

Global Customer Support Security Practices

Effective Date: 6-February-2009

OVERVIEW

Oracle Global Customer Support (“GCS”) follows the security practices identified in this document when performing standard technical support for Oracle customers (“you” or “your”) under the terms of your license agreement, your order of technical support (“order”), and the [Oracle Technical Support Policies](#). 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. 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 will not materially reduce 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) .

Oracle’s information security management system 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 provides new hire training courses, custom training for specific workflows and business cases, and regular ‘hot topics’ training and communications for GCS staff. These efforts work in conjunction with corporate level training and promotion of security policies and practices.

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 product lines. Described below are the security practices applicable to the MetaLink site. Please see the current Oracle Technical Support Policies for more complete information about which Oracle products are supported by each Support web site.

Metalink Security

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

MetaLink employs the following security controls:

- MetaLink is a HTTPS extranet website service using Secure Socket Layer (SSL) encryption.
- Your registration on MetaLink uses a unique Customer Support Identifier (CSI) linked to your Support contract.
- Each CSI has at least one customer-designated MetaLink Customer User Administrator. Your User Administrators approve / reject requests from users for new accounts and CSI associations to existing accounts.
- Your User Administrator can control which features your users may access on MetaLink (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.
- MetaLink SR Attachments (documents uploaded as part of the MetaLink 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 MetaLink 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.
- MetaLink 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 MetaLink.
- 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. The security infrastructure associated with those methods and tools is described below.

Oracle Web Conferencing (OWC) may be used to review issues reported to Oracle. OWC is a real-time collaboration tool that enables GCS to establish one-to-one web conferences to actively assist you with SR diagnosis and resolution.

- GCS allows you to control and participate actively in all OWC sessions accessing your system. You control the OWC 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.
- OWC supports access control via the regular and restricted conference types. You may restrict document sharing and control access when establishing the conference.
- OWC provides 128-bit Secure Socket Layer (SSL) encryption for data transmitted over the Internet.
- 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.

Oracle Configuration Manager (OCM), downloadable from MetaLink, 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.
- OCM configuration information is used to assist in the SR diagnosis and resolution process. OCM does not collect production data, business transactions or passwords.
- 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 need to 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 MetaLink.

Remote Diagnostic 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 does not collect any production data from the instance on which RDA is run.
- RDA information is stored with you; however, you may choose to upload this information as attachments through the SR logging and update process on MetaLink. 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 does not include any production data from the database from which it is generated.
- Diagnostics data are stored with you; however, you may choose to upload diagnostics data as attachments through the SR logging and update process on MetaLink. 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.

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.

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.

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 Virtual Private Network (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.