Oracle Security Standards

Version: 1.0

Table of Contents

DOCUMENT CONTROL

The document control section describes the revision history and summary of the changes made to the document.

1.1 Distribution List

Name	Role	Representing

1.2 Document History

Version	Date	Who	Summary of Changes
1.0	Jan, 18th 2017		Oracle Security Standards

1.3 Terminology

Term	Definition
Access Control	A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are access control lists and tickets.
Authentication	This is the process of identifying a user, usually based on a username and password, to a DBMS. Authentication is not the same as authorization. Authentication only ensures that the individual is who he/she claims to be, but does not give any access rights to database objects.
Authorization	Authorization is the process of providing access to system objects (e.g. Tables, stored procedures) based on the identity of the user.
Encryption	Cryptographic transformation of data – "plaintext" – into a form – "cipher text" – that conceals the data's original meaning to prevent it from being known or used.
FGA	Fine-Grained Auditing; Oracle option that allows auditing of objects at the column level and tracking of sql commands
VPD	Virtual Private Database; Oracle method used to enforce security policies

1.4 Document Location

The source of the document will be found under the KEC ALLIANCE Documentation section

EXECUTIVE SUMMARY

This document addresses security as it relates to the Oracle DBMS. The oracle operating system id and individual DBA operating system accounts are subject to the security requirements for the operating system.

This document is to be used in determining how secure an existing Oracle installation or instance is, as well as providing the minimum required security for Oracle databases. This standard must be followed for all future Oracle databases. Where possible, current databases should be modified to follow this standard.

This document includes specific standards for different types of internal access controls, from the initial authentication of a user to access privileges for data. These are minimum security requirements applicable to all Oracle databases. Where the application and/or a third party hosting requires less security, an official exception must be obtained before the lower level of security can be implemented. The development group and/or third party must agree to accept the vulnerabilities that accompany a lower level of security.

For additional information on Oracle Security, refer to the Oracle Technology Network Oracle OTN Security Technology Center.

PRIVILEGED ACCESS CONTROL STANDARDS

The Privileged Access Control Standards address the assignment of privileges to objects. This is known as authorization. This section includes the assignment of both system and object privileges, as well as development and assignment of roles.

All default schemas must be locked and expired at the initial database creation. Only the default Oracle options required by the application will be unlocked. All default passwords must be modified when the account is unlocked.

Users requesting object and/or system privileges must obtain the DBA team approval. The user will not be granted access until the appropriate approvals have been obtained.

The default Oracle dba role is restricted to Livingston Database Administrators. A role must be created for the developer(s) that supports the application and the associated privileges granted to this role.

Roles must be created for read_only and read_write access to the application tables. The read_only and read_write roles must be used for granting access to users. The read_only and read_write roles will include the necessary system and object level privileges. For example, the read_only role would include the "create session" system privilege. Where multiple application schemas are supported within a single database, it may be necessary to develop multiple read_only and read_write roles (e.g., finance_read_only and finance_read_write).

Creation of pl/sql requires the direct granting of object privileges. It is recommended that pl/sql be created in the application schema that owns the referenced objects. It is recommended that pl/sql code use the authid option to avoid the execution of procedures under the id of the creator.

No development or test database will have links to a production database. All database links must be controlled by creating a separate userid that has limited privileges and using that userid for all database links. Once the database links have been created, the create session privilege must be revoked from the database link owner.

The following privileges are considered dba-level privileges and are restricted to the DBA:

- become user
- alter database
- create/alter/drop profile
- create/alter/drop role
- create/alter/drop tablespaces
- "any" system privileges
- "with admin" option
- "with grant" option
- restricted session

In addition, in production environments, data definition language (ddl) commands will be restricted to the DBA. If any of these restricted privileges are requested by users, the request must be justified by an application-specific need and approved by the system DBA.

The sys.user$ and sys.link$ tables must be accessible only to sys and system. After the database is created, the select privilege on sys.user$ and sys.link$ must be revoked from public. If an application requires select on sys.user$ or sys.link$, the select privilege will only be granted with approval by the DBA.

System privileges and application schema object privileges must not be granted to “public”.

If the UTL_FILE_DIR database initialization parameter is used, it must be limited to specific directories and Oracle userids.

For databases requiring a higher level of security to protect sensitive information, consider using Oracle options such as the following:

- Fine-Grained Auditing (FGA)
- Virtual Private Database (VPD)
- Oracle Identity Management
- Data encryption

Some of these may require the separately licensed Oracle Advanced Security option.

ACCESS AUTHENTICATION STANDARDS

This section addresses user identification.

Only the DBA will be allowed to create and drop users. Requests for usernames must be made to the DBA team. The user request must include the permissions requested, including object and system level permissions. Permissions will be assigned using the appropriate roles. The approval process must include a review by the Oracle DBA for any accounts that are requesting super user or dba-level privileges. In all cases, only the minimum level of database access that is required to perform job-related activities will be granted to a user.

The Oracle training account (scott) will not be created in a production database.

No group accounts will be created unless it is for a service account. A service account is an account used specifically to perform a batch or scheduled job. All service accounts must be approved in accordance with the security requirements for new users. Only the minimum system and object privileges required to complete the job will be granted to service accounts.

The CONNECT_TIMEOUT must be set to 10 or less in the listener.ora file. The SQLNET.EXPIRE_TIME must be set to 10 or less in the sqlnet.ora file.

MONITORING AND LOGGING STANDARDS

This section deals with the database (and associated processes) security monitoring-and-logging including database auditing.

The DBA is responsible for configuring the database(s) to support the security requirements. The DBA may be required to generate a report for upper management or provide a method to obtain security-related data. The Security Plan designates who is responsible for security reviews.

The Oracle database initialization parameter for AUDIT_TRAIL must be set to “DB” in order to support auditing with the sys.aud$ table. For Oracle11g databases that require additional security, the AUDIT_TRAIL must be set to DB_EXTENDED. The Oracle database initialization parameter for AUDIT_SYS_OPERATIONS must be set to TRUE. In addition, the sys.aud$ table must be audited (audit select, insert, update, delete on sys.aud$ by access).

The sys.aud$ table must be reviewed on a regular basis to ensure that no unauthorized sys-level operations are being executed. Any suspicious or unauthorized actions must be reported immediately for further investigation. The level of security is based on requirements for the following:

- Data confidentiality
- Data integrity
- Database availability

The following table lists the review schedule required for each security level:

Security Level	Required Reviews
High	Daily
Medium	Weekly
Low	None Required Annual recommended

A record must be generated for unsuccessful login attempts. This may be accomplished using auditing, locking the userid after six failed login attempts or a combination of both. For databases with highly sensitive data, the number of failed login attempts may be reduced and/or all logins may need to be tracked.

The Oracle Net listener must have the parameter LOGGING_LISTENER set to ON. This is the default and must not be changed.

PASSWORDS, PINS, AND TOKENS

This section addresses the password requirements.

The sys and system passwords must be changed as part of the initial database creation.
A process must be in place for password resets. If a userid is locked due to the use of an incorrect password; at a minimum, the identity of the user requesting the password reset must be confirmed.

After the DBA has created the user, the password will be transmitted either in email or telephone contact directly to the user. If email is used for the notification process, the username and password must be transmitted in separate emails. No passwords will be transmitted via a third party. Users must change the assigned password at the first login. No passwords will be stored in unencrypted format in database tables.

Users that access the database with sqlplus must use the PASSWORD command to change the password. Users that access the database using an application should have a password change option. The password change option must require that the user supply the current password and confirm the new password.

No accounts will be created or modified to use external identification. The database parameters controlling authentication will be set as follows:

- REMOTE_LOGIN_PASSWORDFILE=EXCLUSIVE
- OS_AUTHEN_PREFIX=””
- REMOTE_OS_AUTH=FALSE

The Oracle default profile has unlimited resources with no password requirements. A profile must be created and assigned to all userids and application schemas, excluding those belonging to DBA accounts.

The resources for the user profile must have the following settings:

- FAILED_LOGIN_ATTEMPTS=6
- IDLE_TIME=30 (minutes)
- PASSWORD_GRACE_TIME=7 (days)
- PASSWORD_LIFE_TIME=90 (days)
- PASSWORD_LOCK_TIME=1 (days)
- PASSWORD_REUSE_MAX=6
- PASSWORD_REUSE_TIME=90

The resources for the application schema profile must have the following settings:

- FAILED_LOGIN_ATTEMPTS=6
- PASSWORD_LOCK_TIME=1 (days)

No users will log in with the application schema id unless this is required by the application front end.

In addition, both the application and user profiles must include a PASSWORD_VERIFY_FUNCTION. A function must be created that forces the password to meet the following minimum requirements:

- minimum length 8
- at least one alpha
- at least one number
- password must not be the same as the username
- no character is used more than twice

While the password verification will not be enforced for the DBA, they must still meet these minimum requirements. Only the DBA will be given the default profile in production environments.

Refer to the Appendix for a summary of the Oracle Profiles resource values.

Passwords should not be embedded into scripts unless the scripts can be adequately secured. It is recommended that database maintenance scripts use the sysdba account with the required variables for the database set within the script. For UNIX servers, it is recommended that the password be maintained in a separate, secure file which is referenced at runtime.

On a UNIX system, users logging into the database must never submit the username and password on the command line. This allows other users to see this information with the ps –ef command.

All Oracle Net LISTENERS must be protected with an encrypted password.

USER IDENTIFICATION

This section addresses the default parameters for new users, deletion/purging userids, and handling of temporary passwords.

Upon creation, users will be assigned to a default temporary and default permanent tablespace. No users will be permitted to create objects in the system or sysaux tablespaces.

It is the responsibility of the application team and/or the development team to notify the DBA group when a user is terminated. When the DBA team/group is notified that a user has been terminated, the DBA must immediately change the password, lock the user account or delete the user. If the user is known to have access to application schema passwords, then the relevant passwords must be changed.

A security review must be conducted regularly for the database. This security review must include the following:

- Minimum security requirements are met
- Exceptions to the security requirements are documented
- Procedures for approval of users and assignment of privileges are in place and enforced
- Procedures for reset of passwords are in place and enforced

In addition, a report must be compiled of all locked and expired application user accounts. The customer representative in charge of security should review this report and provide approval for accounts to be purged.

INTEGRITY CHECKS

This section addresses maintenance of the integrity of critical files.

On UNIX servers, Oracle database files must be owned by oracle:dba. The umask of 022 must be set for the oracle user. This will set the file privileges to allow execution by all; but, read and write will be restricted to oracle and the dba group. Only oracle and user accounts for the DBA's will be in the dba group. No application userids will be assigned to the UNIX dba group. If an application account requires the UNIX dba group, an exception must be submitted, approved, and documented before the dba group is assigned.

On UNIX servers, any files containing passwords must be restricted to access by the file owner (700).

In production environments, export files for the full database must be owned by oracle and restricted to access by oracle and the dba group (770). No exports of production data will be provided to vendors unless it is explicitly requested and restricted to a particular schema.

On Windows servers, the oracle id must be in the admin group.

APPENDICES

1.1 Database and Instance Names

Parameter	Value
AUDIT_TRAIL	DB (or DB_EXTENDED)
AUDIT_SYS_OPERATIONS	TRUE
O7_DICTIONARY_ACCESSIBILITY	FALSE
OS_AUTHEN_PREFIX	“” ; NULL
REMOTE_LOGIN_PASSWORDFILE	EXCLUSIVE
REMOTE_OS_AUTH	FALSE
UTL_FILE_DIR	set to specific location

1.2 Oracle Net Parameters

File	Parameter	Value
listener.ora	logging_listener	ON
listener.ora	password	encrypted value
listener.ora	connect_timeout	10
sqlnet.ora	expire_time	10

1.3 Application Development Role

The Application Development Team/Group are not permitted to have the Oracle DBA role. This is an example of the creation of an application team role that can be assigned to the application team in the development environment.

```
create role appdvp
/

grant
   create session,
   debug connect session,
   create materialized view,
   create procedure,
   create sequence,
   create synonym,
   create table,
   create trigger,
   create type,
   create view,
   global query rewrite,
   resumable,
   select any dictionary,
   create indextype
to appdvp
/
```

1.4 Oracle Profiles

Applicable To	Resource	Value
user and application	FALIED_LOGIN_ATTEMPTS	6
user	IDLE_TIME	30
user and application	PASSWORD_LOCK_TIME	1
user	PASSWORD_LIFE_TIME	90
user	PASSWORD_REUSE_MAX	6
user	PASSWORD_REUSE_TIME	90
user	PASSWORD_GRACE_TIME	7
user and application	PASSWORD_VERIFY_FUNCTION	8 characters minimum not same as username at least one number at least one alpha no character is used more than twice

The following DDL is a sample for creating profiles to meet the Security Requirements:

```
CREATE PROFILE secure_profile LIMIT
FAILED_LOGIN_ATTEMPTS  6
IDLE_TIME 30
PASSWORD_LOCK_TIME  1
PASSWORD_LIFE_TIME  90
PASSWORD_REUSE_MAX  6
PASSWORD_REUSE_TIME  90
PASSWORD_GRACE_TIME  7
PASSWORD_VERIFY_FUNCTION  verify_pwd_fct
/

CREATE PROFILE application_profile LIMIT
FAILED_LOGIN_ATTEMPTS  6
PASSWORD_LOCK_TIME  1
PASSWORD_VERIFY_FUNCTION verify_pwd_fct
/
```

1.5 Security Checklist

This is a summary only. It should be used in conjunction with this document and not as a substitute.

Y (Yes) indicates that the requirement has been met. E (exception) indicates that an exception to this standard had been requested.

Y/E	Requirement
	Privileged Access Control Standards
	Default schemas locked & expired upon creation of database
	Standard approval process in place
	Only DBAs accounts have Oracle dba role
	Separate DBA account created for DBA support
	Application development role created (in development) and assigned to the developers.
	read_only and read_write roles created
	pl/sql uses authid (recommendation)
	No database links between development/test and production
	Separate userid for database links
	dba-level privileges restricted to the DBAs
	ddl privileges restricted to the DBAs in production
	sys.user$ and sys.link$ restricted
	No grants to “public”
	ult_file_dir limited to specific directories & userid’s
	Access Authentication Standards
	Only DBAs can drop/create users
	No scott account/examples schemas in production
	No group accounts for end users
	Listener connect_timeout = 10
	Listener sqlnet.expire_time =10
	Monitoring And Logging Standards
	audit_trail=db or db_extended
	audit_sys_operations=true
	audit select, insert, update, delete on sys.aud$ by access
	Regular review of sys.aud$ (daily for high; weekly for medium; annually for low)
	Record unsuccessful login attempts
	Listener logging_listener=on (default)
	Passwords, Pins And Tokens
	Change password for sys and system
	Password meets complexity requirements (password cannot be the same as the username (for production), password must be at least 8 characters, password must have at least one alpha and one numeric character, no character can be used more than twice)
	Process in place for password reset requests
	Email of password to user must not include userid
	User password change requires entry of current password and confirmation of password
	remote_login_passwordfile=exclusive
	os_auth_prefix=””
	remote_os_auth=false
	Secure profile created for application and users (including password verify function to enforce password requirements)
	Only DBA may have default profile

Y/E	Requirement
	Passwords not accessible in programs/scripts
	Unix: userid and password not on same command line
	Listeners have encrypted password
	User Identification
	No users with system or sysaux as default or temporary tablespace
	userid's locked/user deleted upon notification of termination of user
	Security review (high every 120 days; medium every 180 days; low annually)
	Integrity Checks
	Oracle database files owned by oracle:dba
	umask 022
	Files with passwords set to 700
	Full exports set to 770
	Windows: oracle id in admin group

1.6 Security Plan Checklist

The following is a checklist for database-related information which may be included in a Security Plan.

Topic	Information Required
Environment	
	Servers, network, databases, etc.
	Have development and test environments been identified for each production database?
Security Staff	
	Who will perform the security review for new applications to identify roles to be created, grants for each role, identification of sensitive data, etc.
	Who is responsible to ensuring the Oracle Security requirements have been implemented?
	Who is responsible for regular reviews of security-related data?
User Accounts	
	Who is responsible for creation of user accounts?
	What is the process for requesting (and approval of) user access?
	What process is in place for notification of the termination or change in position of a user who has access to the database(s)?
	What is the standard user account name? This should be something that can be traced back to individual users.
	What process is to be used for providing the initial password to new users?
	What process is in place to identify inactive users (including what constitutes and “inactive” user)?
	What action is to be taken for inactive users?
	What process is in place for reset of user passwords, including request, approval and reset action?
Data	
	What process will be in place to protect sensitive data?
	Is there any highly sensitive data that must be regularly transmitted outside of the firewall configuration?
	What actions will be taken to protect sensitive data during transmission (SSL, encryption, etc.)?
	Does the SLA reflect any special availability or system requirements?
Security Review	
	What level of auditing is required by the business?
	Who will perform the review of audit and other security-related data?
	What process will be implemented to provide the audit data to the Security staff?