Division of IT Security Best Practices for Database Management Systems

	Notes and Reference Documents	Acceptable Verification Method
1. Protect Sensitive Data		
1.1. Label objects containing or having dedicated access to sensitive data.		
1.1.1. All new SCHEMA/DATABASES developed by University staff for University developed applications shall contain a label to indicate their sensitivity.	Containers of Tables/Users/Procedures ie… Databases/Schemas/Views shall be labeled with a suffix like **_L#** indicating the highest DCS level contained in the Database/Schema/View.	Manual inspection of the catalog of containers.
1.1.2. In University Developed legacy systems lacking labeling alternate representations of the data including the labels shall be created as new requests are generate.	All new grants of access to a legacy system shall only be given to properly labeled objects. The DBA shall create new schemas / views as needed to accomplish this.	Manual inspection of the catalog of containers.
1.1.3. In 3rd party developed systems lacking labeling alternate representations of the data including the labels shall be created when feasible.	All new grants of access to 3rd party developed system shall only be given to properly labeled objects where feasible. If this is technically infeasible or operationally impractical then an explicit exception must be granted to this system.	Manual inspection of the catalog of containers.
1.1.4. All application or service accounts shall include a label indicating the highest level of data the account has access to at the time of creation.	New application or service accounts shall be created including a suffix like _L# indicating the highest level of data they have access to.	Manual inspection of database user accounts.
1.2. Implement Encryption at Rest.		
1.2.1. Column level encryption may be instead of full database encryption as long as it is implemented consistently on all columns containing sensitive data.	All columns containing the following data types must be encrypted in the database if the whole database cannot be encrypted. • SSN • Credit Card Numbers • HIPPA Protected Medical Information	Manual inspection of database encryption settings.
1.2.2. Encryption must be implemented in back-up tapes	Any off-line copies of the database whether a static dump file, or	Manual inspection of

or storage devices if backup tables/columns are not inherently encrypted.	database generated backup copy must either retain the encryption resident in the database or must use a secondary mechanism to encrypt the off-line data.	off-line copies, or encryption procedures.
1.2.3. Decryption/Restoration procedures must be documented and practiced annually.	The procedure to restore the encrypted data to a new platform from back-up must be documented and practiced as a part of annual disaster recovery procedure.	Review of disaster recovery practice logs.
1.3. Implement Encryption in Transit.		
1.3.1. Client-server based encryption must be implemented whenever possible.	Any built-in strong client-server based transmission encryption available to the system shall be enforced at the database level.	Manual inspection of the database configuration.
1.3.2. IPSEC based encryption must be implemented where client-server encryption is not possible.	IPSEC client to server encryption on the database access port(s) must be used when the database management system does not inherently enforce encryption.	Manual inspection of the server network configuration.
2. Configure Audit Logging		
2.1. Log Management.	Audit logs must be retained for forensic and troubleshooting purposes.	
2.1.1. Audit logs must be retained in an active readily searchable format for 90 days.	The searchable audit logs may remain live in the same repository they were initially generated in, or may be archived to some other repository as long as they are readily searchable by scripts or native tools.	Manual inspection of the audit log repository.
2.1.2. After 90 days logs may be archived to a less accessible format as long as they are still accessible for an additional 9 months.	After 90 days log entries may be archived to back-up tape, CD, DVD or other archival media and retained for an additional 9 months.	Manual inspection of the audit log repository.
2.1.3. Audit logs must be destroyed after 12 months.	When the archived logs reach 12 months they must be destroyed by magnetically erasing tapes, shredding CD / DVD copies, or other means that assure the data may not be retrieved.	Manual inspection of the audit log repository.
2.1.4. Audit log records must be stored on a central log repository.	All audit logs must be stored in a central log repository. This does not require that all logs be stored in the same central repository if logging is incompatible between different database management systems.	Manual inspection of audit log settings.
2.1.5. Audit log records must be stored outside of the database management system they are generated on.	The audit logs may be stored in the local file system or in tables on a remote system, but cannot be retained in the same database management system they are generated on.	Manual inspection of audit log settings.

2.1.6. Audit log generating and receiving systems shall be time synchronized to the same source.	All systems containing database management systems shall be time synchronized to the Universities central time system currently time.missouri.edu.	Manual inspection of system settings.
2.2. Log Events		
2.2.1. Audit Log events shall contain at least a minimum set of information to perform forensic analysis or troubleshooting.	The minimum set of data shall include 2.1.1.1. Source IP address or host name of connection 2.1.1.2. Account attempting operation 2.1.1.3. Date/Time stamp of event 2.1.1.4. Type of event 2.1.1.5. Event details	Manual inspection of audit log items.
2.2.2. Audit log events must not contain actual values from sensitive columns.	The audit logs must not contain sensitive data. In the event that they must contain sensitive data then the shall be held to the same security standards as the sensitive data itself.	Manual inspection of audit log items.
2.2.3. Audit logging must be enabled to store key database management events and events that indicate attempted intrusion on the system.	At a minimum audit logging shall include the following 2.2.3.1. Database Query or Command Errors 2.2.3.2. Connections 2.2.3.3. Creation and Deletion of Objects 2.2.3.4. Privileged Actions 2.2.3.5. Access to Audit Logs If operationally feasible the following additional events should be audited. 2.2.3.6. Select, Insert, Update on Level 3 Data Columns	Manual inspection of the audit log configuration.
2.2.4. Audit logs must be reviewed on a daily basis.	At a minimum time must be scheduled each day to review audit logs. If operationally feasible, error conditions should be reported to the database administrator in real-time.	Interview of DBA review of internal procedured
3. Enforce Least Privilege		
3.1. All Schema /Database ownership should be delegated to an account explicitly created for that Database/Schema and should not be left as root/superuser .	Specific accounts should be created to act as the owner of all Databases/Schemas in use in the system.	Manual inspection of permissions
3.2. All access to operating system commands or the ability	Direct access to operating system level commands should be	Manual inspection of

to execute programs on the system must be strictly prohibited unless a documented business purpose requires it.	disabled or removed. If this is not possible, then only those commands that must be allowed should be enabled.	permissions
3.3. All stored procedures or other internal database methods to execute operating system commands must be removed or disabled based on vendor best practice.	Access to any stored procedures or other commands that would allow direct operating system access should be strictly limited to those accounts with a defined business need.	Manual inspection of permissions and configuration
3.4. All access to database service network ports must be strictly controlled at the server and network level, showing a documented business need for the port to be accessible.	Only those services that require external access via the network should be exposed to the network. Those that must be exposed should have explicit limits set to reduce their scope to the minimum number of systems possible.	Remote inspection of open ports
3.5. All access to the Database Catalog/Data Dictionary must be controlled removing any PUBLIC or ANONYMOUS access and granting only explicit permissions as needed.	All access to the catalog of database objects should be revoked and only those accounts that require access should be granted to the specific components of the catalog that are required.	Manual inspection of permissions and configuration
3.6. Account Privilege Assignment		
3.6.1. System Administrators shall not have root/superuser access to databases except when required to perform emergency procedures or scheduled maintenance.	The system administrator may have an account that can authenticate to the database, but that account should not have root/superuser access to the database management system except when required for specific maintenance.	Manual inspection of permissions and configuration
3.6.2. Database Administrators shall not have root/superuser access to the operating system except when required to perform emergency procedures or scheduled maintenance.	The database administrator may have an account that can authenticate to the operating system, but that account should not have root/superuser access to the operating system except when required for specific maintenance.	Manual inspection of permissions and configuration
3.6.3. Service / Application Accounts shall only have access to Schemas/Databases explicitly documented for their use.	Any service or application accounts with access to objects within the management system may only be given privileges to specific schemas/databases required for the application or service to run properly.	Manual inspection of permissions and configuration
3.6.4. Individual User Accounts shall only have access to Schemas/Databases explicitly documented for their	Any individual accounts with access to objects within the management system may only be given privileges to specific schemas/databases that they have an explicit business purpose to	Manual inspection of permissions and configuration

use.	interact with.	
4. Enforce Account Security		
4.1. The database shall enforce a password policy that, at minimum, matches the current Active Directory password policy http://doit.missouri.edu/accounts .	4.1.1. To ensure complexity, all passwords must have eight to 26 characters and include at least one character from at least three of the following: 4.1.1.1. Lowercase letters: a - z 4.1.1.2. Uppercase letters: A - Z 4.1.1.3. Digits: 0 - 9 4.1.1.4. Special characters: ? . , _ - ~ + = $! A password cannot: 4.1.1.5. Be a word found in the dictionary 4.1.1.6. Be the same as your PawPrint 4.1.1.7. Contain MU-related terms (tiger, Truman, Jesse, etc.) 4.1.1.8. Contain spaces or symbols other than the special characters above 4.1.1.9. Contain personal or directory information (Social Security number, employee ID, etc.) 4.1.2. Accounts shall be locked out after 5 bad attempts and remain locked out for 30 minutes. 4.1.3. Password history shall be enforced to include the 24 previous passwords.	Manual inspection of password restrictions
4.2. Application / Service accounts shall be used exclusively by the application or service they were created to support.	Application or service accounts may not be used by individuals for easy access to data or configured in an application or service they are not documented to be associated with.	Manual inspection of permissions.
4.3. The database shall use the most secure and feasible method provided for by the database management system.	The database management system shall be configured to use the vendor recommended secure authentication method.	Manual inspection of database configuration.
4.4. Account Clean Up.		

4.4.1. Database access shall be periodically reviewed.	A process must exist to retrieve the following data on a periodic basic for each account in the management system. 4.4.1.1. Account Status (enabled / disabled) 4.4.1.2. Last Password Change 4.4.1.3. Last Login	Manual inspection of user attributes
4.4.2. Only internal accounts which are actively using database resources shall persist in the database system.	Accounts without any activity in the past 180 days shall be locked and locked accounts will be deleted after 5 weeks unless the deletion of the account will delete critical business data. In this case all rights to data shall be revoked if possible.	Manual inspection of user attributes
4.4.3. External accounts will only be authorized to access data if they are actively in use.	Accounts without any activity in the past 180 days shall have their login access revoked after 5 weeks all permissions will be removed.	Manual inspection of user attributes
5. Secure the Default Configuration.		
5.1. Default User Accounts.		
5.1.1. The passwords for any default user accounts must be reset to meet the requirements of section 4.1.	See section 4.1	Manual inspection of user attributes
5.1.2. If possible default user accounts must be disabled, expired or deleted.	Use the vendor security guidelines to determine the appropriate method for disabling default accounts.	Manual inspection of user attributes
5.2. Install / Enable Only What is Required.		
5.2.1. Only services required to meet documented business purposes may be installed.	All services enabled on the database management system must have a documented business purpose. If unneeded services are installed by default they must be removed or disabled if removal is not possible.	Manual inspection of installed services
5.2.2. Only features required to meet documented business purposes may be enabled on installed services.	Any features that are a part of installed services that are not required for a documented business purpose should be disabled as recommended by the vendor.	Manual inspection of configured features
6. Vendor Specific Guidelines.		
6.1. The database shall be configured according to any additional best practices provided by the vendor.ecurity.	Any additional guidance related to securing a particular database management system shall be implemented unless it conflicts with a documented business purpose.	See appropriate guide

References:

"A Security Checklist for Oracle9*i*." Oracle White Paper. March 2001.

Beauchemin, Bob. "SQL Server 2005 Security Best Practices – Operational and Administrative Tasks." Microsoft. March 2007.

Kiely, Don. "SQL Server 2005 Security Overview for Database Administrators." Microsoft. January 2007.

Baylis, Ruth and Kathy Rich. "Oracle 9*i* Database Administrator's Guide Release 2 (9.2)" Oracle. March 2002.

"Payment Card Industry (PCI) Data Security Standard Security Audit Procedures Version 1.1", Payment Card Industry Security Standard Council. September 2006.

"Trusted Computer System Evaluation Criteria (Orange Book)." United States Department of Defense. December l985.

"BPM-911 Electronic Records Administration." University of Missouri. June 2006.