ORACLE

Oracle Global Customer Support Security Practices

Effective Date: October 08, 2024

CONTENTS

OVERVIEW

These Oracle Global Customer Support Security Practices ("Security Practices") supplement the Oracle Corporate Security Practices and identify the additional security practices that Oracle Global Customer Support ("GCS") follows when performing Cloud, software and hardware technical support for Oracle customers ("You" or "Your") under the terms of Your Oracle agreement, Your order for technical support ("order"), and the Oracle Technical Support Policies located at:

https://www.oracle.com/corporate/contracts/support-services/policies.html.

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. All terms and conditions for Advanced Customer Services shall be specified in the order for such services and are outside the scope of this document.

These Security Practices are subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of security specified herein during the period for which fees for technical support have been paid.

Refer to the Statement of Changes (PDF) (http://www.oracle.com/us/support/library/gcs-security-practices-soc-186190.pdf) for Security Practices updates.

SECURITY PRACTICES

Oracle's Corporate Security Practices (https://www.oracle.com/assets/corporate-security-practices-4490843.pdf) 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

GCS is a global operation, with Service Request ("SR") management based on global competencies, and global work assignment, categorization, and processing. SRs are processed by GCS engineers, including Oracle employees and contractors, in support centers around the globe on a follow-the-sun model, based on criticality, time zone, and the nature of the issue raised. 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.

CUSTOMER SUPPORT SITES

Oracle offers a number of customer support web sites (such as My Oracle Support, Cloud My Oracle Support, Oracle Restaurants eStore and Oracle Service Cloud, each site operates in support of different Oracle software, Cloud services, and hardware product lines. Your agreement(s) with Oracle may specify additional or other support mechanisms.

Described below are the security practices applicable to the My Oracle Support site. The current Oracle technical support policies are located at: http://www.oracle.com/us/support/policies/index.html

My Oracle Support

My Oracle Support https://support.oracle.com is Oracle's key web-based service for providing interactions with GCS for Oracle software, and hardware product lines, including SR access, knowledge search/browse, support communities and technical forums.

My Oracle Support currently implements the following security controls:

- My Oracle Support is an Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) extranet website service using Secure Socket Layer (SSL) encryption.
- Your registration on My Oracle Support uses a unique Customer Support Identifier (CSI) linked to Your Support contract(s).
- Each CSI has at least one customer-designated My Oracle Support Customer User Administrator. Your Customer User Administrators are responsible for approving or rejecting requests from customer users for new My Oracle Support accounts and CSI associations to existing My Oracle Support accounts. You are also responsible for provisioning and de-provisioning Your My Oracle Support users on a timely basis in accordance with Your own access policies.
- Your Customer User Administrator can control which privileges Your users may access (they may add or remove them) on My Oracle Support (for example, write access to SRs can be enabled or disabled for a given user).
- During Your interaction with My Oracle Support, You or the GCS engineer working on Your Service Request may request an interactive online chat. If You accept the chat invitation (acceptance is not required nor assumed) or start one, a transcript of Your chat with the GCS engineer will be retained along with any corresponding SR attachments You have submitted to Oracle. The chat transcript is available to the chat participant for viewing at any time while the Service Request is open. GCS engineers may also summarize the chat session with You. If they do, those summaries become part of the SR activity, and You will be able to review them as You would any other part of the SR.
- Technical issues reported to Oracle may be used as a basis for Knowledge Management content, but all references to You or Your Content, as well as customer context, are removed from Knowledge Management articles.
- Only Your authorized users 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.
- My Oracle Support has self-service Guided Resolution tools that do not require You to create an SR. Files You upload for analysis using Guided Resolution tools are deleted 7 days after upload.
- Draft SRs that You may save prior to submission are deleted 30 days after submission or 90 days if not submitted.
- My Oracle Support SR Attachments (documents uploaded as part of the My Oracle Support SR create/update process) are saved into a dedicated GCS repository. Your communications with this repository are secured using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).
- My Oracle Support SR attachments are retained as needed to address the SR, and are deleted 7 days following closure of the SR. However, where a bug has been identified as being a possible underlying cause of the SR, the SR Attachment is linked to the Oracle Development bug database and retained while the bug is open. Where a bug requires a code fix for resolution, the SR Attachment is retained for up to 6 months.
- The GCS repository is deployed in a firewall protected demilitarized zone (DMZ) network. The DMZ is designed to permit Internet access to and from a private network, while still maintaining the security of that network. There is no direct Internet connection to the application server. The My Oracle Support site resolves to an IP address registered to a virtual server TLS 1.2 to encrypt the information and mask the location of the source and destination.
- My Oracle Support SR data and records related to the SR are kept for 10 years from the date that the record was created.

Oracle Restaurants eStore

Oracle Restaurants eStore allows you to begin an interactive chat with our support team.

- Oracle Restaurants eStore is an Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) extranet website service using Secure Socket Layer (SSL) encryption.
- Your initial chat with the support team creates the link in the Oracle Restaurants eStore. For all subsequent visits with the same user, you will see your previous chats.

- Chat conversations not associated to a restaurant account are deleted after 90 days.
- Technical issues reported to Oracle may be used as a basis for Knowledge Management content, but all references to You or Your Content, as well as customer context, are removed from Knowledge Management articles.
- When you delete your Oracle Restaurants eStore restaurant user account, all information attached to your restaurant user account will be deleted.
- Data and records related to the SR are kept for 10 years from the date that the record was created.

ADVANCED SUPPORT GATEWAY SERVICES

In addition to the methods and tools described above under "Security of Technologies Used to Perform Technical Support", GCS also uses methods and tools designed specifically for all services delivered using the Advanced Support Gateway, including Platinum Services and Business Critical Service for Systems. The security infrastructure associated with those methods and tools is described below. Information about Platinum Services is available at http://www.oracle.com/us/support/library/platinum-services-policies- 1652886.pdf.

Oracle Advanced Support Gateway

The gateway is the computing platform, consisting of the Oracle Advanced Support Gateway available on My Oracle Support and a physical or virtual hardware platform, which hosts Oracle's fault monitoring tools (e.g., Auto Service Request, Oracle Configuration Manager and Oracle Enterprise Manager). The gateway collects and forwards fault event telemetry to Oracle and enables remote access to Your environment by Oracle.

- The gateway is installed within Your DMZ or within a trusted network at Your location. You are required to make the applicable changes to Your trusted network and firewall to enable communication to and from the gateway.
- The gateway connects to Oracle using Oracle's secure private and encrypted network connection, Oracle Continuous Connection ("OCCN"), as described below. Every message is signed and encrypted using 2048-bit RSA keys.
- The security guide for the Oracle Advanced Support gateway can be found here:- https://docs.oracle.com/en/engineered-systems/advanced-support-gateway/security/gprow.html#scrolltoc

Oracle Continuous Connection Network

OCCN is a secured private and encrypted Oracle network that is used to facilitate remote access to Your environment.

- OCCN is dedicated private network and separate from the Oracle intranet.
- OCCN connects the GCS workstation to the Oracle Advanced Support Platform, as described below, and the Oracle Advanced Support Platform over the internet with the gateway.
- Access to OCCN is managed through two-factor authentication and is only available to authorized GCS personnel.
- Oracle offers two options for the connection between the Oracle Advanced Support Platform and the gateway. Both use the internet for connection. You may choose either option.
    - Network to Network VPN based on Internet Protocol Security (IPSec) is established between You and Oracle. This connection is secured and encrypted using IPSec security framework. You have the option to terminate the connection either on an Oracle supplied VPN or on Your VPN.
    - Software SSL VPN using AES256-SHA1 encryption algorithm to build and secure the logical tunnel.

Oracle Advanced Support Platform

The Oracle Advanced Support Platform enables You to view near real-time status and availability, as well as service request status for Your configurations serviced through the gateway. GCS uses the Oracle Advanced Support Platform to remotely monitor Your configurations serviced through the gateway.

- The Oracle Advanced Support Platform is hosted in an isolated Oracle network.
- The Oracle Advanced Support Platform is centrally managed and uses a granular authorization scheme which allows access for select GCS personnel only.
- Oracle Advanced Support Platform is integrated in My Oracle Support and employs the security features described above in "Web-Based Customer Support Sites." During the initial setup, Oracle will enable Your account access to the Oracle Advanced Support Platform. An Oracle services coordinator will be designated to manage Your accounts on Your behalf.
- The Oracle Advanced Support Platform controls access to the gateway within Your environment by checking authorization, creating log entries, and storing required passwords.

Oracle Analyst Access and Logging

For all Advanced Support Gateway Services, Oracle remote access to Your system is managed through OCCN and the gateway. Authorized GCS personnel must first access OCCN before they access the gateway. The Enterprise Management agent is installed on the customer host to enable real time monitoring. The agent is installed on a separate user ID and must have privileges to monitor Oracle software and hardware.

Oracle's access to the OCCN gateway and to Your environment is logged with username, timestamp, and host name. The logs are stored in an encrypted database and retained for 1 year.

TECHNOLOGIES USED TO PERFORM TECHNICAL SUPPORT

GCS uses a number of methods and tools as part of SR diagnosis and resolution, both for Oracle software and hardware support. The security infrastructure associated with those methods and tools is described below.

Collaboration Tools

GCS uses two collaboration tools to review issues reported to Oracle: Zoom and Oracle Shared Shell for hardware.

These tools share the following **common features**:

- You control and participate actively in all sessions.
- You control the session, what navigation is undertaken, what data is displayed and what commands are issued.
- You also have the ability to shut down the session at any time for any reason.

Additional details:

- **Zoom** conferencing enables GCS to establish web conferences to actively assist You with SR diagnosis and resolution. Refer to Customers Recording Calls for additional information.
    - Oracle may record the session for subsequent diagnostic and resolution purposes and attach the recording to the SR as an SR attachment. You are free to instruct GCS to stop recording at any time.
    - You may permit Oracle, Zoom Remote Control access for diagnostic and resolution purposes. At any time, You may Stop Remote Control in Zoom.
    - Encryption is provided for data transmitted over the Internet.
    - Zoom conferencing requires a minimum of Transport Layer Security (TLS) protocol 1.2.

- **Shared Shell** enables GCS to remotely view or access terminal/command interfaces on Your supported hardware.
    - You have access control for conference participants. You invite participants to the session and are responsible for approving or denying participants. You may terminate any participant at any time.
    - The default access control for conference participants is "view only", where participants may only view what appears in the terminal/command line window. You may also choose "no-execute" access, where a participant may type a command but only You can execute it, or "full" access, which allows a participant to type and execute commands.

- The Shared Shell initiator system does not require any open inbound ports; all Internet communications are initiated through outbound connections from the initiator system.
- 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.
  Shared Shell enforces Transport Layer Security protocol 1.2 encryption.

Customers Recording Calls

Oracle will manage and host any recordings using Oracle-approved monitoring and recording collaboration tools as set forth in the Technologies Used to Perform Technical Support Collaboration Tools section.

Employees asked to agree to or participate on a customer hosted call recording will decline and indicate such recording is not permitted under Oracle policies. The use of Virtual AI Assistants via applications, plug-ins, add-ons, extensions and similar technologies is **prohibited**.

Tools Used

GCS provides a variety of tools designed to collect data to assist with issue resolution. These tools share the following common features:

- They are not designed to capture, collect, transport, or use any production data from the system or device on which the tools are run. The tools specifically target system telemetry data (e.g., hardware and software components, versions, patches applied).
- When transmitting such system telemetry data directly to Oracle without Your active involvement, transmissions are sent using one of a variety of encryption technologies.

Further details about some of the primary tools GCS uses for software and hardware technical support are described below. Additional information about support tools, and more detailed information concerning the metrics collected by each of the tools described below:

Auto Service Request – for Systems and Storage

Auto Service Request (ASR) for systems helps automate the hardware technical support process by using fault event telemetry to detect faults on Your supported Oracle hardware and forwards the data to Oracle for analysis and service request generation. The ASR information captured from Your system and then transported to and stored within Oracle is limited to product failure information for diagnosis and resolution and to customer information for confirming eligibility to receive technical support. This includes fault event data, registration data, and ASR asset activation data (such as host names and serial numbers and service request data). 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).

- Upon initialization of the ASR Client on Your system, You register the system and perform a private/public encryption key exchange. 2048-bit RSA keys are used for signing all future messages (both request and response) of the specific ASR manager in order to provide authentication of messages with the core ASR infrastructure at Oracle.
- While activating Your ASR hardware assets, the ASR Client discovers any Service Tags running on those assets to retrieve their serial numbers and production information. The ASR Client receives telemetry messages from the ASR assets and performs operations to validate and suppress an alarm if necessary. If the message should be sent to the core ASR infrastructure at Oracle for processing, the message is encoded in an XML data structure and sent via HTTPS (port 443), TLS 1.2 and AES256 symmetric encryption.

- The core ASR infrastructure at Oracle utilizes user account credentials for validation of users and digitally-signed and encrypted traffic for validation of customer systems. All data stored by the ASR system is segregated by organization in a multi-tenancy security model, and this security is enforced through multiple layers of API-based access and authorization controls. There is no direct, outside access to the data stored in the core ASR infrastructure.

For Oracle Platinum Services customers and Oracle Business Critical Service for Systems customers, ASR is installed by Oracle on the Oracle Advanced Support Gateway ("gateway"). ASR alerts are written back to Oracle via the gateway connection.

Under Oracle Platinum services, auto-generated SRs can be created for certain fault events, further described in http://www.oracle.com/us/support/library/platinum-fault-monitoring-1958297.pdf

Database Diagnostic Data

Oracle database (Release 11g or higher) diagnostic incident and package information are auto-generated by the database as the system encounters errors during its operation. Diagnostics data is designed to provide error, trace, configuration, and other information relevant to an issue from across the database. This information can help You identify, diagnose, and resolve Your issues without involvement from GCS.

- Diagnostics data are stored with You; however, You may choose to upload diagnostics data as attachments through the SR logging and update process on My Oracle Support. You may transfer any diagnostics data to Oracle using AHF. Any diagnostics data uploads to Oracle will be secured in the dedicated GCS repository as specified above.
- When AHF is not configured, diagnostic collection is performed using Automatic Diagnostic Repository (ADR). The Automatic Diagnostic Repository (ADR) is a directory structure that is stored outside of the database. It is therefore available for problem diagnosis when the database is down. 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.
- For Platinum Services, upload of diagnostic data using AHF is performed automatically if AHF is installed on Your host and the Oracle Advanced Support Gateway (“gateway”), described below. Communication is routed over the VPN established from the gateway to Oracle.

Oracle Autonomous Health Framework

Oracle Autonomous Health Framework (AHF) 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 to Oracle 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.

Oracle Advanced Support Gateway (OASG) Agent for Platinum services

In the case of Oracle Platinum Services, the OASG agent is also used, along with AHF, for compliance checks (e.g. Exachk, Orachk) and diagnostic collections executed through Oracle approved tools.

The OASG agent is a self-contained, non-intrusive, lightweight artifact, with a small runtime footprint running as a process. The agent is specifically designed to operate in coordination with OASG and exclusively communicates with it. It can be installed on any of Oracle products where Platinum is delivered, and AHF installed, including, but not limited to, Engineered Systems.

The agent does not require a separate Java Development Kit (JDK), and has no runtime process or library dependencies on the underlying system.

The OASG agent is designed to improve the reliability of transmitting diagnostics, health check metrics or configuration required to support your system to Oracle securely.

Oracle will install the OASG agent on your Certified Platinum Configuration during the Platinum implementation process. The OASG agent will be installed using privileged credentials provided by You during install and will be, specifically configured for Platinum. When deployed on Your host, Oracle will then

- Maintain the lifecycle of the agent including security patching and regular software updates.
- Rotate keys used for communication and encryption,
- Support heartbeat monitoring of the agent from the respective OASG

The OASG agent will only be supported on OASGs running OL8 or higher.

You can choose to disable the OASG agent at any time by contacting the Oracle Platinum Support Team; but in doing so; you will limit Oracle's ability to deliver the full Oracle Platinum Services as described here: https://www.oracle.com/us/support/library/platinum-services-policies-1652886.pdf.

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, reactive 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.

Remote Diagnostic Agent (RDA)

Remote Diagnostics Agent (RDA) provides further information that can assist in SR diagnosis and resolution. RDA scripts are provided to You by GCS to retrieve configuration, parameters, and other settings from a system as input to and context for the SR diagnosis and resolution process in GCS.

RDA information is stored with You; however, You may choose to upload RDA information as attachments through the SR logging and update process on My Oracle Support. Any RDA uploads to Oracle will be stored in the secured GCS repository.

RDA information, which includes Explorer files for Hardware and Systems, can be used for proactive technical support services, meaning the files are provided by You outside of the reactive SR diagnosis and resolution process. Proactive use of RDA and Explorer files are used to identify areas of potential risk or to identify Oracle recommended practices which You may wish to adopt. The tools data may be used by Oracle to assist You in managing Your Oracle product portfolio, for license and services compliance and to help Oracle improve upon product and service offerings.

- RDA proactive collections and Explorer files are retained for up to 6 years for recurring failure analysis.
- Oracle provides You secure access to the Proactive Analysis Center via Proactive Hardware Services on My Oracle Support, where You can see Support recommendations based on proactive collections.
- Oracle retains the first and last five Explorer files that are uploaded for proactive support.
  Customer may request to have their proactive files purged by submitting a Service Request to Support via the Contact Us option on My Oracle Support.

DATA MANAGEMENT AND PROTECTION

GCS practices conform to Oracle's Corporate Security Practices referenced above and information protection policies, which classify Your data as among the highest two classes of confidential information at Oracle. These policies also impose restrictions on the storage and distribution of Your data.

Data Management

GCS does not create or update Your data. In the event that You provide Oracle access to Your personal information in connection with the provision of the technical support services, GCS will adhere to the following:

- 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.

You maintain control over and responsibility for Your data, including any personal information, residing in Your computing environments. You are responsible for all aspects of Your collection of Your data, including determining and controlling the scope and purpose of collection. Oracle does not and will not collect data from Your data subjects or communicate with data subjects about their data.

Please note that GCS services and systems are not designed to accommodate special security controls that may be required to store or process certain types of sensitive data. Please ensure that You do not submit any health, payment card or other sensitive data that requires protections greater than those specified in these Security Practices. Information on how to remove sensitive data from Your submission is available in My Oracle Support at https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1227943.1.

Notwithstanding the restriction above, 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 protected health information (PHI) subject to the United States Health Insurance Portability and Accountability Act (HIPAA) to Oracle as part of receiving technical support services, then You must:

- For PHI, execute a HIPAA business associate agreement with Oracle that specifically references and covers Your technical support services;
- Submit personal information subject to Applicable European Data Protection Law or PHI only in service request attachments on the My Oracle Support customer portal;
- Not include personal information subject to Applicable European Data Protection Law or PHI in the body of service requests (other than contact information required for Oracle to respond to the service request); and
- When prompted in My Oracle Support, indicate that the service request attachment may contain personal information subject to Applicable European Data Protection Law (also which may be designated as EEA Personal Data in My Oracle Support) or PHI.

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.

MEDIA RETURNS

You are responsible for removing all information and data that You have stored on hard disk drives and solid state drives ("drives") before You return the drives for repair/replacement.

All returned drives are processed through an Oracle logistics repair vendor located in Your region. The vendor is required to run a software-enabled data erasure process that is designed to meet National Institute of Standards and Technology NIST SP800-88 on all drives that are operational. This erasure takes place before Oracle proceeds

with any additional processing or handling of the device. In the event that a returned drive is non-operable, it will be either be returned to the Original Equipment Manufacturer (OEM) for erasure and processing or will be batch logged via serial number, degaussed, and rendered inert, and subsequently shipped to an electronic disposal vendor that destroys the drive.

In no event may You leave a tape in a tape drive that is being returned. If a tape is stuck inside a drive that You are unable to remove, consult Your global field representative to assist with its removal.

ORACLE ENTERPRISE TAPE ANALYSIS AND DATA RECOVERY

Oracle Enterprise Tape Analysis and Data Recovery is available to customers with an active support contract for Oracle Premier Support for Systems. When You have an enterprise tape experiencing issues that require data recovery or analysis, Oracle's tape data recovery lab implements the following security measures:

- You are responsible for sending the tape to the Oracle data recovery lab in a safe and secure manner that does not jeopardize the confidentiality of the data or the integrity of the data on the tape itself. If a tape is stuck inside a drive that You are unable to remove, consult Your global field representative to assist with its removal. Once removed, You may send the tape to Oracle.
- When Oracle receives the tape, it is placed in a locked "In Process" cabinet until it is ready for processing. Upon confirmation that You have provided the information required to start the data recovery process, a data recovery engineer write-protects the tape, creates, and applies a label identifying customer name, VOLSER (Barcoded tape ID) and case number, and inputs the information into the tape log-in system, which is a custom designed RFID tape locker system controlled by software. 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.
- Access to the lab is limited to a limited number of Oracle employees in the Oracle Tape Technology Service Center and Tape Product Sustaining Engineering organizations. The badges of such employees are individually provisioned for access, access is logged, and access privileges are reviewed regularly. All data recovery lab tools and firmware are processed within the data recovery lab itself. If it is necessary for Tape Product Engineering to perform additional analysis, the tape product engineer will perform the work in the data recovery lab.
- Upon completion of the analysis/recovery, Oracle will encrypt the data using Oracle Key Manager Appliance. The original tape and recovery tape are shipped by standard overnight courier, and in the case of international shipments, must follow the standard Oracle US export compliance procedures before leaving Oracle. Once the package is shipped, the tracking number as well as any other pertinent tracking information is placed into the SR notes. You may also arrange to pick up the tape directly from the lab; You are solely responsible for the confidentiality and integrity of the data upon taking possession.