Effective Date: 07-December-2023

This section describes the changes made to the Global Customer Support Security Practices dated April 11, 2023, and reflected in the Global Customer Support Security Practices dated December 07, 2023:

Database Diagnostic Data
- Inserted new second bullet for clarity as per below:

  When AHF is not configured, diagnostic collection is performed using Automatic Diagnostic Repository (ADR). ADR is then packaged using the Incident Packaging Services (IPS). Further details can be found in MOS note :- Collecting Diagnostics for Oracle Support (Doc ID 411.1) found at https://support.oracle.com/epmos/faces/DocumentDisplay?id=411.1.

Oracle Autonomous Health Framework
- Added, “to Oracle” in the seventh bullet second sentence for clarity.

Oracle Autonomous Health Framework for Platinum Services
- Third paragraph added “reactive” after “patching” for clarity.

Oracle Configuration Manager (OCM)
- Removed entire section below.

Oracle Configuration Manager (OCM)
Oracle Configuration Manager (OCM), available from My Oracle Support, is used to collect and analyze Your environment configuration information. OCM gathers configuration information and loads that information to a Customer Configuration Repository (CCR) at Oracle. Providing the auto-collected configuration information to Oracle is voluntary and is done only with Your consent. You control the installation and configuration of OCM. If You configure it to send information to Oracle, OCM pushes Your selected configuration uploads to the Oracle CCR on a regular basis. OCM only initiates outbound communications to Oracle and does not listen for inbound communications.

- In order to collect detailed database configuration information, Your Oracle database must be configured with certain OCM provided PL/SQL procedures. OCM provides scripts that You can run against the Oracle database. These scripts create a database account called ORACLE_OCM in the Oracle database. The account stores the PL/SQL procedures that collect the configuration information and owns the database management system (DBMS) job that performs the collection. After the account has been set up, it is immediately locked, and the password expired as login privileges are no longer required or desired.

- You can choose to enable auto-update for OCM. OCM auto-update uses authentication and encryption. Before any downloaded update is applied, the digital signature is validated, confirming the update was signed with a certificate issued to Oracle (this certificate is different from the certificate used to secure the communications link). The signing software is on a system not connected to the Oracle corporate network.

- When transmitting configuration information to Oracle, OCM uses industry standard protocol (HTTPS) as well as 128 bit encryption using public/private key exchange (otherwise known as asymmetric encryption) for all communications. OCM authenticates Oracle as the recipient by interrogating the certificate returned by Oracle (a recognized certificate authority, specified by Oracle, issues the certificate to Oracle).

- The OCM upload server(s) are deployed in a firewall protected DMZ network. There is no direct Internet connection to the application server. The OCM site resolves to an IP address registered to a virtual server on a SSL Accelerator/Reverse Proxy to encrypt the information and mask the location of the source and destination. At the termination point of the SSL encryption, reverse proxy forwards traffic to the application server. Configuration information is then pushed to the CCR database tiers on Oracle’s internal network, and the files containing the configuration information are then deleted.
• Oracle utilizes a network Intrusion Detection Systems (nIDS) to provide continuous surveillance on the OCM upload site to intercept and respond to security events as they are identified.
• Oracle conducts quarterly vulnerability scans on the OCM upload server to detect known vulnerabilities.
• The configuration information collected in the CCR is secured inside Oracle's Austin Data Center and protected by Oracle network security infrastructure and security controls.
• You may request deletion of Your configuration information by logging an SR indicating the specific configuration information and scope of the deletion request.
• For Platinum Services, OCM is sometimes installed on the Oracle Advanced Support Gateway ("gateway"), described below. Communication is routed over the encrypted VPN established from the gateway to Oracle.

For further information about what information is collected by OCM and how it is used and protected, please consult the OCM license terms and other supporting documentation available on My Oracle Support (https://support.oracle.com).

Oracle Advanced Support Gateway
• Added third bullet for clarity, “The security guide for the Oracle Advanced Support gateway can be found here.”

Other Updates
• Updated hyperlinks
• Corrected spelling
• Reordered sections for clarity

April 11, 2023

Overview
• In the first paragraph added, Cloud in after “performing,” and removed, “standard.”

Security Practices

Web-Based Customer Support Sites
• In the first paragraph added, “(such as My Oracle Support and Oracle Service Cloud),” after, “web sites.”
• In the first paragraph added, Cloud after "software."
• In the first paragraph, last sentence, added, “Your agreement(s) with Oracle may specify additional or other support mechanisms.”
• In the second paragraph added, "are,” after, “support policies.”
• Removed the following language after the hyperlink, “for more complete information about which Oracle software and hardware are supported by each support web site
• Under My Oracle Support section:
  o Twelfth bullet, after "virtual server" removed, "on a SSL Accelerator/Reverse Proxy," and added, “TLS 1.2,” and removed, “At the termination point of the SSL encryption, a reverse proxy forwards traffic to the application server.”

Technologies Used to Perform Technical Support
• Under Collaboration Tools:
  o Removed “Secure Socket Layer (SSL)” and capitalized the “e” in “Encryption.”
  o Shared Shell section, fifth bullet (third sub-bullet), added, “session but,” after, “Shared Shell.”
• Under Tools Used
  o Removed, “are available on My Oracle Support.”
  o Auto Service Request – for Storage (Service Delivery Platform V2) deleted the below and merged with Auto Service Request – for Systems and Storage.
Auto Service Request – for Storage (Service Delivery Platform V2)
The ASR Service Delivery Platform (SDP) is an Oracle configured and managed server installed on Your site that connects to and monitors Your supported Oracle storage devices. The SDP uses the core ASR infrastructure at Oracle, so the ASR infrastructure, network, and security practices described above for ASR for Systems are the same for SDP. Oracle also employs the following additional security measures for SDP:

- All SDP traffic between You and Oracle is initiated either from an Oracle-supplied Virtual Private Network (VPN) router or a customer VPN-capable device to Oracle’s VPN termination routers.

- Oracle service engineers accessing Your storage devices via VPN are authenticated and assigned various roles that are part of the assigned SDP group privileges. An engineer's credentials are encrypted using a secret key. SDP uses the HTTP protocol for authentication purposes; however, since HTTP does not encrypt the user's password, the user's session is encrypted using a 2048 bit RSA certificate.

- The production data stored on Your storage devices is not visible to Oracle service engineers.

- The installation of the SDP server involves Your formal review and approval, as it may require You to make network changes prior to deployment. The encryption type and hash algorithm of the VPN tunnel is reviewed and agreed to during this formal review.

- The SDP security mechanisms follow the CERT/Coordination Center guidelines for remote administration tools.

  - Auto Service Request – for Systems
    - Updated the name of this section to be Auto-Service Request – for Systems and Storage
    - Added the below to the end of the first paragraph

    The production data stored on Your storage devices is not visible to Oracle service engineers. The ASR processes are facilitated by ASR Client software which can be imbedded in the product itself or act as a standalone application such as ASR Manager or StorageTek Service Delivery Platform v2 (SDP2).

    - In the first bullet updated
      - “1024-bit” to “2048-bit”

    - In the second bullet updated
      - Removed, "using RSA with RC4 (128 bit) SSL encryption," and replaced with, “TLS 1.2 and AES256 symmetric encryption.”

    - In the first and second bullet updated
      - “ASR Manager” to “ASR Client.”

  - Database Diagnostic Data
    - No change (moved alphabetically)

  - Oracle Autonomous Health Framework
    - Added new section

Oracle Autonomous Health Framework
Oracle Autonomous Health Framework (AHF) [https://docs.oracle.com/en/engineered-systems/health-diagnostics/autonomous-health-framework/index.html](https://docs.oracle.com/en/engineered-systems/health-diagnostics/autonomous-health-framework/index.html) is a lightweight and non-intrusive diagnostic collection and compliance check package, which You can install a variety of Oracle hardware and software components including Oracle Cloud, Engineered and non-Engineered Systems. AHF contains Oracle ORAchk, Oracle EXAchk, and Oracle Trace File Analyzer. You have access to Oracle AHF as a value add-on to Your existing support contract.
• It is available for download on My Oracle Support, Doc ID 2550798.1 and described in more detail at https://docs.oracle.com/en/engineered-systems/health-diagnostics/autonomous-health-framework/index.html.

• You install the AHF software you downloaded from Oracle, or you activate and configure the software which is shipped as part of the supported Oracle environment and available by default. In all cases, You control the installation and configuration of AHF.

• In order for AHF to collect detailed diagnostic and configuration information from Your Oracle environment, AHF must be installed using privileged credentials to obtain the fullest of capabilities. AHF has reduced capabilities when You install it using a non-privileged user. If you are unable to install using a privileged user, then install AHF using the account that owns the Oracle Home.

• You choose to enable auto-update for AHF using the incorporated AHF scheduler if Your Oracle environment supports it. OpenSSL is required for all environments to support auto-update. The AHF scheduler automatically upgrades AHF when it finds a new version either at the Software stage location or at the Rest Endpoints (Object Store) defined by You.

• The AHF scheduler is configured to run weekly. It checks if a new version of AHF is available, will automatically upgrade AHF to the latest version without changing any of the saved configurations. You can choose to disable auto-update at any time. AHF auto-update uses authentication and encryption.

• You configure AHF to execute recurring compliance checks at regular intervals, send email notifications when the compliance check completes, and purge collection results after a pre-determined period. In this way, AHF helps automate the collection of diagnostic and configuration information on Your supported Oracle environment. By default, AHF will not capture, collect, transport, or use any production data from the system or device on which the package is run.

• Your supported Oracle environment stores collected non-production data locally in a series of files and You use AHF to upload those files to Oracle for both pro-active analysis and reactive service request resolution. You may choose to upload AHF collected files either independently or as attachments through the SR logging and update process on My Oracle Support. Any AHF uploads to Oracle service requests will be stored in the secured GCS repository. AHF only initiates outbound communications to Oracle and does not listen for inbound communications.

  o Oracle Autonomous Health Framework for Platinum Services
  • Added new section

Oracle Autonomous Health Framework for Platinum Services
In the case of Oracle Platinum Services, AHF is the diagnostic tool used Oracle installs and configures AHF on Your Certified Platinum Configuration as part of the process to initiate Oracle Platinum Services, using privileged credentials You provide. For Oracle Platinum Services, AHF is also configured to auto-update AHF when a new version becomes available.

AHF is used to:
• Collect diagnostic files when auto-generated SRs are created for certain faults and events and
• Automatically execute proactive compliance checks periodically or on demand.

The resulting diagnostic files and compliance check reports are uploaded to the Oracle Advanced Support Gateway ("gateway") for the purpose of delivering Oracle Platinum Services including, but not limited to, patching and proactive analysis.

• The EXAchk xml/html report files are also stored on the Oracle Advanced Support Platform specifically for proactive analysis and patch recommendations. The default retention period for these files on the Oracle Advanced Support Platform is seven years.

• Diagnostic collections (tfactl diagcollect) output files are purged from the gateway after they are uploaded to a service request. By default, any diagnostic collections not uploaded to SRs due to failure conditions are purged after fourteen days.
• For other AHF supported compliance checks and file collections such as Exachk, Orachk, SunDiag, AWR, ILOM, Exawatcher, collections are automatically updated periodically and only the file output of the latest two valid compliance checks collection of any type, per host, are retained on the gateway due to disk space considerations.

You can choose to disable AHF at any time; but in doing so, you will limit Oracle’s ability to deliver Oracle Platinum Services as described here: https://www.oracle.com/us/support/library/platinum-services-policies-1652886.pdf.

  o Oracle Configuration Manager (OCM)
    ▪ Moved alphabetically
    ▪ Removed from the third bullet, “Secure Socket Layer (SSL) and.”
  o Last paragraph exposed embedded link for My Oracle Support (https://support.oracle.com)

Advanced Support Gateway Services

Data Processing
• Added new section

  **Data Processing**

  Services Data is data that resides on Oracle, customer or third-party systems to which Oracle is provided access to perform services (including Cloud environments as well as test, development and production environments that may be accessed to perform Oracle consulting and support services). Oracle treats services data according to the terms of this policy and treats services data as confidential in accordance with the terms of your order for services.

  Aggregated SR data may be used to analyze, develop, improve and optimize the use, function and performance of our sites and products and services, and to provide personalized product and service recommendations to customers.

  GCS will adhere to the following when processing your data:

  • Oracle’s Services Privacy Policy, available at https://www.oracle.com/legal/privacy/services-privacy-policy.html; and
  • the applicable version of the Oracle Data Processing Agreement for Oracle Services, available at http://www.oracle.com/dataprocessingagreement.

Other Updates
• Updated hyperlinks
• Corrected spelling

---

March 07, 2022
• **Added fourth bullet, first sub-bullet, to TECHNOLOGIES USED TO PERFORM TECHNICAL SUPPORT Section under Collaboration Tools**

  You may permit Oracle, Zoom Remote Control access for diagnostic and resolution purposes. At any time, You may Stop Remote Control in Zoom.

---

December 14, 2021

**Overview**
• Removed comma after “services”

Security Practices
• Added comma after “standards”

Global Customer Support Operation
November 29, 2021

New Template

October 07, 2019

Table of Contents

- Deleted Table of Contents:

<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Overview</td>
</tr>
<tr>
<td>2. Information Security Program</td>
</tr>
<tr>
<td>3. Global Customer Support Operation</td>
</tr>
<tr>
<td>4. Web-Based Customer Support Sites</td>
</tr>
<tr>
<td>5. Security of Technologies Used to Perform Technical Support</td>
</tr>
<tr>
<td>6. Advanced Support Gateway Services</td>
</tr>
<tr>
<td>7. Data Management and Protection</td>
</tr>
<tr>
<td>8. Media Returns</td>
</tr>
<tr>
<td>9. Network Security</td>
</tr>
<tr>
<td>10. Physical Security</td>
</tr>
<tr>
<td>11. Oracle Enterprise Tape Analysis and Data Recovery Security Practices</td>
</tr>
<tr>
<td>12. Oracle Corporate Security Practices</td>
</tr>
</tbody>
</table>

Overview

- Deleted the title, “Overview”
- Inserted the following at the beginning of the first sentence, “These Oracle Global Customer Support Security Practices (“Security Practices”) supplement the Oracle Corporate Security Practices and identify the additional security practices that…”
- Inserted new second and third sentences, “As used herein, “Your data” means any data stored in Your computer systems and accessed remotely or provided to Oracle for the performance of the services. Capitalized terms that are not otherwise defined in these Delivery Policies shall have the meaning ascribed to them in the Oracle agreement, Your order or the policy, as applicable.”
- Deleted the last sentence, “As used herein, “your data” means any data stored in your computer system and accessed remotely while performing the services. Oracle is responsible for its employees’ and subcontractors’ provision of technical support (including any resulting access to and use of your data) in accordance with the terms of your order and these Security Practices.”

Security Policies

- Replaced the section:

“1. Information Security Program”
Oracle’s information security management program is aligned with ISO/IEC 27001:2005, and Oracle has adopted and implemented information security practices and procedures in relation to: information security policies; management responsibility for security; information asset ownership and classification; physical and logical access security; network, media and O/S security management and control; audit and monitoring; configuration management, and change control; risk assessment, mitigation and remediation; vulnerability management; incident reporting and incident management; business continuity management; and compliance reporting.

GCS practices comply with corporate policies established by Oracle’s Global Information Security and Global Product Security organizations and with technical security standards and procedures set by Oracle’s IT and Support organizations.

GCS also provides new hire training courses, custom training for specific workflows and business cases, and regular ‘hot topics’ training and communications for GCS staff.”

With:

“I. Security Policies

Oracle’s Corporate Security Practices cover the management of security for both its internal operations as well as the services Oracle provides to its customers, and apply to all Oracle employees. These policies, which are generally aligned with the ISO 27002 Code of Practice and ISO 27001 standards, govern all areas of security applicable to the performance of standard software and hardware technical support services. You are strongly encouraged to implement Your own comprehensive system of policies, standards and procedures, according to Your risk-based assessments and business requirements.”

Global Customer Support Operation

- In the second sentence after, “SRs are processed by GCS engineers,” inserted, “including Oracle employees and contractors,”
- Inserted the following as a new third sentence, “Oracle is responsible for its employees' and subcontractors’ provision of the technical support services (including any resulting access to and use of Your data) in accordance with the terms of Your order and these Security Practices.”

My Oracle Support

- In the first paragraph after, “My Oracle Support is” replaced, “the” with, “Oracle’s” and replaced, “website” with, “web-based”
- In the first sentence of the second paragraph replaced, “employs” with, “currently implements”
- In the first bullet replaced, “Transport Layer Security (TLS)” with, “Secure Socket Layer (SSL)”
- In the second bullet, capitalized, “Your”
- In the third bullet, capitalized, “You” and “Your”
- In the first sentence of the third bullet replaced, “approve/reject” with, “are responsible for approving or rejecting”; inserted, “customer” after “from”; inserted, “My Oracle Support” before, “accounts and CSI associations”; inserted, “My Oracle Support” after, “CSI associations to existing”; and inserted a period before, “You”
- In the second sentence of the third bullet inserted, “also” before “responsible”; inserted, “My Oracle Support” after, “de-provisioning Your”; and inserted, “in accordance with Your own access policies” at the end of the sentence
- In the fourth bullet, capitalized, “Your” and replaced, “e.g.” with, “for example”
- In the fifth bullet, inserted, “or add” before, “access privileges”
- In the seventh bullet, replaced, “TLS” with, “SSL”
- In the eighth bullet capitalized, “You” and “Your”
- In the eighth bullet in the first sentence inserted, “GCS” before “engineer”
- In the eighth bullet in the second sentence inserted, “GCS” before, “engineer”; replaced, “preserved and treated in a fashion similar to” with, “retained along with any corresponding”; replaced, “(as specified below)” with, “You have submitted to Oracle.”
- In the eighth bullet in the third sentence inserted, “GCS” before, “engineers”; and in the last sentence, replaced, “Service Request” with, “SR”
• In the tenth bullet, replaced, “customers and customer data” with, “You or Your Content”
• In the 11th bullet in the first sentence replaced, “the creation of” with, “You to create” and in the second sentence replaced, “these” with, “Guided Resolution”
• In the 13a bullet in the fourth sentence inserted, “up to” before, “6 months”; inserted, “either (i)” before, “the bug is closed”; inserted, “or (ii)” publication of a fix for the bug involving a security vulnerability as part of Oracle’s Critical Patch Update (CPU) process” before, “and is then deleted.”
• In the 13a bullet in the fifth sentence deleted, “However,”; inserted, “in a product” after, “code fix”; replaced, “for” with, “while”; deleted, “life of the Oracle” before, ”product”; inserted, “is supported” after, “product”; replaced, “ensure that” with, “prevent”; and replaced, “is not” with, “from being”
• Inserted a new 14th bullet, “My Oracle Support SR data and records related to the SR are kept for 10 years from the date that the record was created.”

Technologies Used to Perform Technical Support – Collaboration Tools
• In the first paragraph, inserted, “Cisco Webex for programs and” before, “Oracle Shared Shell” and inserted, “for hardware” at the end of the sentence
• In “Additional Details” capitalized, “You” and “Your”
• In “Additional Details – Cisco Webex conferencing”, in the third bullet replaced, “supports up to” with, “requires”
• In “Additional Details – Shared Shell”, deleted the third bullet, “Shared Shell includes the ability to transfer files between you and other session participants. File transfer requests can be initiated by you or any other session participant. Only you approve requests to send or receive files.”

Technologies Used to Perform Technical Support – Tools Used for Programs & Hardware
• Capitalized, “You” and “Your”
• In the second bullet, inserted, “such system telemetry” after, “When transmitting”

Technologies Used to Perform Technical Support – Tools for Programs – Oracle Configuration Manager (OCM)
• Capitalized, “You” and “Your”
• In the third bullet, replaced, “Transport Layer Security (TLS)” with, “Secure Socket Layer (SSL)”
• In the fourth bullet in the second sentence inserted, “a SSL” after, “virtual server” and in the third sentence replaced, “TLS” with, “SSL”
• In the seventh bullet replaced, “teams” with, “controls”
• In the eighth bullet replaced, “a Service Request” with, “an SR”

Technologies Used to Perform Technical Support – Tools for Programs – Remote Diagnostic Agent (RDA)
• Capitalized, “You” and “Your”
• In the second paragraph replaced, “this” with, “RDA”
• In the third bullet deleted, “Explorer file upload” and, “the” before, “last five”

Technologies Used to Perform Technical Support – Tools for Programs – Database Diagnostic Data
• Capitalized, “You” and “Your”

Technologies Used to Perform Technical Support – Tools for Hardware – Auto Service Request – for Systems
• Capitalized, “You” and “Your”
• In the second bullet replaced, “1024” with, “2048”

Technologies Used to Perform Technical Support – Tools for Hardware – Auto Service Request – for Storage (Service Delivery Platform)
• Capitalized, “You” and “Your”

Advanced Support Gateway Services – Oracle Advanced Support Gateway
• Inserted, “Advanced Support” before, “Gateway” in the title
• Capitalized, “You” and “Your”
• In the second bullet replaced, “1024” with, “2048”
Advanced Support Gateway Services – Oracle Continuous Connection Network
- Capitalized, “You” and “Your”
- In the last bullet, in the last sub-bullet inserted, “SSL” before “VPN”

Advanced Support Gateway Services – Oracle Advanced Support Platform
- Capitalized, “You” and “Your”
- In the first paragraph inserted, “near” after “view”
- In the first bullet deleted, “and only accessible by authorized GCS personnel” at the end of the bullet

Advanced Support Gateway Services – Oracle Analyst Access and Logging
- Capitalized, “You” and “Your”
- Inserted, “and retained for 1 year” at the end of the second paragraph

Data Management and Protection
- Capitalized, “You” and “Your”
- In the first sentence of the first paragraph inserted, “Corporate Security Practices referenced above and” after “Oracle’s”
- Deleted the second paragraph, “GCS retains your data for the periods specified herein, except as otherwise required by law, and adheres to corporate security policies for secure disposal of your data and media.”

Data Management and Protection – Data Management
- Capitalized, “You” and “Your”
- In the first paragraph in the second sentence inserted, “You Provide” before “Oracle; replaced, “accesses your data” with, “access to Your personal information”; inserted, “the” before “technical support”; inserted, “services” after “technical support”; and inserted, “following:” after “adhere to the”
- Replaced, “privacy practices described at https://www.oracle.com/legal/privacy/services-privacy-policy.html” with 2 new bullets:
  - Oracle’s Services Privacy Policy, available at https://www.oracle.com/legal/privacy/services-privacy-policy.html; and
- Deleted the second paragraph, “Access to your data is granted by Oracle based on job role/responsibility, with access provisioned from a central provisioning repository that is subject to approval processes.”
- In the second paragraph in the first sentence replaced, “your data” with, “Your data, including any personal information,”
- In the second paragraph deleted the third sentence, “If you provide any personally identifiable information to Oracle for use in the performance of the services, you are responsible for providing any required notices and/or obtaining any required consents relating to collection and use of such data.”
- In the fourth paragraph in the first sentence replaced, “some customers may have executed agreements with Oracle governing Global Customer Support’s handling of the personal data of residents in the European Economic Area (“EEA Personal Data”) as well as” with, “if You would like to submit personal information subject to Applicable European Data Protection Law (as such term is defined by the Data Processing Agreement for Oracle Services) or”; and deleted, “If you would like to submit EEA Personal Data or PHI)”
- In the first bullet inserted, “For PHI execute” at the beginning of the bullet
- In the second bullet replaced, “EEA Personal Data” with, “personal information subject to Applicable European Data Protection Law”
- In the third bullet replaced, “EEA Personal Data” with, “personal information subject to Applicable European”; inserted, “Protection Law” after “Data”; and replaced, “SR” with, service request
- In the fourth bullet inserted, “personal information subject to Applicable European Data Protection Law (also which may be designated as)” before EEA Personal Data”

Data Management and Protection – Reporting Breaches
- Deleted this section:

"Reporting Breaches"
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.

Where Oracle Global Information Security determines that customer data has been subject to unauthorized access (including by an Oracle employee) that compromises the confidentiality, integrity or availability of the customer data, Oracle promptly reports such unauthorized access to the customer, unless otherwise required by law."

Data Management and Protection – Disclosure
- Deleted this section:
  
  "Disclosure
  You should not disclose your data to Oracle except to the extent required for Oracle to perform the services for you. Oracle will not disclose your data, 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 disclosure before disclosure is made."

Data Management and Protection – Audit
- Deleted this section:
  
  "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 may 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 your agreement with Oracle."

Media Returns
- Capitalized, “You” and “Your”
- In the second sentence of the second paragraph deleted, “meet both the U.S. Department of Defense Sanitizing Standard 5220.22-M and”; after, “National Institute of Standards and Technology” replaced, “NISTSP800-88” with, “NIST SP800-88”; and in the last sentence replaced, “pulverizes” with, “destroys”

Network Security
- Deleted this section:
  
  “Network Security
  Oracle uses firewall and router rules, access control lists and segmentation on the Oracle corporate network. Oracle’s Global IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication. Oracle audits corporate network usage for suspicious activity.

  Remote workers use VPN encrypted network traffic via industry standard VPN or equivalent technologies."
Physical Security

• Deleted this section: "Physical Security"

Oracle maintains the following physical security standards for the Oracle facilities from which environments may be accessed ("service location(s)"):
  o Physical access to service locations is limited to Oracle employees, subcontractors and authorized visitors.
  o Oracle employees, subcontractors and authorized visitors are issued identification cards that must be worn while on the premises.
  o Visitors 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 with Oracle.
  o Oracle Corporate Security monitors the possession of keys/access cards and the ability to access service locations. Staff leaving Oracle’s employment must return keys/cards and key/cards are deactivated upon termination.
  o After-hours access to service locations is monitored and controlled by Oracle Corporate Security.
  o Oracle Corporate Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.”

Oracle Enterprise Tape Analysis and Data Recovery

• Replaced the title, “Oracle Enterprise Tape Analysis and Data Recovery Security Practices” with, “Oracle Enterprise Tape Analysis and Data Recovery”
• Capitalized, “You” and “Your”
• Replaced the last sentence of the second bullet, “The engineer then places the tape in an RFID locker system until the analysis/data recovery process can begin.” with, “The tape is stored throughout the analysis/data recovery process in a locked cabinet within the data recovery lab. Media is stored in a separate drawer by customer.”
• In the third bullet replaced, “small” with, “limited”

Corporate Security Practices

  □ Deleted this section:
  "Oracle Corporate Security Practices"

  Computer Virus Controls

On all computers issued to Oracle employees, Oracle maintains a mechanism within the Oracle network that scans all email sent both to and from any Oracle recipient for malicious code and deletes email attachments that are infected with known malicious code prior to delivery. Oracle requires all Oracle employee computers to be loaded with virus protection software. Oracle also maintains mechanisms to ensure that virus definitions are regularly updated, and that updated definitions are published and communicated to employees. These mechanisms also give employees the ability to download new definitions and update virus protection software automatically. From time to time, Oracle Global Information Security will conduct compliance reviews to ensure that employees have the virus software installed and that virus definitions on all desktops and laptops are updated.

Personnel

Oracle places strong emphasis on reducing risks of human error, theft, fraud, and misuse of Oracle assets and systems. Oracle’s efforts include personnel screening, making personnel aware of security policies, and training employees to implement security policies. For example, employees are expected to have a clear understanding of password policies, ‘clear desk’ policies, and policies concerning the handling of confidential data.

Access Rights

Oracle employees receive access to systems on the basis of need to know and least-privilege. Oracle tools implement role-based access systems. Approval of employee accounts and privileges is managed
centrally. Oracle employee user accounts are coupled to the central Sign On framework to ensure immediate removal access upon employee termination or re-assignment.

**Employee Training**
Oracle employees are required to complete an online data privacy awareness-training course. The course instructs employees on the definitions of data privacy and personal data, recognizing risks relating to personal data, understanding their responsibilities for data and reporting any suspected privacy violations. Employees also are required to complete training in corporate ethics.

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

Oracle promotes awareness of, and educates employees about, issues relating to security. Oracle 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.

**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 information security policies, procedures and practices may be subject to disciplinary action, up to and including termination.”

August 23, 2016

**My Oracle Support Security**
- In the first bullet replaced, “Secure Socket Layer (SSL)” with, “Transport Layer Security (TLS)”
- In the seventh bullet, in the third sentence, removed “SSL” and in the fourth sentence, replaced, “SSL” with, “TLS”

**Security of Technologies Used to Perform Technical Support – Collaboration Tools**
- In the first sentence, changed, “three” to, “two” and deleted, “Oracle Beehive Conferencing and Cisco Webex for programs” and deleted, “for hardware” after the last reference to, “Cisco Webex”
- Deleted the last bullet in the first paragraph
- Deleted the first sub-bullet point
- Added two new sub-bullet points to this section
- Under, “Additional Details:” in the, “Shared Shell” bullet, added a new sixth sub-bullet

**Security of Technologies Used to Perform Technical Support – Tools Used for Programs & Hardware**
- In the third bullet replaced, “Secure Socket Layer (SSL)” with, “Transport Layer Security (TLS)”
- In the fourth bullet, in the third sentence, removed “SSL” and in the fourth sentence, replaced, “SSL” with, “TLS”
- In the, “Tools for Programs” section, under, “Remote Diagnostic Agent (RDA)” in the third paragraph, third bullet point, after, “Oracle retains the first…”, added, “Explorer file uploaded” and, “the” after, “…and”
• In the, “Tools for Hardware” section, under, “Auto Service Request – for Systems”, in the second bullet, after, "...from the ASR assets..." deleted, “and performs operations to validate and suppress an alarm if necessary”; replaced, “128 bit” with, “256 bit”; and replaced, “SSL” with, “TLS”

Oracle Continuous Network
• In the last sub-bullet point, deleted, “SSL”

May 6, 2016

My Oracle Support Security
□ Deleted the eighth bullet
• Edited the second sentence of the new eighth bullet from, "...and treated in a fashion similar to the attachments described previously." to, "...and treated in a fashion similar to SR attachments (as specified below)."
□ Added three new bullet points at the end of this section.

Security of Oracle Technologies Used to Perform Technical Support – Collaboration Tools
• Replaced the first paragraph, “GCS uses two main collaboration tools to review issues reported to Oracle: Oracle Web Conferencing (OWC) for programs and Oracle Shared Shell for hardware. Both tools share the following common features: “, with, “GCS uses three collaboration tools to review issues reported to Oracle: Oracle Beehive Conferencing and Cisco Webex for programs and Oracle Shared Shell and Cisco Webex for hardware. These tools share the following common features:”
□ In the second paragraph deleted, "about OWC and Shared Shell".
□ In the first bullet after the second paragraph, replaced, “OWC”, with, “Beehive and Webex conferencing” and deleted, “one to one” before “web conferences”.
□ In the first sub-bullet, replaced, “OWC”, with, “They are”.
□ Deleted the second sub-bullet
□ In the new second sub-bullet, deleted, “OWC” before, “session” and inserted, “and attach the recording to the SR as an SR attachment.” at the end of the sentence.
□ In the “Shared Shell” bulleted section, the fifth sub-bullet was changed from, “Oracle logs Shared Shell sessions for subsequent diagnostic and resolution purposes. The log files are stored on Oracle systems with restricted access that is provisioned via an approval process. The log files are also stored on the initiator system from which you launched Shared Shell. “, to, “Oracle retains Shared Shell session logs for up to 90 days for debugging, diagnostic and issue resolution purposes. The log files are stored on Oracle systems with restricted access that is provisioned via an approval process. These files are also available to you on the initiator system from which you started a Shared Shell session, but are not available on the system of a participant that you may have invited to a session.”.

Tools Used for Programs & Hardware – Tools for Programs – Oracle Configuration Manager (OCM)
• In the fourth bullet, inserted, “and the files containing the configuration information are then deleted.” at the end of the sentence.
• In the seventh bullet, before, “Austin Data Center”, deleted, “Tier IV”.
• In the eighth bullet, replaced, “their”, with, “your”.

Tools Used for Programs & Hardware – Tools for Programs – Remote Diagnostic Agent (RDA)
• In the second sentence of the second paragraph, after, “Any RDA uploads to Oracle will be...”, inserted “stored in the”. And after “secured”, deleted, “in the dedicated” and deleted, “as specified above” at the end of the sentence.
□ Added a new sub-section for Explorer files at the end of this section.

Tools Used for Programs & Hardware – Tools for Programs – Database Diagnostic Data
□ Deleted the sub-section for Oracle Platinum Services customers
Tools Used for Programs & Hardware – Tools for Hardware – Auto Service Request – for Systems
  - Added the following sentence at the end of this section, "Under Platinum services, auto-generated SRs can be created for certain OEM fault events, further described http://www.oracle.com/us/support/library/platinum-fault-monitoring-1958297.pdf"

Data Management and Protection
  - Deleted the second paragraph of this section.
  - In the last paragraph, after, “GCS”, inserted, “retains your data for the periods specified herein, except as otherwise required by law, and…”.

Data Management and Protection – Data Management
  - In the first paragraph, updated the url for privacy practices to, "https://www.oracle.com/legal/privacy/services-privacy-policy.html, ".
  - In the third paragraph, after, “…collection and use of such data…", deleted, “(including any such consents necessary for Oracle to provide the services)”.  
  - In the fifth paragraph, in the first sentence, replaced, “if you are”, with, “some customers may have executed agreements with Oracle governing Global Customer Support’s handling of the personal data of residents in the European Economic Area (“EEA Personal Data”) as well as protected health information (PHI).” And made the remaining part into the following new sentence, "”). If you would like to submit EEA Personal Data or PHI to Oracle as part of receiving technical support services, then you must:”. 
  - In the first bullet, after, “Execute”, inserted, “either (i) EU Standard Contractual Clauses or data transfer agreement or (ii) a HIPAA”.
  - In the second, third, and fourth bullets, inserted, “EEA Personal Data or” before, “PHI”.
  - In the third bullet, added, “(other than contact information required for Oracle to respond to the SR)” at the end of the bullet. 
  - Deleted the final bullet.

Reporting Breaches
  - Replaced the first paragraph with the following, “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.”
  - Replaced the second paragraph with the following, “Where Oracle Global Information Security determines that customer data has been subject to unauthorized access (including by an Oracle employee) that compromises the confidentiality, integrity or availability of the customer data, Oracle promptly reports such unauthorized access to the customer, unless otherwise required by law.”
  - Deleted the third paragraph.

Media Returns
  - In the second paragraph, in the second sentence, deleted, “As an additional security precaution,…”; inserted, “both” after, “designed to meet”; and inserted, “and National Institute of Standards and Technology NISTSP800-88” after, “U.S. Department of Defense Sanitizing Standard 5220.22-M”.
  - In the second paragraph, in the fourth sentence, added, “be” before, ‘either”; replaced, “manufacturer” with “Original Equipment Manufacturer (OEM)”; and inserted, “, degauss and rendered inert, and subsequently”, after, “logged via serial number”.

Oracle Enterprise Tape Analysis and Data Recovery Security Practices
  - In the second bullet, deleted, “required” before “information” and inserted, “required to start the data recovery process” after “information”.


December 22, 2015

Data Management and Protection

- The end of the last sentence of the Audit subsection was changed from “under the terms of the Agreement” to “under the terms of your agreement with Oracle”

October 21, 2015

Data Management and Protection

- At the end of this section added a new subsection called “Audit”

June 12, 2015

Data Management and Protection

- At the end of the Data Management subsection, added new paragraph specific to the United States Health Insurance Portability and Accountability Act (HIPAA)

October 10, 2014

Web-Based Customer Support Sites

- Added a new ninth bullet beginning with “During you interaction with My Oracle Support….”

April 7, 2014

- Document format updated

April 2, 2013

Security of Technologies Used to Perform Technical Support

- Under the first bullet of the last paragraph of the “Database Diagnostic Data” section, “Services” was replaced with “Support” so that it correctly reflects “Oracle Advanced Support Gateway”

- In the last paragraph of the “Auto Service Request – for Systems” section, (i) added “and Oracle Business Critical Services for Systems customers” after “For Oracle Platinum Services customers” and (ii) replaced “Platinum Services” with “Advanced Support Gateway Services” after “as further described in the”

Advanced Support Gateway Services

- The section has been renamed from “Platinum Services” to “Advanced Support Gateway Services”

- In the first paragraph of this section, the following changes were made: (i) in the first sentence, added “all services delivered using the Advanced Support Gateway, including” after “and tools designed specifically for” and added “and Business Critical Service for Systems” after “Platinum Services” and (ii) added a new third sentence – “Information about Business Critical Service for Systems is available at http://www.oracle.com/us/corporate/contracts/bus-critical-service-for-systems-1927926.pdf”

- Under the “Oracle Advanced Support Platform” section, the following changes were made:
  - In the first paragraph, the following changes were made: (i) in the first sentence, “Certified Platinum Configuration” was replaced with “configurations serviced through the gateway” after
“service request status for you” and (ii) in the second sentence, “Certified Platinum” was removed and “serviced through the gateway” was added at the end
  o In the third sentence of the third bullet, “Platinum Services Patch” was removed and replaced with “Oracle services coordinator”

• Under the “Oracle Analyst Access and Logging” section, the following change was made to the beginning of the first sentence: “For all Advanced Support Gateway Services” replaces “Under Oracle Platinum Services”

December 5, 2012

Security of Technologies Used to Perform Technical Support
  • In the last paragraph of “Tools for Hardware”, “Advanced Customer” has been removed after “Oracle” so that is now reads “Oracle Gateway”

Platinum Services
  • The subsection formerly called “Oracle Advanced Customer Gateway” has been changed to “Oracle Gateway”. The definition of gateway has been modified to align with changes made in the Oracle Platinum Services Policies.

September 21, 2012

Overview
  □ In the first sentence of the first paragraph, added URLs for the Oracle Software Technical Support Policies and Oracle Hardware and Systems Support Policies
  • Deleted the last sentence of the first paragraph which read – “For a fuller discussion of Oracle GCS data management practices and how to control data that may be collected by Oracle’s technical support tools, see the “Data Management” section below.”

Information Security Program
  • In the second paragraph, replaced “Global Information Technology organization” with “IT and Support organizations”

Web-Based Customer Support Sites
  o In the first paragraph, the following changes were made: (i) in the first sentence, deleted “customers”, (ii) in the second sentence, added “including the My Oracle Support Mobile site” and (iii) in the third sentence, added the URL for the Oracle technical support policies
  □ In the My Oracle Support Security section, the following changes were made:
    o In the third through fifth bullets, added “Customer” before “User Administrator”
    o In the second sentence of the sixth bullet, deleted “Secure File Transfer Protocol (sftp) and/or” after “secured using” and before “Hypertext Transfer Protocol”
    o In the second sentence of the seventh bullet, replaced “A” with “The”
    o In the eighth bullet, the following changes were made:
      ▪ In the first sentence, (i) deleted ”is open and for up to 7 days after SR closure”, added ”may be” after “they”, added “as needed to address” after “retained” and added “and any associated bugs” after “SR”
      ▪ Added a new second sentence that begins – “SR attachments are deleted 7 days…..”
    o In the ninth bullet, (i) deleted “who have the SR CSI in their profile can view your SRs via My Oracle Support” and (ii) and added the following – “…that have been approved by the Customer
User Administrator to add a given CSI to their profile may view SRs associated with that CSI in My Oracle Support.”

Security of Technologies Used to Perform Technical Support

- In the first sentence of the first paragraph, replaced “program” with “software”
- Under “Collaboration Tools,” removed “are as follows” at the end of the sentence that now reads “Additional details about OWC and Shared Shell:”
- Under “Tools Used for Programs & Hardware”, the following changes were made to the first two paragraphs directly under the heading:
  - In the first sentence, deleted “customers”
  - Under the first bullet, (i) removed “do not” from the first sentence and replaced with “not designed to” and (ii) added a new second sentence – “The tools specifically target system telemetry data (e.g., hardware and software components, versions, patched applied)”
  - In the second paragraph, the following changes were made: (i) in the first sentence, replaced “current” with “primary” and “program” with “software”, and (ii) in the second sentence, replaced “other” with “support” and added “and more detailed information concerning the metrics collected by each of the tools described below are available on My Oracle Support.”
- Under “Oracle Configuration Manager (OCM)” in the “Tools for Programs” subsection, the following changes were made:
  - In the first paragraph, the following changes were made: (i) in the first sentence, replaced “downloadable” with “available”, added “My Oracle Support” and “collect and analyze” so that the first sentence reads – “Oracle Configuration Manager (OCM), available from My Oracle Support, is used to collect and analyze your environment configuration information.” and (ii) in the second sentence, “through acceptance of the OCM license agreement” was deleted
  - In the first bullet the following changes were made: (i) at the end of the second sentence “after you install OCM” was deleted and (ii) in the last sentence “because” was replaced with “as”
  - In the eighth bullet, “Customers” was replaced with “You”
  - A new ninth bullet was added – “For Platinum Services, OCM is installed on the Oracle Advanced Support Gateway (“gateway”) described below. Communication is routed over the encrypted VPN established from the gateway to Oracle.”
  - In the last paragraph of this section, “My Oracle Support” was added to the end of the sentence.
- Under “Remote Diagnostic Agent (RDA)” in the “Tools for Programs” subsection, “My Oracle Support” was added to the end of the first sentence of the second paragraph
- Under “Database Diagnostic Data” in the “Tools for Programs” subsection, “secured pipeline” was deleted from the end of the second sentence in the bullet
- In the “Tools for Programs” subsection, a new section was added to the end that starts – “ForOracle Platinum Services customers, Oracle will….”
- Under “Tools for Hardware”, the following changes were made:
  - Under “Auto Service Request – for Systems”, the following was added to the end of this section – “For Oracle Platinum Services customers, ASR is installed by Oracle on the Oracle Advanced Customer Gateway (“gateway”), as further described in the Platinum Services section below. ASR alerts are written back to Oracle via the gateway connection.
  - Under “Auto Service Request – for Storage (Service Delivery Platform)”, the last bullet was removed – “Additional details can be found in the SDP Security White Paper, which is available upon request.”

Platinum Services

- New section added

Data Management and Protection

- In the second paragraph, (i) added a new second sentence which begins – “My Oracle Support SR attachments are transferred…..” and (ii) moved the sentence – “GCS adheres to corporate security policies for secure disposal of your data and media.” to a new third paragraph

Oracle Enterprise Tape Analysis and Data Recovery Security Practices
New section added

Oracle Corporate Security Practices
- A new subsection called “Access Rights” was added under “Personnel”

January 10, 2011

Overview
- In the first paragraph:
  - Added “program and hardware”

Information Security Program
- In the third paragraph:
  - Added “also” after GCS in the first sentence
  - Deleted the last sentence

Web-Based Customer Support Sites
- In the first paragraph, added “program and hardware” in the first and third sentences
- In the “My Oracle Support Security” section:
  - Added “and hardware” in the first sentence
  - Added the following to the end of the third bullet – “you are responsible for provisioning and de-provisioning your users on a timely basis

Security of Technologies Used to Perform Technical Support
- In the first paragraph added “both for Oracle program and hardware support”
- Added new section called “Collaboration Tools”
- Removed “Oracle Web Conferencing” paragraph; OWC content is now in the “Collaboration Tools” section
- Added new section called “Tools Used for Programs and Hardware”

Data Management and Protection
- In the second sentence of the fourth paragraph of the Data Management sub-section, “credit” has been replaced with “payment”

Media Returns
- New section added

Network Security
- In the second paragraph, “Virtual Private Network” has been deleted

October 11, 2010

Overview
- Modified the first paragraph of this section.

Information Security Program
- New section added.

Data Management and Protection ~ Data Management
- Added new paragraph to end of this section regarding sensitive data.
December 1, 2009

Overview
- Modified the second paragraph of this section.

Web-Based Customer Support Sites
- Replaced MetaLink with My Oracle Support in this section.

Security of Technologies Used to Perform Technical Support
- Replaced MetaLink with My Oracle Support in this section.

Data Management and Protection ~ Data Management
- Updated link to the privacy policies.

February 6, 2009

This section describes the changes made to the Global Customer Support Security Practices dated December 26, 2008 and reflected in the Global Customer Support Security Practices dated February 6, 2009:

Web-Based Customer Support Sites
- Updated the MetaLink Security section to include GCS repository.

Security of Technologies Used to Perform Technical Support
- Updated the Software Configuration Manager section to reflect new name of Oracle Configuration Manager.
  - Further updates made to this section include: (i) database configuration requirements for OCM, (ii) auto-update for OCM, (iii) network security information for OCM, (iv) use of network Intrusion Detection Systems (nIDS), (v) quarterly vulnerability scans, and (vi) customer deletion of configuration information.
- Remote Diagnostic Agent (RDA) section updated to include GCS repository.
- Database Diagnostic Data section updated to include GCS repository.

December 26, 2008

This section describes the changes made to the Global Customer Support Security Practices dated April 1, 2008 and reflected in the Global Customer Support Security Practices dated December 26, 2008:

Created Global Customer Support Security Practices ~ Statement of Changes

Overview
- Removed reference to “on-site technical support and any premium technical support offerings” and replaced with “Advanced Customer Services” to reflect current naming standards.
- Added subject to change language and link to Global Customer Support Security Practices ~ Statement of Changes.

Web-Based Customer Support Sites
- Removed reference to Customer Connection as support for PeopleSoft and JD Edwards programs has been migrated to OracleMetaLink.
Data Management

- Updated privacy practices URL.