Database Configuration Standard

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Industry Configuration Standards 3

1.5 Related Documents / References 3

2. Standard Statements 4

2.1 Secure Installation and Configuration Checklist 4

2.2 Networking Security Checklists 6

2.3 Client Checklist 6

2.4 Listener Checklist 7

2.5 Network Checklist 7

3. Standard Compliance & Enforcement 9

3.1 Compliance Measures 9

3.2 Enforcement 9

4. Exception Process / Glossary 10

4.1 Exception Process 10

4.2 Glossary / Acronyms 10

5. Document Management 11

5.1 Document Revision Log 11

5.2 Document Ownership 11

5.3 Document Coordinator 11

5.4 Document Approvers 11

5.5 Distribution 11

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

The objective of this standard is to ensure the XXXXs business and technical requirements for databases are translated into a baseline that will allow administrators to easily configure databases to adequately protect the XXXX’s information assets against external and internal threats.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/
* Oracle Database Security Guide

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## Secure Installation and Configuration Checklist

For databases, establishing a secure configuration is a very strong first line of defense, using industry-standard best security practices for operational database deployments. The following provides the basis for a secure configuration:

1. **Install only what is required**

Do a custom installation. Avoid installing options and products you do not need. Choose to install only those additional products and options, in addition to the database server, that you require. Or, if you choose to do a *typical* installation instead, then improve your security after the installation processes finish, by removing the options and products you do not need

1. **Lock and expire default user accounts.**

Oracle Database installs with many default (preset) database server user accounts. Upon the successful creation of a database server instance, the Database Configuration Assistant automatically locks and expires most default database user accounts.

Once the database is installed, lock SYS and SYSTEM as well, and use AS SYSDBA for administrator access. Specify administrative passwords individually.

This account (AS SYSDBA) tracks the operating system user name, maintaining accountability. If you only need access for database startup and shutdown, then use AS SYSOPER instead. SYSOPER has fewer administrative privileges than SYS, but enough to perform basic operations such as startup, shutdown, mount, backup, archive, and recover.

Database Configuration Assistant is not used during a manual installation, so all default database users remain unlocked and are able to gain unauthorized access to data or to disrupt database operations. Therefore, after a manual installation, use SQL to *lock* and *expire* all default database user accounts except SYS, SYSTEM, SCOTT, and DBSNMP. Do it to SCOTT, too, unless it is being actively used. Also lock SYS and SYSTEM as described earlier. If a locked account is later needed, then a database administrator can simply unlock and activate that account with a new password.

Use the following script to find user accounts that have default passwords.

sqlpus sys as sysdba Enter password: password SELECT d.username, u.account\_status FROM DBA\_USERS\_WITH\_DEFPWD d, DBA\_USERS u WHERE d.username = u.username ORDER BY 2,1;

1. Change default user passwords.

Security is most easily broken when a default database server user account still has a default password even after installation. The following steps fix this:

* Change the default passwords of administrative users immediately after installing the database server. In any Oracle environment (production or test), assign strong, secure passwords to the SYS and SYSTEM user accounts immediately upon successful installation of the database server. Under no circumstances should the passwords for SYS and SYSTEM retain their default values. Similarly, for production environments, do not use default passwords for any administrative accounts, including SYSMAN and DBSNMP.
* Change the default passwords of all users immediately after installation. Lock and expire all default accounts after installation. If any such account is later activated, then change its default password to a new secure password.
* Enforce password management. Apply basic password management rules, such as password length, history, and complexity, to all user passwords. If possible, use Oracle Advanced Security (an option to the Enterprise Edition of Oracle Database) with network authentication services (such as Kerberos), token cards, smart cards, or X.509 certificates. These services provide strong user authentication and enable better protection against unauthorized access.

Use the **Checkpwd** tool to identify accounts with weak passwords

>checkpwd system/oracle@//127.0.0.1:1521/orcl password\_list.txt

1. Enable data dictionary protection

Implement data dictionary protection to prevent users who have the ANY system privilege from using it on the data dictionary. Oracle Database sets the O7\_DICTIONARY\_ACCESSIBILITY to FALSE. This setting prevents using the ANY system privilege on the data dictionary, except for authorized users making DBA-privileged connections (for example CONNECT/AS SYSDBA).

1. Practice the principle of least privilege.

The following practices implement this principle:

* Grant necessary privileges only.

Do not provide database users more privileges than necessary. Enable only those privileges actually required to perform necessary jobs efficiently:

1) Restrict the number of system and object privileges granted to database users.

2) Restrict the number of SYS-privileged connections to the database as much as possible. For example, there is generally no need to grant CREATE ANY TABLE to any non-DBA-privileged user.

* Revoke unnecessary privileges and roles from the role PUBLIC.

This default role, granted to every user in an Oracle database, enables unrestricted use of its privileges, such as EXECUTE on various PL/SQL packages. If unnecessary privileges and roles are not revoked from PUBLIC, then a minimally privileged user could access and execute packages otherwise inaccessible to him.

* Restrict permissions on run-time facilities.

Do not assign *all permissions* to any database server run-time facility, such as the Oracle Java Virtual Machine (OJVM). Instead, grant specific permissions to the explicit document root file paths for such facilities that may execute files and packages outside the database server.

1. Enforce access controls effectively

Authenticate clients properly. Although remote authentication can be turned on (TRUE), your installation is more secure with it turned off (FALSE, which is the default). With remote authentication turned on, the database implicitly trusts every client, because it assumes every client was authenticated by the remote authenticating system. However, clients in general (such as remote PCs) cannot be trusted to perform proper operating system authentication, so turning on this feature is a very poor security practice. To enforce proper server-based authentication of clients connecting to an Oracle database, leave or turn this feature off (remote\_os\_authentication=FALSE, which is the default).

1. Restrict operating system access.

The following practices implement appropriate restrictions on operating system access:

* Limit the number of operating system users.
* Limit the privileges of the operating system accounts (administrative, root-privileged, or DBA) on the Oracle Database host (computer) to the fewest and least powerful privileges required for each user.
* Disallow modifying the default permissions for the Oracle Database home (installation) directory or its contents, even by privileged operating system users or the Oracle owner.
* Restrict symbolic links. Ensure that when any path or file to the database is provided, neither that file nor any part of that path is modifiable by an untrusted user. The file and all components of the path should be owned by the DBA or some trusted account, such as root. This recommendation applies to all types of files, such as data files, log files, trace files, external tables, bfiles, and so on.

1. Apply all security patches and workarounds

Plug every security hole or flaw as soon as corrective action is identified. Always apply all relevant and current security patches for both the host operating system and Oracle Database, and for all installed Oracle Database options and components.

Periodically, check the security site on Oracle Technology Network for details on security alerts released by Oracle Corporation at <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>. Also check the Oracle Worldwide Support Service site, My Oracle Support, for details on available and upcoming security-related patches at <https://support.oracle.com/>

## Networking Security Checklists

Security for network communications is improved by using client, listener, and network checklists to ensure thorough protection. Using SSL (TLS v1.2) is an essential element in these lists, enabling top security for authentication and communications.

* SSL Checklist

SSL (TLS v1.2) is the Internet standard protocol for secure communication, providing mechanisms for data integrity and data encryption. These mechanisms can protect the messages sent and received by you or by applications and servers, supporting secure authentication, authorization, and messaging by means of certificates and, if necessary, encryption. Good security practices maximize protection and minimize gaps or disclosures that threaten security. While the primary documentation for Oracle SSL configuration and practices is Oracle Database Advanced Security Administrator's Guide, the following list illustrates the cautious attention to detail necessary for the successful use of SSL:

1. Ensure that configuration files (such as for clients and listeners) use the correct port for SSL, which is the port configured upon installation. You can run HTTPS on any port, but the standards specify port 443, where any HTTPS-compliant browser looks by default. Or the port can be specified in the URL, for example, <https://secure.server.com:4445/>.
2. If a firewall is in use, then it too must use the same port(s) for secure (SSL) communication.
3. Ensure that tcps is specified as the PROTOCOL in the ADDRESS parameter in the tnsnames.ora file (typically on the client or in the LDAP directory). An identical specification must appear in the listener.ora file (typically in the $ORACLE\_HOME/network/admin directory).
4. Ensure that the SSL mode is consistent for both ends of every communication. For example, between the database on one side and the user or application on the other. The mode can specify either client or server authentication (one-way), both client and server authentication (two-way), or no authentication.
5. Ensure that the server supports the client cipher suites and the certificate key algorithm in use.
6. Do not remove the encryption from your RSA private key inside your server.key file, which requires that you enter your pass phrase to read and parse this file.

## Client Checklist

Because authenticating client computers is problematic over the Internet, typically, user authentication is performed instead. This approach avoids client system issues that include falsified IP addresses, hacked operating systems or applications, and falsified or stolen client system identities. Nevertheless, the following steps improve the security of client connections:

* Configure the connection to use SSL.

Using SSL communication makes eavesdropping difficult and enables the use of certificates for user and server authentication.

* Set up certificate authentication for clients and servers.

## Listener Checklist

Because the listener acts as the database gateway to the network, it is important to limit the consequences of malicious interference:

* Restrict the privileges of the listener, so that it cannot read or write files in the database or the Oracle server address space.

This restriction prevents external procedure agents spawned by the listener (or procedures executed by such an agent) from inheriting the ability to do such reads or writes. The owner of this separate listener process should not be the owner that installed Oracle or executes the Oracle instance (such as ORACLE, the default owner).

* Secure administration by doing the following:
  + Protect the listener with a password.
  + Prevent online administration.
  + Use SSL when administering the listener.
  + Remove the external procedure configuration from the listener.ora file if you do not intend to use such procedures.
* Monitor listener activity.

## Network Checklist

Protecting the network and its traffic from inappropriate access or modification is the essence of network security. The following practices improve network security:

1. Restrict physical access to the network. Make it difficult to attach devices for listening to, interfering with, or creating communications.
2. Protect the network access points from unauthorized access. This goal includes protecting the network-related software on the computers, bridges, and routers used in communication.
3. Because you cannot protect physical addresses when transferring data over the Internet, use encryption when this data needs to be secure.
4. Use firewalls.

Appropriately placed and configured firewalls can prevent outsider access to your organization intranet when you allow internal users to have Internet access.

* + Keep the database server behind a firewall.
  + Ensure that the firewall is placed outside the network to be protected.
  + Configure the firewall to accept only those protocols, applications, or client/server sources that you know are safe.
  + Use a product like Oracle Connection Manager to multiplex multiple client network sessions through a single network connection to the database. It can filter on source, destination, and host name. This functionality enables you to ensure that connections are accepted only from physically secure terminals or from application Web servers with known IP addresses. (Filtering on IP address alone is not enough for authentication, because it can be faked.)

1. Never poke a hole through a firewall.

For example, do not leave the Oracle Listener port 1521 open, allowing the database to connect to the Internet or the Internet to connect with the database. This could introduce significant security vulnerabilities that hackers are likely to exploit. Hackers could enable even more port openings through the firewall, create multithreaded operating system server problems, and enable access to crucial information on databases behind the firewall. If the Listener is running without a password, then hackers can probe for critical details about the databases on which it is listening. These details include trace and logging information, banner information, and database descriptors and service names, enabling malicious and damaging attacks on the target databases.

1. Prevent unauthorized administration of the Oracle Listener.

Always establish a meaningful, well-formed password for the Oracle Listener, to prevent remote configuration of the Oracle Listener. Further, prevent unauthorized administration of the Oracle Listener.

1. Check network IP addresses.

Use the Oracle Net *valid node checking* security feature to allow or deny access to Oracle server processes from network clients with specified IP addresses. Set parameters in the protocol.ora file (Oracle Net configuration file) to specify client IP addresses that are denied or allowed connections to the Oracle Listener. This action prevents potential Denial of Service attacks.

1. Encrypt network traffic.

If possible, utilize Oracle Advanced Security to encrypt network traffic between clients, databases, and application servers.

1. Harden the host operating system (the system on which Oracle Database resides).

Disable all unnecessary operating system services. Many UNIX and Windows services are not necessary for most deployments. Such services include FTP, TFTP, TELNET, and so forth.

For each disabled service, be sure to close both the UDP and TCP ports. Leaving either type of port enabled leaves the operating system vulnerable.

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review the database configuration settings | * Confirm from the standard if the configuration settings on the database are the same |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Glossary / Acronyms

|  |  |
| --- | --- |
| FTP | File Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| UDP | User Datagram Protocol |
| LDAP | Lightweight Directory Access Protocol |
| URL | Uniform Resource Locator |
| RSA | Rivest–Shamir–Adleman |
| TCP | Transmission Control Protocol |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Distribution

* *IT*
* *Information Security*