Database Security Standard

Version 1.3

Reference: 6.100 – Information Technology and Security Policy
6.101 – Use of County Information Technology Resources
6.107 – Information Technology Risk Assessment
3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information
County Fiscal Manual (CFM)

Developed by: Application Security Engineering Team

TABLE OF CONTENTS

1.0 PURPOSE

To protect the confidentiality, integrity and availability of County databases. This standard document establishes the minimum levels of database security for County Information Technology (IT) resources. Although the focus is based on industry best practices for minimum security, departments are encouraged to go beyond the minimum requirements as suited to the business need.

2.0 RELEASE NOTES AND HISTORY LOG

The content in this document will be periodically updated to reflect the changes in the County environment. In addition, this document will be constantly maintained to capture industry best practices as the technology and standards continues to evolve.

DATE	NEW VERSION NUMBER	MODIFIED BY:	DESCRIPTION of CHANGE
11/1/11	1.0	Soheil Naimi (LASD)	1) Created first draft of standard
2/19/13	1.1	Policy Committee	
1/28/14	1.2	Application Security SET	Document review
12/13/16	1.3	Application Security SET	Document refresh
4/11/17	1.3	Application Security SET	Final review
7/11/17	1.3	Application Security SET	Completed final review

3.0 OVERVIEW

Each Departmental Information Security Officer (DISO), or designee, must ensure that all applicable federal and state regulations, as well as, County and departmental IT security policies, standards, and procedures are met.

This standard is applicable to all County and third-party provided databases, whether they are hosted internally in the County network or externally.

The following industry best practices were considered for the standard:

- Ensure physical database security
- Separate the database and web servers
- Keep patches current
- Use web application and database firewalls
- Encrypt stored files and backups
- Manage database access tightly
- Audit and monitor database activity

The checklist must be followed whenever the database is initially configured or reconfigured to accept significant additional functionality or to store or access data of greater sensitivity, and updated as required.

The settings in this Standard are grouped into two categories, “Mandatory” and “Addressable.” These categories are defined as follows:

Mandatory – All Mandatory settings must be applied.

Addressable – The "addressable" designation does not mean that an implementation specification is optional. However, it permits entities to determine whether the addressable implementation specification is reasonable and appropriate for that entity. If it is not, the entity must adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate. Exceptions to settings in this category must have documented justification for the exception from the Departmental Information Security Officer (DISO).

4.0 DATABASE SECURITY CHECKLIST

	Requirements	Mandatory	Addressable	Comments
1.0	**Authentication**			
1.1	Authentication is required in order to access the database.	**X**		
1.2	Database passwords must conform to the LA County "Password Security Standard" as published on the Countywide Information Security Website.	**X**		
1.3	The default database administrator account (e.g., 'sa', 'SYS') should only be used for initial setup. All data and maintenance access must use non-default accounts.	**X**		
1.4	To improve access control, the database shall use Active Directory or a similar directory service to authenticate users.		**X**	
1.5	Network traffic containing authentication credentials must be encrypted.	**X**		
1.6	All connections to databases must be authenticated.	**X**		
2.0	**User Access Controls**			
2.1	Databases shall enforce the principle of least privilege.	**X**		
2.2	Review and update user access rights at least quarterly and when a job assignment changes. (CFM 8.7.4.2)	**X**		
2.3	Appropriate access must be implemented for links between databases.	**X**		
2.4	Review all ports and database connections to ensure only necessary ports are opened.	**X**		
3.0	**Encryption**			
3.1	Confidential/sensitive information at rest (including backup media) must be encrypted or obfuscated.	**X**		
3.2	Confidential/sensitive information in transit must be encrypted.	**X**		
3.3	All encryption keys or decryption mechanisms must be safeguarded.	**X**		
4.0	**Auditing**			
4.1	Database must log relevant security events (e.g., login attempts, privilege escalation, database configuration changes, critical object access)	**X**		
4.2	All requests and/or transactions denied based on security privileges must be logged across the databases.	**X**		
4.3	Database must provide an immediate real-time alert to appropriate support staff of all audit failure events requiring real-time alerts.		**X**	

4.4	Access to the location where the logs are stored must be restricted to authorized users only.	**X**		
4.5	An appropriate retention period must be specified for all security logs as required by applicable laws, regulations, and security policies.	**X**		
5.0	**Physical Security**			
5.1	All production database servers must be located in a Data Center facility or secure location with limited physical access.	**X**		
5.2	Database backups stored on tape, disk, or other media must be stored in an appropriately secured location.	**X**		
5.3	For repurposing and disposal, follow the County's guidelines (e.g., Media Disposal standard, BOS IT Security Policy #6.112)	**X**		
6.0	**Database Hardening**			
6.1	Do not place databases in the network DMZ	**X**		
6.2	All database servers must be located on a firewalled server segment.	**X**		
6.3	Remove any features not in use otherwise disable.	**X**		
6.4	Change default ports.		**X**	
6.5	Limit the privileges of the operating system accounts (administrative, root-privileged or DBA) on the Database server to the least privileged method needed for the required tasks.	**X**		
6.6	Segment databases (e.g., production, test, QA, development) on the network to restrict access.	**X**		
6.7	Monitor security related logs for any security breaches or attempted breaches.	**X**		
6.8	Ensure database software is upgraded to the latest supported version and patch level to minimize vulnerabilities and risks.		**X**	
6.9	Run a vulnerability scanner on the database.		**X**	
6.10	Databases directly accessed by internet servers should be segmented from intranet assets.		**X**	
7.0	**Backup and Recovery**			
7.1	All databases must have backup in place to prevent loss of data reflecting the criticality of the system and business needs.	**X**		
7.2	Backup must be tested to ensure the data is recoverable.	**X**		
7.3	All encryption keys or decryption mechanisms must be backed up separately.	**X**		

5. REFERENCE

1. NIST Special Publication 800-123 “Guide to General Server Security”

2. Los Angeles County Board Of Supervisors Policy Manual Chapter 6 – Information Technology

3. County Fiscal Manual (CFM) Chapter 8 – Information Technology Controls