Oracle Corporate Security Practices

Version 1.5
Effective Date: 15 May 2018

CONTENTS

Introduction

The Oracle Corporate Security Practices ("Security Practices") describe the security practices implemented pursuant to Oracle's Corporate security program, and adhered to by Oracle for its operational and services infrastructure under its control, including Oracle's corporate network and systems. As used in this document, "customer data" means any data stored in a customer's computer system (data accessed by or provided to Oracle while performing services for a customer) or customer's Oracle Cloud instance. Third parties engaged by Oracle and that are also provided access to customer data by Oracle ("subprocessors"), will be contractually committed to materially equivalent security practices.

These practices are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under an order.

1. Scope

1.1 Overview

The Security Practices are designed to protect the confidentiality, integrity, and availability of both customer and Oracle data. Oracle continually works to strengthen and improve the security controls and practices for Oracle internal operations and services offered to customers.

As noted above, this document describes the security practices adhered to by Oracle for its operation and services infrastructure. Companies that Oracle acquires are required to align with these Security Practices as part of the integration process.

Oracle's Cloud, Support, Consulting, and Advanced Customer Support Services lines of business have also developed more detailed statements of security practices that apply to many of their service offerings, which are available for review and also incorporated into the applicable order for services. More details on these practices can be found here:

- Cloud Hosting & Delivery Policies
- Global Customer Support Security Practices
- Consulting Security Practices
- Advanced Customer Services Security Practices

2. Oracle Information Security

2.1 Overview

Oracle's security policies cover the management of security for both Oracle's internal operations and the services Oracle provides to its customers, and apply to all Oracle Employees, contingent workers, and sub-processors. They are generally aligned with the ISO/IEC 27002:2013 and 27001:2013 standards, and govern all areas of security within 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.

2.2 Privacy

The *Oracle Privacy Policy* describes how Oracle collects and uses personal information collected from the Oracle websites that link or refer to the policy as well as from offline sales and marketing activities. It also describes how users can control that collection and use. This policy is available at https://www.oracle.com/legal/privacy/privacy-policy.html.

The *Oracle Services Privacy Policy* describes Oracle's treatment of data that resides on Oracle, customer or third-party systems (including personal information or "PI") to which Oracle may be provided access in connection with the provision of services. This policy is available at https://www.oracle.com/legal/privacy/services-privacy-policy.html.

The *Oracle Marketing Cloud and Oracle Data Cloud Privacy Policy* describes how Oracle Marketing Cloud and Oracle Data Cloud services facilitate the collection and use of information by our customers in connection with interest-based advertising, and is designed to provide tools to help understand and control the collection and use of that information. This policy is available at https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html.

2.3 Enforcement

Oracle requires the reporting of and response to information security incidents in a timely and efficient manner. Oracle also maintains a detailed Incident Response Plan to provide specific guidance for personnel involved in or supporting incident response.

Oracle's Global Information Security (GIS) organization conducts security reviews, assessments, and audits periodically to confirm compliance with the Oracle information security policies, procedures, and practices.

Where non-compliance is found, GIS works with the relevant Lines of Business to resolve those issues in a timely a manner. GIS reserves the right to intervene as deemed necessary and to isolate environments in non-compliance that put infrastructure or other environments at serious risk.

Oracle employees who fail to comply with Oracle information security policies, procedures, and practices may be subject to disciplinary action, up to and including termination.

3. Organizational Security

Oracle's overarching Organizational Security is described in the Oracle Security Organization Policy and the Oracle Information Security Policy. The Chief Corporate Architect, who reports directly to the CTO, manages the functional departments directly responsible for identifying and implementing security controls at Oracle. The Global Information Security, Global Product Security, Global Physical Security, and Oracle Security Architecture organizations comprise Oracle Corporate Security, which provides independent security policy, guidance and compliance oversight to Oracle worldwide.

3.1 Oracle Security Oversight Committee

The Oracle Security Oversight Committee (OSOC) oversees the implementation of Oracle-wide security programs, including security policies and data privacy standards. The OSOC is chaired by Oracle's CEO, General Counsel, and Chief Corporate Architect.

3.2 Global Security Organizations

3.2.1 Global Information Security

Global Information Security (GIS) is responsible for security oversight and assurance, policy compliance and enforcement, leading the development of information security policy and strategy, as well as training and awareness at the Corporate level. GIS serves as the primary contact for security incident response, providing overall direction for incident prevention, identification, investigation, and resolution.

3.2.2 Global Product Security

Global Product Security (GPS) acts as a central resource to help Oracle development teams improve the security of Oracle products. GPS' primary mission is to promote the use of the Oracle Software Security Assurance (OSSA) standards throughout Oracle. Responsibilities include assisting in improving the security of Oracle products in their development phase, performing security assessments of Oracle products using a variety of techniques, and evaluating potential product security vulnerabilities.

3.2.3 Global Physical Security

Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of our employees, business enterprise and assets. More information on applicable physical security controls are described in section 6.

3.2.3 Corporate Security Architecture

Corporate Security Architecture (CSA) is responsible for setting Information Security Architecture strategy and direction in support of long-term Corporate objectives and verifying alignment of IT initiatives with Corporate Security Architecture strategy and direction. In addition, CSA identifies and guides IT security infrastructure improvements and reviews security-related technical aspects of IT projects and acts as technical advisor on Corporate Security matters.

3.3 Oracle Information Technology Organizations

Oracle Information Technology (IT) and Cloud DevOps organizations are responsible for IT security strategy, architectural design of security solutions, engineering, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation, and security technical assessment for new infrastructure.

3.4 Confidentiality Agreements

All Oracle employees and subprocessors who may have access to customer data are subject to a written confidentiality agreement. Prior to performing services for Oracle and prior to accessing any Oracle system or resource, service providers are required to sign a Services Provider Agreement, a Network Access Agreement, and a work order defining the services to be provided.

Oracle is obligated to protect the confidentiality of customer data in accordance with the terms of the Ordering Document, Exhibit, and Statement of Work.

3.5 Independent Review of Information Security

Global Information Security, in conjunction with Oracle Internal Audit, oversees compliance of the security controls, processes, and procedures for Oracle services.

4. Asset Classification and Control

4.1 Responsibility, Inventory, and Ownership of Assets

Overarching controls related to assets are addressed by the *Oracle Information Protection Policy*, the *Oracle Desktop and Laptop Security Policy*, the *Oracle Information Systems Inventory Policy,* and the *Oracle Acceptable Use Policy for Company Resources*. All information assets have an owner who is responsible for the protection and inventory of assets based on the sensitivity and value of information. If ownership has not been assigned, it will default to the administrators of the application or system. This includes maintenance of operations guides and other documentation describing the environments.

4.2 Asset Classification and Control

Oracle provides guidelines for all Oracle personnel regarding information classification schemes and minimum handling requirements associated with those classifications in order to provide protection for Oracle and customer information assets. Oracle has defined three classes of confidential information – Internal, Restricted, and Highly Restricted – with each classification requiring corresponding levels of security controls (e.g., encryption requirements for data classified as Restricted or Highly Restricted). Customer data is classified as among Oracle's top two categories of confidential information, which have associated limits on access, distribution and handling. Oracle keeps the information confidential in accordance with the terms of customer's order.

5. Human Resources Security

Oracle places a strong emphasis on personnel security. Measures taken to minimize risks associated with human error, theft, fraud, and misuse of facilities include personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

The *Oracle Code of Ethics and Business Conduct* sets forth Oracle's high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business throughout the world. The standard applies to Oracle employees, contractors, and temporary employees. It covers the areas of legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required every two years. The Code of Ethics and Business Conduct is available at the following URL: http://www.oracle.com/us/corporate/investor-relations/cebc-176732.pdf

5.1 Employee Screening

Oracle currently uses an external screening agency to perform pre-employment background investigations for newly hired U.S. personnel. Personnel screening in other countries varies according to local laws, employment regulations and Oracle policy.

5.2 Security Awareness Education and Training

Oracle promotes security awareness and educates employees through regular newsletters, ad hoc security awareness campaigns, and security related Corporate send mails.

Each employee is required to complete information protection awareness training. The course instructs employees on their obligations under the various Oracle privacy and security policies (such as the *Information Protection Policy*, *Acceptable Use Policy for Company Resources* and the *Services Privacy Policy*). The course also covers data privacy principles and data handling practices that may apply to employees' jobs at Oracle and are required by company policy, including those related to use, access, integrity, sharing, retention, security and disposal of data.

Oracle performs periodic compliance reviews to determine if employees have completed the online awareness-training course. If Oracle determines that an employee has not completed the required course, the employee will be promptly notified and instructed to complete the required training, and may be subject to disciplinary action.

Oracle promotes awareness of, and educates employees about, issues relating to security. Oracle currently prepares and distributes to its employees quarterly newsletters, ad hoc notices and other written material on security. Oracle also may update existing training courses, and develop new courses from time to time, which employees will be directed to complete.

5.3 Enforcement

Security reviews, assessments, and audits are conducted periodically to confirm compliance with Oracle information security policies, procedures, and practices. Employees who fail to comply with Oracle information security policies, procedures and guidelines may be subject to disciplinary action, up to and including termination.

6. Physical Security

Overarching controls related to physical security are described in the *Oracle Identification and Access Badge Policy*. Oracle Global Physical Security utilize a security risk-based defense in depth or layered methodology designed to balance prevention, detection, protection and response.

Oracle maintains the following physical security standards designed to prohibit unauthorized physical access at all Oracle facilities from which customer data may be handled ("Service Locations"):

- Service Locations have physical access limited to Oracle employees, subcontractors, and authorized visitors.
- Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on the premises.
- Visitors to Service Locations are required to sign a visitor's register, be escorted and/or observed when they are on the premises, and/or be bound by the terms of a confidentiality agreement.
- Security monitors the possession of keys/access cards and the ability to access the Service Locations. Staff leaving Oracle employment must return keys/cards.
- After-hours access to Service Locations is monitored and controlled by Security.

- Oracle Physical Security authorizes all repairs and modifications to the security barriers and entry controls at Service Locations owned by Oracle.

7. Communications and Operations Management

Oracle aligns with the IT service management process areas as outlined in the ITIL Infrastructure Library and uses this framework as a guide for operational delivery. Oracle's internal documentation specifies current operational processes and procedures for employees' performance of technical functions.

7.1 Segregation of Duties

Roles within operations are well defined, allowing for segregation of duties. Segregation of duties is achieved by organizing operations into functional groups, where each function is performed by separate groups of employees. Examples of the functional groups include database administrators, System Administrators, and network engineers.

7.2 Protection Against Malicious Code

Oracle's Desktop and Laptop Security Policy requires that all computers connected to Oracle's intranet have anti-virus, firewall and desktop asset management software installed, that all computers that hold Oracle data running a Windows operating system must have Microsoft security updates enabled, and that Oracle personnel install the approved full disk encryption software on their laptops, unless an approved exception has been authorized for appropriate business purposes.

Oracle's Global IT (GIT) organization keeps anti-virus products up-to-date with virus definitions and security updates. GIT is responsible for notifying internal Oracle system users of any credible virus threats and when security updates are available and Oracle employees are required to comply with instructions received through e-mail from the GIT organization. Oracle has also licensed and installed third-party anti-virus and anti-spam products to scan all emails and attachments (inbound and outbound).

7.3 Network Security Management

Overarching policies related to network infrastructure are described in the *Oracle Network Security Policy* and *Oracle Server Security Policy*. Oracle employs intrusion prevention and detection systems within the Oracle corporate networks to provide surveillance for intercepting and responding to security events as they are identified. Events are analyzed using signature and anomaly detection and Oracle updates the signature database frequently. Alerts are forwarded to Oracle's IT security for review and response to potential threats. Oracle uses router rules, access control and security lists and segmentation on the Oracle network. Oracle's Global IT and Cloud DevOps departments manage and monitor routers and firewall logs and network devices are safeguarded via centralized authentication with audited usage.

7.4 Monitoring and Protection of Audit Log Information

The following sections describe controls utilized by Oracle to monitor and protect audit log information as detailed in the overarching *Oracle Logging and Log Analysis Policy.*

- Logging

  Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console

messages, and system errors. Oracle implements controls to protect against operational issues, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.

- Log Review

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

- Log Security

Access to logs is provided on the basis of need to know and least privilege. Where feasible, log files are protected by cryptographic hash sum, and are monitored. Logs on intranet-accessible systems are relocated daily to systems that are not intranet-accessible.

8. Access Control

Overarching policies for access are described in the *Oracle Logical Access Controls Policy*. Access control refers to the policies, procedures, and tools that govern the access to and use of resources. Examples of resources include a physical server, a file, a directory, a service running on an operating system, a table in a database, or a network protocol.

- Oracle uses the principle of "Least privilege" in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.

- Oracle uses the principle of "Default deny" that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.

In the event of employee terminations, deaths or resignations, Oracle will take actions to terminate network, telephony and physical access for such former employees. Oracle Corporate Security will periodically review accounts of terminated employees to verify that access has been terminated and that stale accounts are removed from the Oracle network.

8.1 Access Control

The *Oracle Logical Access Control Policy* is applicable to access control decisions for all Oracle employees and any information processing facility for which Oracle has administrative authority. The policy does not apply to publicly accessible internet-facing Oracle systems or customer's end users.

8.2 User Access Management

- User Registration
  - Access privileges are granted based on job role and require management approval.
- Privilege Management
  - Authorization is dependent on authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All Oracle authorization decisions for granting, approval, and review of access are based on the following principles:
  - “Need to know” - Only provide access when required for job function or role

- "Segregation of duties" - Avoid a conflict of interest in the access that is provided
- "Least privilege" - Restricted access to only those resources and information required for a legitimate business purpose

- User Password Management

As described in the *Oracle Password Policy*, Oracle enforces strong password policies for Oracle network, operating system, and database accounts in an effort to reduce the chances of intruders gaining access to systems or environments through exploitation of User accounts and their associated passwords.

- Review of Access Rights

Network and operating system accounts are reviewed regularly with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to terminate network, telephony, and physical access for such former employees.

- Password Use

The use of passwords is addressed in the *Oracle Password Policy.* Oracle employees are obligated to follow rules for password length and complexity, and keep their passwords confidential and secure at all times. Passwords may not be disclosed to any unauthorized person. Under certain circumstances, passwords may be communicated between authorized Oracle employees for the purpose of providing support services.

8.3 Network Access Controls

Network controls implemented for Oracle address the protection and control of customer data during its transmission from one end system to another. The *Oracle Use of Network Services Policy* states that computers, servers, and other data devices connected to the Oracle network must comply with Global IT (GIT) and GIS standards for security, configuration, and access method, in accordance with *Oracle's Acceptable Use Policy for Company Resources.*

9. Information Systems Acquisition, Development, and Maintenance

9.1 Access Control to Program Source Code

Access to Oracle source code is provided on a strict "Need to know" basis to those who require it for an authorized business purpose.

9.2 Technical Vulnerability Management

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.

10. Information Security Incident Response

Oracle evaluates and responds to incidents that create suspicions of unauthorized access to, or handling of, customer data in its possession or under its control, whether the data is held on Oracle hardware assets, those of vendors/suppliers, or on the personal hardware assets of Oracle employees and contingent workers. Oracle's Global Information Security (GIS) organization is required to be informed of such incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those incidents.

If Oracle becomes aware and determines that an incident involving your customer data qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, customer data transmitted, stored or otherwise processed on Oracle systems that compromises the security, confidentiality or integrity of such customer data, Oracle will report such breach to you without undue delay.

Oracle will not disclose production data located on Oracle systems, including text and images, except in accordance with your order, your instructions, or to the extent required by law. Oracle will use diligent efforts to inform you, to the extent permitted by law, of any request for such disclosure before disclosure is made.

11. Oracle's Resilience Management

Oracle has a global Risk Management and Resiliency Program (RMRP), which comprises, among other elements, contingency planning and plan testing designed to enable our critical, internal operations to continue in spite of potentially business-disruptive incidents. The RMRP addresses:

- Personal safety;
- Incident management;
- Business continuity; and
- Technological system recovery.

12. Audit

In the event that the applicable order for services provides you with the right to audit Oracle's compliance with these security practices, the following procedures apply. You must send Oracle's Global Information Security organization a written request, including a detailed audit plan, at least two weeks in advance of the proposed audit date. The parties will work cooperatively to agree on a final audit plan. The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to on-site policies and regulations, and may not unreasonably interfere with business activities. If you would like to use a third party to conduct the audit, the third party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Oracle. Upon completion of the audit, you will provide Oracle with a copy of the audit report, which is classified as confidential information under the terms of the Agreement. Additional audit terms may be included in your order for services.

13. Customer Data Retention

Except as otherwise specified in an order for services or required by law, upon termination of services or at your request, Oracle will delete your production customer data located on Oracle computers in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the data. For Cloud Services, customer data management is generally "self service" and additional information on features to assist you with data management can be found in the applicable "Service Feature Guidance" document. For other Oracle services, you may consult with your Oracle services contact for additional information on data deletion prior to service completion.

As described in the *Oracle Media Sanitization and Disposal Policy*, media containing Customer Data will be securely sanitized, or destroyed and disposed of when the media is no longer required or able to be used, or the storage media becomes otherwise obsolete. Currently approved sanitization methods are degaussing, shredding, incineration, and verified overwrites of the data. Some hardware such as SSD may include acceptable built-in secure erasure functionality.

14. Reference

As stated above, these security practices should be read in conjunction with any more detailed security practices created by Oracle's Cloud, Global Customer Support, Consulting, and Advanced Customer Services lines of business, which are available for review and also incorporated into the applicable order for services. More details on these practices can be found here:

- Cloud Hosting & Delivery Policies
- Global Customer Support Security Practices
- Consulting Security Practices
- Advanced Customer Services Security Practices

These practices are subject to change at Oracle's discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under an order.