

Global Customer Support Security Practices

Effective Date: 10-January-2011

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](#) and/or [Oracle Hardware and Systems Support Policies](#). 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. 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.

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](#) (P D F) .

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 Global Information Technology organization.

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.

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.

WEB-BASED CUSTOMER SUPPORT SITES

Oracle offers customers 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. Please see the current Oracle Technical Support Policies 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 a 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 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 User Administrator can control which features your users may access on My Oracle Support (for example, write access to SRs can be enabled or disabled for a given user).
- Your 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 Secure File Transfer Protocol (sftp) and/or Hypertext Transfer Protocol over Secure Socket Layer (https).
- The GCS repository is deployed in a firewall protected demilitarized zone (DMZ) network. A 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 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.
- My Oracle Support SR attachments are transferred to the dedicated GCS repository where they are retained while the SR is open and for up to 7 days after SR closure.
- Only your authorized users who have the SR CSI in their profile can view your SRs via My Oracle Support.
- Technical issues reported to Oracle may be used as a basis for Knowledge Management content, but references to customers and customer data, as well as customer context, are removed from Knowledge Management articles.

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 program and hardware support. The security infrastructure associated with those methods and tools is described below.

Collaboration Tools

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:

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.

- Secure Socket Layer (SSL) encryption is provided for data transmitted over the Internet.

Additional details about OWC and Shared Shell are as follows:

- **OWC** enables GCS to establish one-to-one web conferences to actively assist you with SR diagnosis and resolution.
 - OWC is designed to work with any Internet proxy and firewall without the need to open any additional ports.
 - You may request that the GCS engineer set a password for individual OWC sessions for SRs.
 - Oracle may record the OWC session for subsequent diagnostic and resolution purposes. You are free to instruct GCS to stop recording at any time.
- **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 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.

Tools Used for Programs & Hardware

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

- They do not capture, collect, transport, or use any production data from the system or device on which the tools are run,
- 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 current tools GCS uses for program and hardware technical support are described below. Additional information about other tools may be available on My Oracle Support.

Tools for Programs

Oracle Configuration Manager (OCM)

Oracle Configuration Manager (OCM), downloadable from My Oracle Support, is used to upload 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 through acceptance of the OCM license agreement.

- 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 after you install OCM. 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 because 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 Secure Socket Layer (SSL) 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 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.
- 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 Tier IV Austin Data Center and protected by Oracle network security infrastructure and security teams.
- Customers may request deletion of their configuration information by logging a Service Request indicating the specific configuration information and scope of the deletion request.

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 secured in the dedicated GCS repository as specified above.

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 the OCM secured pipeline. 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 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), using RSA with RC4 (128 bit) SSL 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.

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.
- Additional details can be found in the SDP Security White Paper, which is available upon request.

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 SR data in accordance with specific retention schedules for technical support related information. GCS 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: <http://www.oracle.com/html/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 (including any such consents necessary for Oracle to provide the services). 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>.

Reporting Breaches

- GCS will promptly evaluate and respond to incidents that create suspicions of unauthorized misappropriation of any of your data. Oracle Global Information Security (GIS) will be informed of such incidents and, depending upon the nature of the activity, will define escalation paths and response teams to address the incidents.
- If Oracle determines that your data has been misappropriated (including by an Oracle employee), Oracle will promptly report such misappropriation to you in writing.
- Oracle personnel are instructed in addressing incidents where your data has been misappropriated, including prompt reporting and escalation procedures.

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.

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. As an additional security precaution, the vendor is required to run a software-enabled data erasure process that is designed to meet the U.S. Department of Defense Sanitizing Standard 5220.22-M 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 either be returned to the manufacturer for erasure and processing or will be batch logged via serial number and 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.

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

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.

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.

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.