Oracle Corporate Security Practices

April 2024 | Version 3.3

INTRODUCTION

Oracle's mission is to help people see data in new ways, discover insights and unlock endless possibilities.

Oracle's security practices reflect the various ways Oracle engages with its customers:

- Oracle Corporate Security programs, policies and recommendations guide the IT teams managing Oracle's corporate network and systems as well as guiding the operational, cloud and services Lines of Business.
- 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 data in a customer's cloud tenancy.
- Third parties provided access to customer data by Oracle ("subprocessors") are required to contractually commit to materially equivalent security practices.

Oracle continually works to strengthen and improve the security controls and practices for internal operations and services offered to customers. These practices are subject to change at Oracle's discretion.

Companies that Oracle acquires are required to align with these security practices as part of the integration process. This duration and outcome of each aspect of the integration process relies on the size, complexity, contractual commitments and regulatory requirements applicable to the acquired company's products, services, personnel and operations.

Oracle's Cloud, Support, and Services lines of business have developed statements of security practices that apply to the respective service offerings. These are published and incorporated into applicable orders.

The purpose of this paper is to summarize key Oracle's security practices and programs. This paper does not exhaustively describe all security practices and programs which may be applicable and relevant to individual Lines of Business, products or services.

TABLE OF CONTENTS

ORACLE CORPORATE SECURITY

Oracle's Corporate Security Programs are designed to protect both Oracle and customer data, such as:

- 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 27002:2022 and ISO/IEC 27001:2022 standards and guide 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. The Chief Corporate Architect manages the Corporate Security departments which guide security at Oracle. These departments manage the corporate security programs, define corporate security policies, and provide global oversight for Oracle's security policies and requirements.

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.

Corporate Security Organizations

Global Information Security

Global Information Security (GIS) defines policies for the management of information security across Oracle. GIS provides direction and advice to help Lines of Business (LoBs) protect Oracle information assets (data), as well as the data entrusted to Oracle by our customers, partners and employees. GIS also coordinates the reporting of information security risk to senior leadership such as the Oracle Security Oversight Committee and Board of Directors. GIS programs direct and advise on the protection of data developed, accessed, used, maintained, and hosted by Oracle.

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 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. Physical security controls are described later in this document.

Corporate Security Architecture

The Oracle corporate security architect helps set internal information-security technical direction and guides Oracle's IT departments and lines of business towards deploying information security and identity management solutions that advance Oracle's information security goals. The corporate security architect works with Global Information Security and Global Product Security, and the Development Security Leads to develop, communicate and implement secure architectures.

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.

Line of Business Security Organizations

Lines of Business (LoB) have security teams which oversee their products, systems and cloud services managed by that organization. LoBs are required to define technical standards in accordance with Oracle's information security policies, as well as drive compliance to Oracle policies and standards within their organization and cloud service teams. LoBs are also required to comply with Corporate Security program requirements and directions. This paper does not describe LoB's specific security organizations, standards, and programs.

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.

Independent Review of Information Security

Oracle's Business Assessment & Audit is an independent global audit organization which performs global process and regional reviews. These reviews examine key business risk management protocols and compliance with Oracle policies, standards and select laws and regulations across Oracle's Lines of Business.

PRIVACY

The Oracle General Privacy Policy addresses information we collect in connection with your use of Oracle websites, mobile applications, and social media pages that link to the General Privacy Policy, your interactions with Oracle during in-person meetings at Oracle facilities or at Oracle events, and in the context of other online or offline sales and marketing activities.

The 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. Oracle Advertising Privacy Policy (also referred to as the 'Privacy Policy' or the 'Oracle Data Cloud Privacy Policy') informs consumers on the collection, use, sharing, and selling (collectively referred to as 'processing') of your personal information in connection with Oracle's provision of Oracle Advertising services designed to help Oracle's customers' and partners' online and offline marketing activities ('Oracle Advertising'). This policy also explains your privacy rights in relation to these processing activities.

CUSTOMER DATA PROTECTION

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

ASSET CLASSIFICATION AND CONTROL

Responsibility, Inventory, and Ownership of Assets

Oracle's formal information protection policy provides guidelines for all Oracle information classification and minimum handling requirements for each classification.

Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. Oracle's information systems asset inventory policy requires that Lines of Business (LoBs) mantain accurate and comprehensive inventories of information systems, hardware and software. This policy applies to all information assets held on any Oracle system, including both enterprise systems and cloud services.

Asset Classification and Control

Oracle categorizes information into four classes—Public, Internal, Restricted, and Highly Restricted—with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data:

- "Public" information is not sensitive, and there is no need with it remaining confidential to Oracle.
- "Oracle Internal" information must remain confidential to Oracle.
- "Oracle Restricted" and "Oracle Highly Restricted" information must remain confidential to Oracle and access within Oracle must be restricted on a "need to know" basis, with additional handling requirements for "Oracle Highly Restricted" information.

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.

Employees who fail to comply with Oracle policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.

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.

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.

Security Awareness Education and Training

Oracle promotes security awareness and educates employees through regular newsletters and 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 privacy principles and data handling practices required by company policy.

PHYSICAL SECURITY

Oracle 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 currently has implemented the following protocols in Oracle facilities:

- 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.
- Mixture 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 physical security events.
- Centrally managed electronic access control systems with integrated intruder alarm capability and CCTV monitoring and recording. The access control system logs and CCTV recordings are retained for a period of 30-90 days as per Oracle's Record Retention Policy which are based on the facility's function, risk level and local laws.

OPERATIONS MANAGEMENT

Protection Against Malicious Code

Oracle policy requires the use of antivirus protection and firewall software on endpoint devices such as laptops, desktops 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 organization keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates. They are responsible for:

- notifying internal Oracle system users of both any credible virus threats and when security updates are available
- providing automation to manage and 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 security event investigation and forensic purposes. Identified anomalous activities feed into security event management processes. 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 and other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

Network Controls

Oracle has implemented and maintains strong network controls for the protection and control of both Oracle and customer data during its transmission. Oracle's network security policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems. Unused network ports must be deactivated.

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 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.

Oracle's network security policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the Oracle corporate network, including network segmentation requirements. Oracle IT manages wireless networks and monitors for unauthorized wireless networks.

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, file, application, data in a database and network device.

- 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 configuration approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address.

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. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability and auditing functionality. This policy does not apply to customer end user accounts for Oracle cloud services.

User Access Management

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. Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include developers, database administrators, system administrators, and network engineers.

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?

Password Management

The use of passwords is addressed in the Oracle password policy. Oracle has strong password policies (including length and complexity requirements) for the Oracle network, operating system, email, database and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. System-generated and assigned passwords are required to be changed immediately on receipt.

Employees must keep their passwords confidential and secured at all times and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any Oracle system or applications passwords for non-Oracle applications or systems.

Periodic 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.

INFORMATION SYSTEMS DEVELOPMENT, AND MAINTENANCE

Technical Vulnerability Management

Oracle has formal practices designed to identify, analyze, and remediate the technical security vulnerabilities that may affect our enterprise systems and your Oracle Cloud environment.

The Oracle IT, security and development teams monitor relevant vendor and industry bulletins, including Oracle's own security advisories, to identify and assess relevant security patches. Additionally, Oracle requires that vulnerability scanning using automated scanning systems be frequently performed against the internal and externally facing systems it manages. Oracle also requires that penetration testing activities be performed periodically in production environments.

Oracle's strategic priority for the handling of discovered vulnerabilities in Oracle Cloud is to remediate these issues according to their severity and the potential impact. The Common Vulnerability Scoring System (CVSS) is one of the criteria used in assessing the relative severity of vulnerabilities and their potential impact. Oracle requires that identified security vulnerabilities be identified and tracked in a defect tracking system.

Oracle aims to complete all cloud remediation activities, including testing, implementation, and reboot (if required) within planned maintenance windows. Emergency maintenance will be performed as described in the Oracle Cloud Hosting and Delivery Policies and applicable Pillar documentation.

Oracle Software Security Assurance 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.

Customers and security researchers can report suspected security vulnerabilities: How to Report Security Vulnerabilities to Oracle or by submitting a Service Request in their designated support system.

INFORMATION SECURITY INCIDENT RESPONSE

A security incident is a security event that Oracle, per its incident response process, has determined results in the actual or potential loss of confidentiality, integrity, or availability of Oracle managed assets (systems and data).

Oracle will respond to information security events when Oracle suspects unauthorized access to Oracle-managed assets. Cloud customers are responsible for controlling user access and monitoring their cloud service tenancies via available tooling and logging.

Security Incident Policy and Operations

Oracle's Security Incident Management Policy defines requirements for reporting and responding to information security events and incidents. This policy authorizes the Oracle Global Information Security organization to provide overall direction for security event and incident preparation, detection, investigation, resolution and forensic evidence handling across Oracle's Lines of Business (LoB). This policy does not apply to availability issues (outages) or to physical security events.

Global Information Security further defines roles and responsibilities for the incident response teams within the LoBs. All LoBs must comply with Global Information Security guidance for managing information security events and implementing timely corrective actions.

Upon discovery of a security event, Oracle incident response plans support rapid and effective event triage, including investigation, response, remediation, recovery, and post-incident analysis. LoB incident response teams, as required by the Security Incident Management Policy, conduct post-event analysis to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the LoBs to collect information and maintain a chain of custody for evidence during event investigation. Oracle can support legally admissible forensic data collection when necessary.

Notifications

If Oracle determines a security incident involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts, suspected incidents and incident history are not shared externally.

ORACLE SOFTWARE SECURITY ASSURANCE

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 services.

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 organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the cloud.
- **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.

Coding Standards & Security Training

Developing secure software requires consistently applied methodologies across the organization; methodologies that conform to stated policies, objectives, and principles. Oracle's objective is to produce secure code. To that end, Oracle requires that all of development abide by secure coding principles that are documented and maintained to remain relevant. Developers must be familiar with these standards and apply them when designing and building Oracle products.

Oracle Secure Coding Standards and related guidance have evolved and expanded over time to encompass emerging technologies such as Artificial Intelligence and Machine Learning (AI/ML) and address the most common issues affecting Oracle code, new threats as they are discovered, and new customer use cases for Oracle technology.

All Oracle staff are required to take security training. Technical development staff, up to and including vice presidents, who are involved in building, maintaining, customizing or testing product code are required to take an OSSA awareness course.

Additionally, Oracle adapted its secure coding principles and created training material for use by its consulting and services organizations when they are engaged in producing code on behalf of customers.

Security Analysis & Testing

Oracle requires that security testing be performed for its on-premises and cloud products. 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 support comprehensive security testing 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 uses a commercial static code analyzer as well as a variety of internally developed tools, to catch problems while code is being written.
- Dynamic analysis activity takes place during latter phases of product development: at the very least, the product or component should be able to run. 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 at Oracle. Automatic tools employ fuzzing technique to test network-accessible product interfaces and protocols, while manual tools require making the modifications by hand.

Oracle will not provide customers sensitive security assurance artifacts (including but not limited to static code analysis reports). Oracle will not submit its product to third-party static code assessments. For more information, see MOS Article: General Instructions for Submitting Security Questionnaires to Oracle (Doc ID 2337651.1).

Security Fixing Policies

The Critical Patch Update (CPU) is the primary mechanism for the backport of security bug fixes for all Oracle on-premises products. Critical Patch Updates are available to customers with valid support contracts. Critical Patch Updates are released quarterly on the third Tuesday of January, April, July, and October. Oracle retains the ability to issue out of schedule patches or workaround instructions in case of particularly critical vulnerabilities and/or when active exploits are reported in the wild. This program is known as the Security Alert program.

Vulnerabilities are remediated by Oracle in order of the risk they pose to users. This process is designed to patch the security defects with the greatest associated risk first in the Critical Patch Update, resulting in optimizing the security posture of all Oracle customers.

A standardized CPU schedule helps organizations plan their security maintenance windows. The CPU schedule is designed to avoid typical blackout dates during which customers cannot typically alter their production environments.

As much as possible, Oracle tries to make Critical Patch Updates cumulative; that is, each Critical Patch Update contains the security fixes from all previous Critical Patch Updates. This provides customers the ability to catch up quickly to the current security release level, since the application of the latest cumulative CPU resolves all previously addressed vulnerabilities.

Applicability of Critical Patch Updates and Security Alerts to Oracle Cloud Environments

The Oracle Cloud operations and security teams regularly evaluate Oracle's Critical Patch Updates and Security Alerts as well as relevant third-party security updates as they become available and apply the relevant patches in accordance with applicable change management processes.

Source Code Protection

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 Software Security Assurance policies and practices are designed to prevent the introduction of security vulnerabilities in Oracle-developed code. Additionally, Oracle maintains strong controls over the technical description of security vulnerabilities in Oracle code. Oracle's Security Vulnerability Information Protection Policy defines the classification and handling of information related to product security vulnerabilities and requires that information concerning security bugs be recorded in a tightly controlled database.

Oracle's policies prohibit the introduction of backdoors into its products. Backdoors are deliberately (and maliciously) introduced code intended to bypass the security controls of the application in which it is embedded. Backdoors do not include:

- Unintentional defects in software that could lead to a weakening of security controls (security bugs)
- Undocumented functionality designed to be generally inaccessible by customers but serves a valid business or technical purpose (diagnostics and troubleshooting utilities)

Oracle assesses third-party software and hardware to avoid the use of products:

- With known vulnerabilities
- Developed with poor security assurance
- That may potentially include backdoors or other malicious components

External Security Evaluations

Oracle submits certain products for external security evaluations. These evaluations involve rigorous testing by independently accredited organizations ("labs") with further oversight and certification completed by government bodies. Independent verification helps provide additional assurance to Oracle customers with regards to the security posture of the validated products. Organizaations in many industries have business and compliance requirements that imply the use of validated products. Such evaluations include Common Criteria and FIPS 140.

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: emergency response to unplanned and emergent events, crisis management of serious incidents, 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. By consolidating emergency response, crisis management, business continuity and disaster recovery, they can become a robust collaborative and communicative system.

REVISION HISTORY

Version 3.3	04 Apr 2024	Updated introduction, information security incident response and Oracle Software Security Assurance sections
Version 3.2	12 Sep 2023	Clarified physical security and technical vulnerability management controls
Version 3.1	20 Jan 2023	Expanded Oracle Software Security Assurance (OSSA) section and updated the order of sections.
Verison 3.0	30 Sep 2022	Updates to all sections.
Version 2.1	20 May 2021	Clarified operational responsibilities for Incident Response.
Version 2.2	10 Sep 2021	Added wireless network management practices. Updated Operations Management, Incident Response, Technical Vulnerability Management and Access Control sections.
Version 2.3	22 Apr 2022	Clarified Global Information Security and Incident Response sections

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com   facebook.com/oracle   twitter.com/oracle

- This document is provided *for* information purposes only, and the contents hereof are subject to change without notice.
- This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document.
- This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle Corporate Security Practices
April, 2024