Oracle Global Customer Support Security Practices

Effective Date: 23-August-2016

Table of Contents

1. Overview

Oracle Global Customer Support ("GCS") follows the security practices identified in this document when performing standard program and hardware technical support for Oracle customers ("you" or "your") under the terms of your license agreement, your order of technical support ("order"), and the Oracle Software Technical Support Policies located at: http://www.oracle.com/us/support/library/057419.pdf and/or Oracle Hardware and Systems Support Policies located at http://www.oracle.com/us/support/library/hardware-systems-support-policies-069182.pdf. 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. 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.

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. To view changes that have been made, please refer to the attached Statement of Changes (PDF).

2. 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.

3. 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 in support centers around the globe on a follow-the-sun model, based on criticality, time zone, and the nature of the issue raised.

4. Web-Based Customer Support Sites

Oracle offers a number of customer support web sites; each site operates in support of different Oracle programs and hardware lines. Described below are the security practices applicable to the My Oracle Support site, including the My Oracle Support Mobile site. Please see the current Oracle technical support policies located at: http://www.oracle.com/us/support/policies/index.html for more complete information about which Oracle programs and hardware are supported by each support web site.

My Oracle Support Security

My Oracle Support is the key website service for providing interactions with GCS for Oracle programs and hardware, including SR access, knowledge search / browse, support communities and technical forums.

My Oracle Support employs the following security controls:

- My Oracle Support is an HTTPS extranet website service using Transport Layer Security (TLS) 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 approve / reject requests from users for new accounts and CSI associations to existing accounts; you are responsible for provisioning and de-provisioning your users on a timely basis.
- Your Customer User Administrator can control which features your users may access on My Oracle Support (e.g., write access to SRs can be enabled or disabled for a given user).
- Your Customer User Administrator can view users associated with its CSIs, and has the ability to remove access privileges for users.
- 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).
- 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 on an Accelerator/Reverse Proxy to encrypt the information and mask the location of the source and destination. At the termination point of the TLS encryption, reverse proxy forwards traffic to the application server.
- During your interaction with My Oracle Support, you or the 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 engineer will be preserved and treated in a fashion similar to SR attachments (as specified below). The chat transcript is available to the chat participant for viewing at any time while the Service Request is open. Engineers may also summarize the chat session with you. If they do, those summaries become part of the Service Request activity, and you will be able to review them as you would any other part of the Service Request.
- 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.
- Technical issues reported to Oracle may be used as a basis for Knowledge Management content, but all references to customers and customer data, as well as customer context, are removed from Knowledge Management articles.
- My Oracle Support has self-service Guided Resolution tools that do not require the creation of an SR. Files you upload for analysis using these 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 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 saved into the Oracle Development bug database and retained while the bug is open. The SR Attachment is deleted from the bug database 7 days after the bug is closed if it is a duplicate bug, does not require a code fix or is unable to be resolved by a code fix. Where a bug requires a code fix for resolution, the SR Attachment is retained for 6 months after the bug is closed in order to assist with the diagnosis or confirm a match with issues identified in other related code, and is then deleted. However, if some or all of the data contained in the SR Attachment is used as a test case for confirming the code fix, that data may be stored in an Oracle source code repository for regressing testing for the life of the Oracle product to ensure that the bug is not reintroduced into subsequent versions.

5. Security of 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: Oracle Shared Shell and Cisco Webex. 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:

- **Cisco Webex conferencing** enables GCS to establish web conferences to actively assist you with SR diagnosis and resolution.
    - 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.
    - Secure Socket Layer (SSL) encryption is provided for data transmitted over the Internet
    - Cisco Webex conferencing supports up to Transport Layer Security (TLS) protocol 1.0

- **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.
    - 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.
    - 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.

Tools Used for Programs & Hardware

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 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, are available on My Oracle Support.

Tools for Programs

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 Transport Layer Security (TLS) and industry standard protocol (HTTPS) as well as 128bit 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 an Accelerator/Reverse Proxy to encrypt the information and mask the location of the source and destination. At the termination point of the TLS 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 teams.
- You may request deletion of your configuration information by logging a Service Request indicating the specific configuration information and scope of the deletion request.

- 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.

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.

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 this 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 Explorer file uploaded and the 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.

.

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 OCM. Any diagnostics data uploads to Oracle will be secured in the dedicated GCS repository as specified above.

Tools for Hardware

Auto Service Request – for Systems
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).

- Upon initialization of the ASR manager on your system, you register the system and perform a private/public encryption key exchange. 1024-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 manager discovers any Service Tags running on those assets to retrieve their serial numbers and production information. The ASR manager receives

telemetry messages from the ASR assets, and 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), using RSA with RC4 (256 bit) TLS 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"), as further described in the Advanced Support Gateway Services section below. ASR alerts are written back to Oracle via the gateway connection. 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

Auto Service Request – for Storage (Service Delivery Platform)
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.

6. 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. Information about Business Critical Service for Systems is available at http://www.oracle.com/us/corporate/contracts/bus-critical-service-for-systems-1927926.pdf.

Oracle 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 1024-bit RSA keys.

Oracle Continuous Connection Network

OCCN is a secure private and encrypted Oracle network that is used to transport fault event telemetry from the gateway to Oracle and facilitates 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 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 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 and only accessible by authorized GCS personnel.
- 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 programs.

Oracle’s access to the OCCN gateway and to your environment is logged with user name, timestamp and host name. The logs are stored in an encrypted database.

7. Data Management and Protection

GCS practices conform to Oracle’s 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.

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

GCS does not create or update your data. In the event that Oracle accesses your data in connection with the provision of technical support, GCS will adhere to the privacy practices described at https://www.oracle.com/legal/privacy/services-privacy-policy.html.

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.

You maintain control over and responsibility for your data 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. 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. 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, 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) subject to the United States Health Insurance Portability and Accountability Act (HIPAA). If you would like to submit EEA Personal Data or PHI to Oracle as part of receiving technical support services, then you must:

- Execute either (i) EU Standard Contractual Clauses or data transfer agreement or (ii) a HIPAA business associate agreement with Oracle that specifically references and covers your technical support services.
- Submit EEA Personal Data or PHI only in service request attachments on the My Oracle Support customer portal.
- Not include EEA Personal Data or PHI in the body of service requests (other than contact information required for Oracle to respond to the SR).
- When prompted in My Oracle Support, indicate that the service request attachment may contain EEA Personal Data or PHI.

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.

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.

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.

8. 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 both the U.S. Department of Defense Sanitizing Standard 5220.22-M and National Institute of Standards and Technology NISTSP800-88 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 pulverizes 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.

9. 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.

10. Physical Security

Oracle maintains the following physical security standards for the Oracle facilities from which environments may be accessed ("service location(s)"):

- Physical access to service locations is limited to Oracle employees, subcontractors and authorized visitors.
- Oracle employees, subcontractors and authorized visitors are issued identification cards that must be worn while on the premises.
- Visitors 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.
- 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.
- After-hours access to service locations is monitored and controlled by Oracle Corporate Security.
- Oracle Corporate Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.

11. Oracle Enterprise Tape Analysis and Data Recovery Security Practices

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 engineer then places the tape in an RFID locker system until the analysis/data recovery process can begin.
- Access to the lab is limited to a small 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.

12. 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.