EFFECTIVE DATE	1.0	
	REVIEW DATE		
	REVISION DATE		

SIGN-OFF

SIGN-OFF LEVEL	DATE	NAME	SIGNATURE
Top management			
Executives			
Security Director			
IT Director			
Internal Audit Team Director			

1. POLICY OVERVIEW

This document establishes “the Organization’s Database Security Policy” that outlines the rules governing the protection and security of information in databases (or “database management systems” (DBMSs)).

1.1 PURPOSE

This policy has been developed in order to establish the baseline protection and security controls for secure database systems.

1.2 SCOPE

This Policy applies to database systems used in the provision of the organization’s services.

1.3 MANAGEMENT COMMITMENT

IT and Security Directors have reviewed and approved this Policy and the Top Management supports the purpose thereof. Disciplinary action may be taken against any employee violating this Policy; this might include the suspension of the violating employee, restrictions on his access to some systems or information, or more severe penalty, including, but not limited to, the employee’s termination.

1.4 COMPLIANCE WITH INTERNATIONAL POLICIES

This Policy has been set based on ISO 27001, NIST Special Publication (SP) 800-53 (Rev. 5), the Database Security Standard for Information Protection (DSSIP), the Database Management System Security Standard (SS-05) standard and complies as well with ISO 27002 Best Practices for Information Security.

2. POLICY DEFINITIONS

Database Management System (DBMS):

Is a general-purpose software that enables users to create, define, query, update, and manage a database.

Production Database:

Refers to the information that is constantly stored and used to conduct business tasks and processes. It must be accurate, documented and it should be managed on a continuous basis to guarantee its worth to the organization.

Data masking:

Is a technique used to conceal, replace or obscure (obfuscate) sensitive data and information. In fact, “Data Masking” could be static (when a data item is hidden (masked) in the original database), dynamic (when automation and relevant rules are used in order to secure data in real-time) or on-the-fly (when data are masked in the memory of the application server they reside in).

Segregation of Duties:

Is a security principle that divides critical functions among different staff members in an attempt to ensure that no one has enough information or access privilege to perpetrate damaging fraud crimes.

Data at Rest Encryption

Refers to the encryption of the data stored in the databases that are not transferred through networks, including offline backups.

Data in transit

It represents the data transferred from one place to another.

3. ROLES AND RESPONSIBILITIES

Stakeholder	Responsibilities
Top Management	• Approves and officially endorses this Policy. • Issues administrative instructions that are binding on all organization's employees to implement the policies, and set the regulation of disciplinary penalties related to the employee's failure to implement these policies, in a manner that does not conflict with the applicable regulations and laws.
Executives	• Reviews and officially endorses this Policy.
Security Team	• Sets security plans, procedures, policies and measures in collaboration with the IT Department. • Reviews and updates this policy periodically. • Implements and reviews the mechanisms needed to endorse this Policy. • Maintains the security and protection of systems and data. • Manages, updates and follows up on the tools that maintain system and data security. • Collaborates with IT and Internal Audit Teams to secure the organization's digital assets. • Rejects or approves any necessary exceptions to this Policy.
HR Team	• Ensures that all employees are aware of the organization's security policies. • Specifies the information security responsibilities and confidentiality clauses in contracts.
IT Team	• Collaborates with the Security Team to issue the plans, procedures and measures needed for the implementation of this policy. • Informs all organization's employees of their security duties and responsibilities before giving them access to sensitive data and systems. • Implements the necessary mechanisms requested by the Security Team.

Stakeholder	Responsibilities
Internal Audit Team	• Carries out an internal audit of the security controls of the policy and its efficiency. • Assesses and consolidates the organization's readiness for encountering any cyberattacks. • Assesses and manages risks. • Ensures the compliance with policies and standards.
Managers	• Ensures that the employees concerned are familiar with this policy.
Employees	• Employees must implement this policy and act in accordance therewith.

4. DATABASE SECURITY POLICY CONTROLS

4.1 GENERAL SECURITY REQUIREMENTS

- All server operating systems must be secured and hardened.
- Network devices and networks must be hardened, managed and controlled to ensure information protection.
- Non-secure services or unencrypted protocols (HTTP, FTP, etc.) must be avoided.
- Unnecessary ports or services must be removed or disabled, whenever possible.
- Protective controls (such as intrusion detection systems, firewalls, anti-malware solutions, etc.) must be implemented.
- Technical security evaluations should be carried out (such as penetration testing, vulnerability assessments, cyber response exercises, and cyber-attack simulations).
- A well-known incident reporting mechanism should be developed to enable the reporting of any suspected or monitored information security incident.
- Any suspected or monitored information security incident should be reported to the incident handling team within a definite time frame.
- Cybersecurity responsibilities and confidentiality clauses must be specified in employment contracts to ensure the confidential information protection.
- Physical security controls should be established to protect information assets.

4.2 INFORMATION SECURITY TRAINING

- Information security training must be provided regularly to protect the organization's information assets.

4.3 SECURE DATABASE PLAN AND REQUIREMENTS

- Information Security requirements must be determined in any plans for any systems of databases that will be created or updated. These requirements should include confidentiality, integrity and availability.
- All databases must be hosted on servers that do not carry out any other function such as "web application" function.
- The security risks associated with special databases should be determined, and the appropriate solutions should be developed.
- The suitable security controls must be developed and implemented to protect confidential information in the databases.
- Duties must be segregated with different privileges so that no single personnel or team becomes completely responsible for all the processes of databases; this entails the implementation of "segregation of duties" principle.
- The usage of actual business data kept in databases should only be allowed in testing environments as per business needs, taking into account the implementation of the proper security controls

4.4 ASSETS MANAGEMENT

- An asset inventory of information and other relevant assets must be developed and maintained.
- The asset inventory of information and other relevant assets to databases must be regularly reviewed and updated and during the installation, change or removal of an asset.
- More than one asset inventory of information and other relevant assets can be developed, such as asset inventories of hardware, software, databases, and virtual machines (VMs), etc.
- The asset ownership, whether databases or relevant assets, should be assigned to a group or an individual.
- The asset owner is responsible of the appropriate management of an asset throughout its life cycle, and should make sure that:
  - The information and other relevant assets are included in the asset inventory;
  - The information and other relevant assets are properly classified and secured;
  - The classification is reviewed on a regular basis;
  - The components supporting the technology assets are identified and should be linked together, as for example databases, storage, software components and sub-components;
  - The requirements for the appropriate usage of information and other relevant assets are in place;
  - The security restrictions imposed on access to databases and systems are compatible with the classification; and are adequate, appropriate and, reviewed on a regular basis;
  - Information and other relevant assets are securely handled and removed from the inventory when deleted or discarded;
  - The asset owners are involved in determining and managing risks associated with their assets).

4.5 INFORMATION CLASSIFICATION AND LABELING

- Data in databases should be classified as per the security requirements and protected according to that security classification.
- An appropriate set of Information labeling procedures should be established and implemented as per the information classification plan approved by the organization.

4.6 DATA LEAKAGE PROTECTION

- Data leakage preventive measures should be implemented to prevent data leakage.
- Data Masking techniques should be used to hide, replace, encrypt or obscure (obfuscate) sensitive data items to reduce the exposure of sensitive data to any risks.
- Restrictions should be imposed on data transmission over network or user actions that expose sensitive information to risks, as for example, copying database entries into a spreadsheet.

4.7 DATABASE SECURITY OPERATIONS

- Authentication and authorization procedures must be set, and used in granting or rejecting access to databases.
- After installation, accounts, codes, files, examples, and virtual objects that are no more needed must be deleted from the database management system (DBMS) and the operating system.
- It should be verified that the production environment is separated from the testing environment.
- Changes to database systems should be consistent with the organization's Change Management Control processes.
- The security operation procedures and responsibilities should be established, documented, maintained and implemented for databases.
- Database patching process should be carried out regularly and in a timely manner.
- Data transfer from databases must be officially documented and restricted to previously specified business activities.
- The privileged users of databases should be monitored and reviewed to check the extent of their compliance with the cybersecurity rules.

4.8 HARDENING DATABASE CONFIGURATIONS

- Data should be validated and inputs should be checked to restrict database management system (DBMS) transactions.
- It should be ensured that the server-side scripting is disabled, so long as it is no more needed.
- Passwords should be managed; the default passwords should be changed and blank passwords use should be rejected.
- Databases must be configured so that connection is established through authorized network interfaces only.
- Database management system (DBMS) Versions must be supported by the vendor; they should be updated and patched regularly.
- Role-based access controls must be activated and configured appropriately.

4.9 DATABASE DATA ENCRYPTION

- Data must be encrypted both in transit and at rest.
- All encryption materials needed for secure communications must be accessible in read-only access mode.
- All stored data and encrypted channels must not employ a sample or default certificate.
- All encryption keys must be generated for a specific use case and be well-secured.
- All encryption certificates must be checked and authenticated by both the Certificate Authority (CA) and the service provider.

4.10 DATABASE LOGGING REQUIREMENTS

- The clocks of all applications must be synchronized with the underlying operating system clock.
- The database settings must be configured in order to log, capture and alert on key data and database activities as a minimum the following:
  - Logging and alerting when confidential or personal information is accessed;
  - Logging data processing activities (such as, insertion, deletion and change);
  - Logging and alerting on security activities (such as, users' creation/deletion);
  - Logging and alerting on high-risk database activities (such as, turning on/off auditing), unusual or suspicious activities.

4.11 DATABASE BACKUP AND DISASTER RECOVERY

- Database systems must be backed up regularly.
- It should be ensured that all databases are backed up.
- Replication slave backups must be carried out for all database systems.
- It should be ensured that an up-to-date Disaster Recovery Plan (DRP) is developed; and the needed skills and resources must be provided and employed appropriately to attain business objectives.
- Appropriate business continuity plans should be developed to ensure disaster recovery in case incidents or malware attacks occur. This includes all essential data and software backup (both online and offline backup) and data recovery procedures.
- The backups must be stored in a safe and well-secured remote location, at a sufficient distance to avoid any damage ensuing from a disaster at the main site;
- Regular tests should be carried out for backup media to ensure their reliability for emergency use when required.
- Backups should be protected by encryption as per the identified risks.

4.12 POLICY EXCEPTIONS

The security team must be informed of any proposed changes to be made to the system; the endorsement of any exception to the fundamental controls principles stipulated in this Policy must be documented and formally approved by the IT Director. Policy exceptions must determine:

- The nature of the exception;
- A realistic clarification of the necessity of the Policy exception;
- Any risks ensuing from the Policy exception;
- Evidence of the IT Director's approval of this exception.