INTRODUCTION

Oracle, a global provider of enterprise cloud computing, is empowering businesses of all sizes on their journey of digital transformation. Oracle Cloud provides leading edge capabilities in software as a service, platform as a service, infrastructure as a service and data as a service.

Oracle’s security practices are multidimensional and reflect the various ways Oracle engages with its customers:

- The Oracle Corporate Security Practices (“Security Practices”) are implemented pursuant to Oracle’s Corporate security program and are adhered to by Oracle for its operational and services infrastructure under its control, including Oracle’s corporate network and systems.
- The term “customer data” as used in this document 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 who have been provided access to customer data by Oracle (“subprocessors”) are contractually committed to materially equivalent security practices.

Oracle continually works to strengthen and improve the security controls and practices for Oracle internal operations and services offered to customers. 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

These practices are subject to change at Oracle’s discretion; however, Oracle does not expect to materially reduce the level of security specified in this document.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Oracle Information Security</td>
<td>3</td>
</tr>
<tr>
<td><strong>Organizational Security</strong></td>
<td>3</td>
</tr>
<tr>
<td>Oracle Security Oversight Committee</td>
<td>3</td>
</tr>
<tr>
<td>Global Security Organizations</td>
<td>3</td>
</tr>
<tr>
<td>Global Information Security</td>
<td>3</td>
</tr>
<tr>
<td>Global Product Security</td>
<td>3</td>
</tr>
<tr>
<td>Global Physical Security</td>
<td>3</td>
</tr>
<tr>
<td>Corporate Security Architecture</td>
<td>4</td>
</tr>
<tr>
<td>Global Trade Compliance</td>
<td>4</td>
</tr>
<tr>
<td>Oracle Information Technology Organizations</td>
<td>4</td>
</tr>
<tr>
<td>Confidentiality Agreements</td>
<td>4</td>
</tr>
<tr>
<td>Independent Review of Information Security</td>
<td>4</td>
</tr>
<tr>
<td>Privacy</td>
<td>4</td>
</tr>
<tr>
<td><strong>Asset Classification and Control</strong></td>
<td>5</td>
</tr>
<tr>
<td>Responsibility, Inventory, and Ownership of Assets</td>
<td>5</td>
</tr>
<tr>
<td>Asset Classification and Control</td>
<td>5</td>
</tr>
<tr>
<td><strong>Human Resources Security</strong></td>
<td>5</td>
</tr>
<tr>
<td>Employee Screening</td>
<td>5</td>
</tr>
<tr>
<td>Security Awareness Education and Training</td>
<td>5</td>
</tr>
<tr>
<td>Enforcement</td>
<td>5</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td>6</td>
</tr>
<tr>
<td><strong>Operations Management</strong></td>
<td>6</td>
</tr>
<tr>
<td>Protection Against Malicious Code</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring and Protection of Audit Log Information</td>
<td>6</td>
</tr>
<tr>
<td>Network Controls</td>
<td>7</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>7</td>
</tr>
<tr>
<td>User Access Management</td>
<td>7</td>
</tr>
<tr>
<td>User Registration</td>
<td>7</td>
</tr>
<tr>
<td>Privilege Management</td>
<td>7</td>
</tr>
<tr>
<td>User Password Management</td>
<td>7</td>
</tr>
<tr>
<td>Review of Access Rights</td>
<td>8</td>
</tr>
<tr>
<td>Password Use</td>
<td>8</td>
</tr>
<tr>
<td>Segregation of Duties</td>
<td>8</td>
</tr>
<tr>
<td><strong>Information Systems Acquisition, Development, and Maintenance</strong></td>
<td>8</td>
</tr>
<tr>
<td>Access Control to Program Source Code</td>
<td>8</td>
</tr>
<tr>
<td>Technical Vulnerability Management</td>
<td>8</td>
</tr>
<tr>
<td><strong>Information Security Incident Response</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Oracle’s Resilience Management</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Oracle Software Security Assurance (OSSA)</strong></td>
<td>9</td>
</tr>
<tr>
<td>Secure Coding Standards &amp; Security Training</td>
<td>9</td>
</tr>
<tr>
<td>Security Analysis &amp; Testing</td>
<td>10</td>
</tr>
<tr>
<td><strong>Customer Data Protection</strong></td>
<td>10</td>
</tr>
<tr>
<td>Reference</td>
<td>10</td>
</tr>
</tbody>
</table>
ORACLE INFORMATION SECURITY

Oracle’s Corporate Security Program is designed to protect the confidentiality, integrity and availability of both Oracle and customer data, such as:

- The mission-critical systems that customers rely upon for Cloud, technical support and other services.
- Oracle source code and other sensitive data against theft and malicious alteration.
- Personal and other sensitive information that Oracle collects in the course of its business, including customer, partner, supplier and employee data residing in Oracle’s internal IT systems.

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 personnel, such as employees and contractors. These policies are generally aligned with the ISO/IEC 27002:2013 and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle.

Reflecting the recommended practices in security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective and corrective security controls with the objective of protecting information assets.

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, is one of the directors of the Oracle Security Oversight Committee (OSOC). The Chief Corporate Architect manages the functional departments directly responsible for identifying and implementing security controls at Oracle. These departments drive the corporate security program, define corporate security policies, assess compliance and provide operational oversight for the multidimensional aspects of Oracle’s security policies and practices.

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.

Global Security Organizations

Global Information Security

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

Global Product Security

The Global Product Security organization acts as a central resource to help Oracle development teams improve the security of Oracle products. Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance is Oracle’s methodology for building security into the design, build, testing, and maintenance of its products.

Under the leadership of Oracle’s Chief Security Officer, Global Product Security promotes the use of Oracle Software Security Assurance standards throughout Oracle, acts as a central resource to help development teams improve the security of their products, and handles specialized security functions.

Global Physical Security

Global Physical Security is responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of Oracle’s employees, facilities, business enterprise, and assets. Oracle’s physical security standards and policies have been developed to generally align with several physical security industry initiatives, including the International Organization for Standardization (ISO), United States Customs Trade Partnership Against Terrorism (CTPAT), American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18, and
the Payment Card Industry Security Standards Council. More information on applicable physical security controls are described in this document.

Corporate Security Architecture


Corporate Security Architecture (CSA) manages a variety of programs and leverages multiple methods of engaging with leadership and operational security teams responsible for Oracle operations, services, cloud and all other lines of business.

Global Trade Compliance

Oracle Global Trade Compliance (GTC) is responsible for import and export oversight, guidance and enforcement to enable worldwide trade compliant business processes across Oracle in order to uphold and protect Oracle’s global trade privileges. GTC manages Oracle’s global trade compliance portfolio and is responsible for global trade regulatory interpretation and coordination of policy advocacy, Global Brand Protection, Hardware Compliance Strategy and Market Access programs. Further, GTC reviews and resolves global trade compliance matters; serves as the clearinghouse for all global trade compliance information, including product classification, and is empowered to take actions necessary to ensure Oracle remains compliant with U.S. and applicable local Customs, import, and export laws, regulations and statutes.

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.

Confidentiality Agreements

Oracle employees are required to maintain the confidentiality of customer data. Employees must sign a confidentiality agreement and comply with company policies concerning protection of confidential information as part of their initial terms of employment. Oracle obtains a written confidentiality agreement from each subcontractor before that subcontractor provides services.

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.

PRIVACY

The Oracle General Privacy Policy addresses information Oracle collects in connection with your use of our websites and mobile applications, your interactions with Oracle and in the context of our offline sales and marketing activities, including Profit Magazine and Oracle Magazine. This policy is available at https://www.oracle.com/legal/privacy/privacy-policy.html.

The Oracle Services Privacy Policy describes our privacy and security practices that apply when handling (i) services personal information in order to perform Consulting, Technical Support, Cloud and other services on behalf of Oracle customers; and (ii) personal information contained in systems operation data generated by the interaction of (end-)users of these services with Oracle systems and networks. This policy is available at https://www.oracle.com/legal/privacy/services-privacy-policy.html.

The Oracle Data Cloud Privacy Policy addresses how Oracle facilitates the collection and use of marketing and interest-based information to help enable interest-based advertising by Oracle’s Marketing and Data Cloud customers. This policy is available at https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html.

Learn more about Oracle privacy policies at https://www.oracle.com/legal/privacy/.
ASSET CLASSIFICATION AND CONTROL

Responsibility, Inventory, and Ownership of Assets
Oracle’s formal information protection policy provides guidelines for all Oracle personnel regarding information classification schemes and minimum handling requirements associated with those classifications.

Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle’s information systems inventory policy requires that an accurate and current inventory be maintained for all information systems holding critical and highly critical information assets in Oracle corporate and cloud infrastructures.

Asset Classification and Control
Oracle categorizes confidential information into four classes — Public, Internal, Restricted, and Highly Restricted — with each classification requiring corresponding levels of security controls, such as encryption requirements for data classified as Restricted or Highly Restricted.

Oracle has formal requirements for managing data retention. These operational policies define requirements per data type and category, including examples of records in various Oracle departments. Retention of customer data in cloud services is controlled by the customer and is subject to terms in their contract.

Customer data is classified under one of Oracle’s top two categories of confidential information for the purpose of placing limits on access, distribution and handling of such data. Oracle keeps the information confidential in accordance with the terms of customer’s order.

HUMAN RESOURCES SECURITY
Oracle places a strong emphasis on personnel security. The company maintains ongoing initiatives intended to help minimize risks associated with human error, theft, fraud and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

Oracle maintains high standards for ethical business conduct at every level of the organization, and at every location where Oracle does business around the world. These apply to Oracle employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. Oracle requires its employees to receive training in ethics and business conduct every two years.

Oracle’s Code of Ethics and Business Conduct is available at: https://www.oracle.com/assets/cebc-176732.pdf

Employee Screening
In the United States, 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 local Oracle policy.

Learn about Oracle's commitment to diversity and inclusion at https://www.oracle.com/corporate/careers/culture/diversity.html

Security Awareness Education and Training
Oracle promotes security awareness and educates employees through regular newsletters and ad hoc security awareness campaigns. Each employee is required to complete information-protection awareness training upon hiring and every two years thereafter. The course instructs employees on their obligations under Oracle privacy and security policies. This course also covers data-privacy principles and data-handling practices that may apply to employees’ jobs at Oracle and are required by company policy.

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 these policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.
PHYSICAL SECURITY

Oracle Global Physical Security uses a risk-based approach to physical and environmental security. The goal is to address requirements for prevention, detection, protection and response while maintaining a positive work environment that fosters innovation and collaboration among Oracle employees and partners. Oracle regularly performs risk assessments to confirm that appropriate mitigation controls are in place and maintained.

Oracle currently has implemented the following protocols:

- Physical access to facilities is limited to Oracle employees, contractors, and authorized visitors.
- Oracle employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on Oracle premises.
- Visitors are required to sign a visitor’s register, be escorted and/or observed when they are on Oracle premises, and/or be bound by the terms of a confidentiality agreement with Oracle.
- Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving Oracle’s employment must return keys/cards and key/cards are deactivated upon termination.
- Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.
- Oracle use a combination of 24/7 onsite security officers or patrol officers, depending on the risk/protection level of the facility. In all cases officers are responsible for patrols, alarm response, and recording of security incidents.
- Oracle has implemented centrally managed electronic access control systems with integrated intruder alarm capability. The access logs are kept for a minimum of six months. Furthermore, the retention period for CCTV monitoring and recording ranges from 30-90 days minimum, depending on the facility’s functions and risk level.

OPERATIONS MANAGEMENT

Protection Against Malicious Code

Oracle policy requires the use of antivirus protection and firewall software on endpoint devices (e.g., laptop, desktop/workstations) and mobile devices. Additionally, all computers running a Windows operating system that hold Oracle data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process Oracle or customer information must be encrypted using approved software. Reports enable lines of business management to verify deployment of laptop encryption for their organization.

Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.

The Oracle Information Technology (OIT) organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. OIT is responsible for notifying internal Oracle system users of both any credible virus threats and when security updates are available. OIT provides automation to verify antivirus configuration.

Employees are prohibited from altering, disabling or removing antivirus software and the security update service from any computer. Any Oracle employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.

Monitoring and Protection of Audit Log Information

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 designed to protect against operational problems, including log file media becoming exhausted, failing to record events and/or logs being overwritten.

Oracle reviews logs for forensic purposes and incidents. Identified anomalous activities feed into the security-incident management process. Access to security logs is provided on the basis of need-to-know and least privilege. Where available for cloud services, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

See the Cloud Services Hosting and Delivery Policies, Pillar documentation and Program Documentation for information about available logs and monitoring features for your Cloud services: https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
Network Controls

Oracle has implemented and maintained strong network controls to 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 well-established standards for security, configuration and access method.

For administration of network security and network-management devices, Oracle requires IT personnel to use secure protocols with authentication, authorization and strong encryption. Network devices must be located in an environment protected with physical access controls and other physical security measures defined by Oracle’s Global Physical Security (GPS).

Communications to and from the Oracle corporate network must pass through network security devices at the border of Oracle's internal corporate network. Remote connections to the Oracle corporate network must exclusively use approved virtual private networks (VPNs). Corporate systems available outside the corporate network are protected by alternative security controls such as multifactor authentication.

Access to the Oracle corporate network by suppliers and third parties is subject to limitations and prior approval per Oracle’s third-party network access policy.

ACCESS CONTROL

Access control refers to the policies, procedures and tools that govern 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.

- Least privilege is a system-oriented approach 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.
- Default-deny is a network-oriented approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source, and destination.

Oracle’s 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. This policy does not apply to publicly accessible, internet-facing Oracle systems or end users.

User Access Management

User Registration

Oracle user access is provisioned through an account provisioning system that is integrated with Oracle’s Human Resources database. Access privileges are granted based on job roles and require management approval.

Privilege Management

Authorization is dependent on successful 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: Does the user require this access for his job function?
- Segregation of duties: Will the access result in a conflict of interest?
- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

User Password Management

Oracle enforces strong password policies for the Oracle network, operating system, and database accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords.
Review of Access Rights
Oracle regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, Oracle takes appropriate actions to promptly terminate network, telephony and physical access.

Password Use
The use of passwords is addressed in Oracle's password policy. Oracle employees are obligated to follow rules for password length and complexity, and to keep their passwords confidential and secured at all times. Passwords may not be disclosed to unauthorized persons. Under certain circumstances, authorized Oracle employees may share passwords for the purpose of providing support services.

Segregation of Duties
Oracle enforces well-defined roles allowing for segregation of duties among operations staff. Operations are typically organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include database administrators, system administrators and network engineers. Teams using a “DevOps” model where more than one function may be performed by an employee are required to implement additional controls providing protection equivalent to segregation of duties.

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Access Control to Program Source Code
Oracle maintains strong security controls over its source code. Oracle's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories. Oracle's objectives with protecting its source code are twofold:

1. Protect the company's intellectual property
2. Protect Oracle and its customers against malicious attempts to alter Oracle's source code or exploit security vulnerabilities.

Technical Vulnerability Management
Oracle policy requires the deployment of the Oracle Critical Patch Updates (CPUs) and Security Alert patches as well as associated recommendations within a reasonable time of their release. Additional policies require remediation of vulnerabilities in non-Oracle technology.

The Oracle server security policy requires servers (both physical and virtual) owned and managed by Oracle and servers managed by third parties for Oracle to be physically and logically secured in order to prevent unauthorized access to the servers and associated information assets.

INFORMATION SECURITY INCIDENT RESPONSE
Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, Oracle has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.

Oracle evaluates and responds to events that create suspicion of unauthorized access to or handling of customer data, whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. Oracle’s Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to incidents. This policy authorizes Oracle Global Information Security (GIS) organization to provide overall direction for incident prevention, identification, investigation, and resolution within the Lines of Business (LoBs).

Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems within the Lines of Business (LoBs) are utilized to collect information and maintain a chain of custody for evidence during incident investigation. Oracle is capable of supporting legally admissible forensic data collection when necessary.
In the event that Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is also not shared externally.

**ORACLE’S RESILIENCE MANAGEMENT**

Oracle’s Risk Management Resiliency Policy defines requirements and standards for all Oracle Lines of Business (LOBs) plans for and response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test and evaluate business continuity capability for Oracle across lines of business and geographies. It authorizes a centralized Risk Management Resiliency Program (RMRP) Program Management Office (PMO) and defines the compliance oversight responsibilities for the program. The policy mandates an annual operational cycle for planning, evaluation, training, validation and executive approvals for critical business operations.

The Risk Management Resiliency Program (RMRP) objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting Oracle’s operations.

The RMRP approach is comprised of several subprograms: initial emergency response to unplanned and emergent events, crisis management of serious incidents, Information Technology Disaster Recovery and business-continuity management. The goal of the program is to minimize negative impacts to Oracle and maintain critical business processes until regular operating conditions are restored.

Each of these subprograms is a uniquely diverse discipline. However, by consolidating emergency response, crisis management, business continuity and disaster recovery, they can become a robust collaborative and communicative system.

**ORACLE SOFTWARE SECURITY ASSURANCE (OSSA)**

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle’s methodology for building security into the design, build, testing and maintenance of its products, whether they are used on-premises by customers or delivered through Oracle Cloud. Oracle’s goal is to ensure that Oracle’s products help customers meet their security requirements while providing for the most cost-effective ownership experience.

Oracle Software Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

- **Fostering security innovations.** Oracle has a long tradition of security innovations. Today this legacy continues with solutions that help enable organizations to implement and manage consistent security policies across the hybrid cloud data center: database security and identity management and security monitoring and analytics.
- **Reducing the incidence of security weaknesses in all Oracle products.** Oracle Software Security Assurance key programs include Oracle’s Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups and the use of automated analysis and testing tools.
- **Reducing the impact of security weaknesses in released products on customers.** Oracle has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

**Secure Coding Standards & Security Training**

So that Oracle products are developed with consistently high security assurance, and to help developers avoid common coding mistakes, Oracle employs formal secure coding standards.

Oracle Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc., and provide specific guidance on topics such as data validation and user management.

All Oracle developers must be familiar with these standards and apply them when designing and building products. The coding standards have been developed over a number of years and incorporate best practices as well as lessons learned from continued vulnerability testing by Oracle’s internal product assessment team. Oracle provides that developers are familiar with its coding standards by requiring that they undergo secure coding training. The Secure Coding Standards are a key component of Oracle Software Security Assurance and adherence to the Standards is assessed and validated throughout the supported life of all Oracle products.
Security Analysis & Testing

Security testing of Oracle code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals and are carried out by different teams. Functional and non-functional security tests complement each other to provide comprehensive security coverage of Oracle products.

Functional security testing is typically executed by regular product Quality Assurance (QA) teams as part of normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist reviews process.

Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis:

- Static security analysis of source code is the initial line of defense used during the product development cycle. Oracle currently uses the Fortify static code analyzer, as well a variety of internally developed tools, to help catch problems while code is being written.
- Dynamic analysis activity takes place during latter phases of product development. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within Oracle. Automatic tools employ fuzzing technique to test network-accessible product interfaces and protocols, while manual tools require making the modifications by hand.

Note that under Oracle Software Security Assurance, Oracle is committed to protecting all customers equally and will not provide information to individual customers. As a result, Oracle does not share security testing results that may result in disclosing certain vulnerabilities or inner working of security-sensitive functions. Oracle will not share artifacts collected under Oracle Software Security Assurance policies and programs.

CUSTOMER DATA PROTECTION

Oracle's media sanitization and disposal policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media include laptops, hard drives, storage devices and removable media such as tape.

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 at:

- 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.

REVISION HISTORY

Version 2.1 20 May 2021 Clarified operational responsibilities for Incident Response.