



Oracle Data Services Inbound Security Policies

December 10, 2021
Copyright © 2021, Oracle and/or its affiliates
Public

CONTENTS

Overview	3
Oracle Data Services Security Policy	3
ORACLE INFORMATION SECURITY PRACTICES - GENERAL	3
SECURITY STANDARDS	3
SECURITY ORGANIZATION	3
VULNERABILITY ASSESSMENT	3
PENETRATION TEST	4
INCIDENT MANAGEMENT	4
Account and Access Management	4
USER ACCOUNTS	4
SECURITY AWARENESS	4
PASSWORD REQUIREMENTS	4
ACCOUNT DEACTIVATION	5
Data Access and Encryption	5
DATA ACCESS CONTROLS	5
REMOTE ACCESS VIA VPN	5
ENCRYPTED COMMUNICATION CHANNELS	5
ENCRYPTION AT REST	5
Inbound Data Controls	5
DATA FILE ENCRYPTION	5
FILE FORMAT SPECIFICATIONS	5
PROHIBITED DATA TYPES	5
DATA RETENTION AND DELETION	5

OVERVIEW

The Oracle Data Services Inbound Security Policy (“**ISP**”) describes the security measures Oracle uses to protect OA Supplier Data. “**OA Supplier Data**” (formerly known as **ODC Supplier Data**) is data provided to OA by OA partners and data suppliers which OA uses to power Oracle technologies, products, and services. In your agreement with Oracle, OA Supplier Data may be referred to as “Company Data” or “Your Data” or some other term describing the data you make available to OA. The ISP **only** applies when incorporated by reference in your supplier or partner agreement with Oracle.

The ISP may reference other Oracle documents. Capitalized terms that are not defined in the ISP have the meaning given to them in such other Oracle documents or in any agreement between you and Oracle that references the ISP.

Oracle may update the ISP to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, and patterns of system use, but updates to the ISP will not materially reduce the level of security that Oracle uses to protect OA Supplier Data.

ORACLE DATA SERVICES SECURITY POLICY

Oracle Information Security Practices - General

Oracle has security controls and practices designed to protect the confidentiality, integrity, and availability of OA Supplier Data. Oracle continually works to strengthen and improve those security controls and practices.

Oracle’s practices are generally aligned with the ISO/IEC 27002 Code of Practice, from which Oracle selects a comprehensive set of controls for implementation.

Oracle personnel (including employees, contractors, and temporary employees) must comply with the Oracle information security practices and other Oracle policies that govern their employment or the services they provide to Oracle.

Oracle takes a holistic approach to information security, implementing a multilayered defense security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight.

Security Standards

Oracle’s corporate security policies are aligned with the ISO 27001 controls. These include the following: organizational security; organizational security infrastructure; asset classification and control; personnel security; physical and environmental security; communications and operations management; access control; systems development and maintenance; business continuity management; and compliance.

Security Organization

The Oracle Security Oversight Committee (“**OSOC**”) is responsible for approving the implementation of security programs, including security and privacy policies. Oracle Corporate Security, comprised of several teams including Global Information Security, Global Product Security, Global Physical Security, Corporate Security Architecture, and Global Trade Compliance, is responsible for security oversight, compliance and enforcement of regulatory and legal security requirements. Oracle’s Chief Privacy Officer provides oversight and management of privacy-related regulatory issues. Oracle’s Business Audit and Assessment organization is responsible to Oracle’s Board of Directors to audit compliance of all these functions and to report audit results. Oracle’s Global Information Security (“**GIS**”) is the organization that is responsible for corporate-wide security oversight, compliance, and enforcement. This includes leading the development and management of information security policy and strategy, information security assessments, and training and awareness. OA has its own internal security organization responsible for line-of-business security management, including service-specific and data-supplier-specific security initiatives.

Vulnerability Assessment

Security vulnerability tests are performed regularly (but no less than once annually) on Oracle systems. There are multiple ongoing security checks, threat and risk assessments, vulnerability scanning, and penetration testing used to validate system controls. Audit and compliance checks are also frequently conducted to identify changes to the “known-good” posture and to take corrective or improvement actions as needed.

Oracle subscribes to vulnerability notification systems to stay apprised of security incidents, advisories, and other related information. Oracle takes actions on the notification of a threat or risk once it has the opportunity to confirm that both a valid risk exists and that the recommended changes are applicable to the particular system or environment.

Oracle GIS conducts periodic security reviews, assessments, and audits to confirm compliance with Oracle information security policies, procedures, and practices.

Penetration Test

Penetration tests are periodically performed on Oracle systems—including upon release of a new Internet-facing application or service—when major changes are made to an Internet facing application or service, or as required to comply with regulatory requirements.

Incident Management

Oracle evaluates and responds to incidents of suspicious activity or unauthorized access to or handling of OA Supplier Data. When Oracle GIS learns of such incidents, GIS evaluates the incident and defines escalation paths and response teams. GIS will work with you and law enforcement (if necessary) to address or respond to incidents. The goal of Oracle incident response is to maintain the confidentiality, integrity, and availability of OA Supplier Data and to establish root causes of incidents and implement remediation. Oracle maintains documented procedures for addressing incidents including prompt and reasonable reporting, escalation procedures, and chain of custody controls and practices. If Oracle determines that any OA Supplier Data has been misappropriated, Oracle will notify the supplier of such misappropriation within twenty-four (24) hours, unless prohibited by law.

Oracle internal policies describe the requirements for Oracle personnel to report and respond to incidents. Oracle's response plan procedures include detailed directions and procedures for designated personnel performing relevant functions during an incident. This plan is reviewed and tested at least annually.

Oracle logs certain audit and security related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to the environment or Oracle applications, as well as system alerts, console messages, and system errors. Oracle implements controls to protect against operational problems, including exhaustion of the log file media, failure to record events, or logs being overwritten. Security logs are currently kept for 1 year.

Oracle reviews logs for forensic purposes and incidents, and identified anomalous activities feed into the security incident management process.

ACCOUNT AND ACCESS MANAGEMENT

User Accounts

Oracle maintains policies that describe the principles for development, executive approval, implementation and maintenance of information security policies and practices at Oracle. In these policies, Oracle describes governing principles for user accounts including 'need to know' 'least privilege' access controls and segregation of duties. All employees, contractors, and temporary employees are subject to these policies.

Oracle's Logical Access Controls Policy describes access control requirements for Oracle resources, including need-to-know, least privilege and authorization rules.

Users are assigned predefined roles based on segregation of duty and limit access, as appropriate. System administrators that require root or administration privileges are also assigned separate accounts with privileged access necessary to perform administrative responsibilities. Analysts, developers and others who may have access to systems that store or process OA Supplier Data must explicitly request access to such systems or data, and these requests are approved by Oracle security and the requestor's manager.

Security Awareness

Oracle conducts mandatory security and privacy awareness training for all employees when they are hired and no less than once every two years thereafter. Frequency and scope of additional security training depends on employee roles.

Oracle requires employees, prior to accessing any data or Oracle systems, to undergo security awareness training that addresses data privacy, customer data segregation, appropriate use of Oracle systems, data loss prevention, and other security-related topics.

Oracle employees and contractors who may have access to OA Supplier Data are subject to a written confidentiality agreement. Before performing services for Oracle and before accessing any Oracle system or resource, service providers must sign agreements defining the services to be provided and the service providers' confidentiality obligations.

Password Requirements

Access to Oracle systems is restricted to authorized personnel only. Oracle enforces strong password policies on infrastructure components and production systems used to operate the Oracle environment. This includes requiring a

minimum password length, password complexity, and regular password changes. Strong passwords or multi-factor authentication are used throughout the infrastructure to reduce the risk of intruders gaining access through exploitation of user accounts. System access controls include system authentication, authorization, access approval, provisioning, and revocation for employees and other Oracle-defined users. Network, operating system, database and application accounts for Oracle employees are reviewed regularly to ensure employee access levels. When employees or personnel leave the company or are no longer under contract, Oracle takes prompt actions to terminate network, system, application, telephony, and physical access for such former employees.

Account Deactivation

Oracle has a process for employment terminations. Terminations are processed automatically through the Oracle Human Resources Management System. Human Resources processes both voluntary and involuntary terminations. After a termination is processed, automated notifications are issued for terminations (regardless of type) based on the effective date of the termination. The recipient list for the notifications includes Oracle security and all necessary parties. Oracle then creates an exit ticket for the off-boarding employee, and access to systems is noted and terminated at this time.

DATA ACCESS AND ENCRYPTION

Data Access Controls

Oracle maintains a Logical Access Controls Policy that specifies access control requirements for Oracle resources, including need-to-know, least privilege and authorization rules. Account provisioning and management standards and procedures are in place to review and approve account requests. There is no direct access to Production systems via the administrator or root accounts.

Remote Access via VPN

Access to Oracle services environments is over Virtual Private Network (“VPN”), thus establishing a private and encrypted connection for the network session. Additionally, remote administrative activities are conducted over the Oracle VPN.

Encrypted Communication Channels

Remote access for Oracle personnel from a non-Oracle location to the Oracle network requires connection either an IPSec or SSL encrypted VPN. Administrative access to Oracle Production environments requires two-factor authentication over a VPN.

Encryption at Rest

Personal Data provided to Oracle by its data suppliers is encrypted at rest using the symmetric AES algorithm with a 256-bit key length. OA Supplier Data delivered via an encrypted container (.GPG, .PGP or encrypted .ZIP files) retains the original encrypted container, and is decrypted into ephemeral memory for such functions as generating match keys.

INBOUND DATA CONTROLS

Data File Encryption

Oracle only accepts PGP encrypted data files. Data files must be transmitted via an Oracle-approved encrypted protocol, such as SFTP or HTTPS (TLS 1.2+). Oracle stores data files on an AES-256 encrypted storage resource.

File Format Specifications

Oracle does not accept data files in a content or format that is not approved by Oracle before such transfer.


Prohibited Data Types

Currently, Oracle does not accept files which include:

- Social Security Numbers
- PCI/PAN (such as credit card or debit card information)
- HIPAA-protected information
- Drivers' License numbers
- Information on minors (under sixteen (16) years) old
- Other data that your agreement with Oracle prohibits you to transmit to Oracle

Oracle will perform manual and automated quality and content control checks on ingested files, and any file with unapproved content or which deviates from agree upon formatting will be rejected.

Data Retention and Deletion



Oracle will only store and process OA Supplier Data for as long as necessary to fulfill a business purpose. Upon your written request, Oracle will delete or render permanently inaccessible data provided by any of OA's data suppliers within thirty (30) business days of receiving the request.