



COMPLIANCE COMPONENT

Last Updated: 8/3/05

DEFINITION	
<i>Name</i>	Database Management Systems (DBMS) – Security
<i>Description</i>	<p>Security within the DBMS protects the integrity of the data, records and databases. It can provide encryption protection at the data level and allows organizations to have another layer at which to manage and control all access to the information.</p> <p>Major elements of DBMS security include user authentication, user authorization, encryption of data and/or user-id and password, and the auditing user actions.</p> <p>NOTE: All elements of DBMS Security are implemented in concert with and to further support the overarching processes, protocols, standards and procedures outlined within the Security Domain of Missouri’s Adaptive Enterprise Architecture. For specific details regarding standards for user authentication, user authorization, encryption of data and/or user-id and password, and auditing user actions please see the documentation provided within the Security Domain.</p>
<i>Rationale</i>	Without database security, the database and/or data can easily become corrupted, whether intentional or not. It is important to restrict access to the database from unauthorized users to protect sensitive data.
<i>Benefits</i>	<p>Database security provides:</p> <ul style="list-style-type: none"> • Protection of data independent of the application, programming language, database tools, etc. • Protection against potential legal actions relating to data integrity or privacy issues. • One layer of the ‘defense in depth’ strategy of the Security Domain. • Privacy of information passing over the public networks. • Auditing and enforcement of licensing contracts. • Notification of potential intrusion attempts.
ASSOCIATED ARCHITECTURE LEVELS	
<i>Specify the Domain Name</i>	Information
<i>Specify the Discipline Name</i>	Database Management
<i>Specify the Technology Area Name</i>	Database Management Systems
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Standard
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p>DBMS can / will provide authentication and support the ‘defense in depth’ strategy of the overarching state security protocols specified by state security standards.</p> <p>Authenticating users is the basis for providing accountability. Allowing only authenticated users to access system resources protects those resources from</p>

inappropriate access. Authentication is a way of implementing decisions about whom to trust. Authentication methods seek to guarantee the identity of system users: that a person is who he/she says he/she is.

NOTE: For specific password criteria please see Security Domain standards. The items identified below are typical of the specifics addressed by the Security Domain:

DBMS-based Authentication

Shall

- Not allow users to share user-ids
- Require strong/complex passwords
- Require separate sign-ons for separate systems
- Require user to always enter a password
- Prevent reuse of passwords N number of times
- Not store passwords in unsecured files
- Require password expiration
- Require minimum length requirement on passwords
- Remove authorities for user-ids when individuals leave employment

A user's function within an organization determines his or her authorized level of access to applications, system resources and the database. The user's authorizations can be set at the database level by granting privileges and roles to the database user-id and by setting the appropriate access controls on specific database objects. Authorization capabilities are handled by the DBMS, authorization criteria are determined by business management.

DBMS-based Authorization

Shall Support

- Limitation of user's ability to only the tasks that he/she needs
- Granting of data access only to those who need it
- Limited access to smallest number of people necessary to do job/task
- Production data changes occurring only through tested applications that ensures adherence to business rules

Should

- Modify user access as individual's job requirements change

Encrypting sensitive data passing over public network segments or otherwise open networks ensures privacy. Encryption is primarily a defense against unauthorized operation system (OS)/file-system access to database data. By encrypting critical data within the database, even if DBMS files are breached at the OS level, critical data remains encrypted and unreadable. Encryption is a technique of encoding data, so that only authorized users can understand it. Encryption standards and best management practices have been outlined by the Security Domain.

DBMS-based Encryption of data

Shall support

- Encrypting of sensitive data (e.g., SSN, passwords, account numbers)
- Encrypting of sensitive/critical data when passing over a public network
- Encrypting of user-ids and passwords

		<p>Auditing of user authentication aids in the investigation of suspicious database access. Suspicious use of databases can also be tracked though this is typically not done due to the high level of overhead and records captured. Auditing can also be used to track changes to the database and data, and can aid in complying with licensing contracts.</p> <p><u>DBMS-based Auditing of user actions</u> <i>Shall provide</i></p> <ul style="list-style-type: none"> • An audit utility • The ability to identify the user, action, time of action, and object that action is performed on. <p><i>Nice to have</i></p> <ul style="list-style-type: none"> • DBMS audit utility can capture values of data before and after changes 	
<i>Document Source Reference #</i>			
Compliance Sources			
<i>Name</i>	MAEA Security Domain	<i>Website</i>	www.oit.gov
<i>Contact Information</i>			
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
KEYWORDS			
<i>List Keywords</i>	authentication, authorization, encryption, auditing, security, user-id, password		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>			
COMPONENT SUB-CLASSIFICATION			
Sub-Classification	Date	Additional Sub-Classification Information	
<input type="checkbox"/> <i>Technology Watch</i>			
<input type="checkbox"/> <i>Variance</i>			
<input type="checkbox"/> <i>Conditional Use</i>			
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input checked="" type="checkbox"/> <i>Under Review</i>	<input type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>

AUDIT TRAIL

<i>Creation Date</i>	02-11-04	<i>Date Approved / Rejected</i>	
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			