ORACLE CONSULTING &
ADVANCED CUSTOMER SUPPORT
SECURITY PRACTICES

This document identifies the security practices that Oracle organizations performing software or hardware consulting services, and Oracle’s Advanced Customer Support (“ACS”) organization (for purposes of this document all such organizations collectively “Oracle”) follow when performing such consulting or ACS services (“services”) under the terms of the agreement, the ordering document, and the exhibit (collectively the “order”). It also clarifies your security obligations with respect to your environments and the data therein. These practices are subject to change at Oracle’s discretion; however, Oracle will not materially reduce the level of security specified in this document during the performance of services under your order.

I. Definitions

The term “environment(s)” means your technology environments to which Oracle is granted access in order to provide the services under an exhibit. The term “subcontractors” means subcontractors retained by Oracle and its subsidiaries that assist in performing the services.

II. Security Policies

Oracle’s corporate security policies 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 aligned with the ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standards, govern all areas of security applicable to the 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.

Oracle’s corporate security policies are confidential information and are not available for review by customers or third parties. However, brief summaries of certain security policies relevant to the provision of the services are provided below.

Organizational Security

- The Oracle Information Security Policy describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Oracle. This over-arching information security policy also describes governing principles such as 'need to know', least privilege, and segregation of duties. All employees, contractors and temporary employees are subject to Oracle security policies.

Asset Classification and Control

- The Oracle Information Protection Policy provides guidelines for all Oracle personnel regarding information classification schemes and minimum handling requirements associated with those classifications in an effort to ensure proper protection of Oracle and customer information assets.

- The Oracle Desktop and Laptop Security Policy requires the implementation of anti-virus and personal firewall software, and strongly recommends the use of Software Update
Service (SUS) for Windows, and Oracle's desktop asset management software on desktop and laptop computers.

- The Oracle Acceptable Use Policy sets requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resources.

Human Resource Security

- The Oracle Code of Ethics and Business Conduct sets forth Oracle's high standards for ethics and business conduct at every level of the company, and at every location where Oracle does business throughout the world. The standards apply to employees, independent contractors, and temporary employees and cover the areas of legal and regulatory compliance and business conduct and relationships. Compliance-tracked training in ethics and business conduct and sensitive information handling is required once every two years. The policy is available at http://www.oracle.com/us/corporate/investor-relations/cebc-176732.pdf.

Physical and Environmental Security

- The Oracle Logging and Log Analysis Policy states corporate-level mandates for log retention, review, and analysis. Areas covered include minimum log requirements, responsibilities for the configuration and implementation of logging, alert review, problem management, retention, security and protection of logs, as well as compliance review.

- The Oracle Media Sanitization and Disposal Policy establishes guidelines for secure erasure of information, from all types of electronic media, where use for current purposes is no longer needed and a decision has to be made regarding recycling or destruction. The policy is intended to protect Oracle resources and information from security threats associated with the retrieval and recovery of information on electronic media.

Access Control

- The Oracle Logical Access Controls Policy describes logical access control requirements for all Oracle systems, including authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users' with access to Oracle systems which are not Internet facing publicly accessible systems.

- The Oracle Password Policy requires protection of information assets by Oracle employee use of strong password controls where passwords are being used as a method of authentication.

Business Continuity Management

- The Oracle Business Continuity Policy addresses the requirements for the development, maintenance and testing of emergency response, disaster recovery, and business continuity practices to minimize the impact of business disruptive events on Oracle’s internal business operations globally.
Compliance

- The *Oracle Services Privacy Policy* describes Oracle’s treatment of data that resides on Oracle, customer or third-party systems (including personally identifiable information or “PII”) to which Oracle may be provided access in connection with the provision of the services. This policy is available at: [http://www.oracle.com/html/services-privacy-policy.html](http://www.oracle.com/html/services-privacy-policy.html) and incorporated herein by reference.

- The *Oracle Information Security Incident Reporting and Response Policy* requires reporting of and response to information security incidents in a timely and efficient manner. Oracle also maintains a detailed Incident Response Plan to provide specific guidance for personnel involved in or supporting incident response.

III. Physical Security

**Physical Security Safeguards**: Oracle maintains the following physical security standards, which are designed to prohibit unauthorized physical access at the Oracle offices from which the 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.
- 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 Security.
- Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.

IV. Network Security

Oracle takes the following steps to secure access to the environments:

- Oracle employs intrusion detection systems within the Oracle network to provide continuous surveillance for intercepting and responding to security events as they are identified. Oracle utilizes a network-based monitoring approach to detect attacks on open firewalls ports within Oracle’s network. Events are analyzed using signature detection, which is a pattern matching of environment settings and user activities against a database of known attacks. Oracle updates the signature database as new releases become available for commercial distribution. Alerts are forwarded to Oracle’s IT department for review and response to potential threats.
• Oracle uses router rules, access control lists and segmentation on the Oracle network.

• Oracle’s IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication; usage is audited.

• When Oracle accesses the environments residing on your system over the Internet, it uses only (a) encrypted network traffic via industry standard Virtual Private Network (VPN) or equivalent technology, or (b) technology permitted by your network administrator (e.g., direct dial-up or DSL if permitted on your network). Unless otherwise specified in the order, in (a) above, Oracle uses Oracle Continuous Connection Network (OCCN), which utilizes a persistent VPN tunnel and Cisco Software VPN Combination, for internet-based connections to the environments.

• To the extent specified in your order, Oracle may also use a desktop/laptop client based product when it accesses the environments residing on your system over the Internet. Examples include: Cisco Software VPN, Nortel Software VPN, Checkpoint Software VPN, Netscreen Software VPN, Point-To-Point Tunneling Protocol (PPTP), Neoteris Secure Sockets Layer (SSL) VPN, Aventail SSL VPN.

V. Data Management/Protection

Oracle generally does not require or request access to production data in order to provide services. You are responsible for providing Oracle access to production data in a development or test environment and/or to a production computing environment only to the extent necessary to perform the services.

Data Management: During the performance of the services, you maintain control over and responsibility for any data residing in the environments. Oracle does not and will not:

• Change any data, other than as required for the performance of the services.
• Have any role in determining or maintaining the accuracy of any data.
• Control how data is hosted, processed, stored or destroyed by you.
• Control your access to data, other than restricting access to data through applying physical and logical access controls, as applicable, as part of the services.
• Monitor your use of or access to data, except as necessary to provide the services.

Deletion of Environments: Upon termination of services or at your request, Oracle will delete the environments located on Oracle computers in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the environments. Unless otherwise specified in writing, Oracle will archive environments on tape for six months following termination of the services.

Reporting Breaches: If the order specifies that Oracle is required to access a production environment to perform the services and/or to receive production data into a development or test environment to perform the services, Oracle will take the following additional measures:

• Oracle will promptly evaluate and respond to incidents that create suspicions of unauthorized misappropriation of your data. Oracle Global Information Security 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 data in your environments has been misappropriated (including by an Oracle employee), Oracle will promptly report such misappropriation to you in writing.

• Oracle infrastructure staff and Oracle Global Information Technology (GIT) personnel are instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures.

Disclosure of Data: Oracle will not disclose data located on Oracle systems, 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 such 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 the Agreement.

VI. Access Control

Account Provisioning and Passwords: Oracle maintains the following standards for provisioning access to and creating passwords for the environments that are in the control of Oracle:

• Access is provisioned on a need to know basis.

• Passwords conform to the strong password guidelines that include complexity, expiration, duplicity and length. Passwords will not be written down or stored on-line unencrypted.

• Passwords are treated as Oracle confidential information.

• At your request, Oracle will agree with you on a schedule for periodic password changes.

• User IDs and passwords to your systems are not communicated to any other person without your prior authorization.

General Access: In the event of employee terminations, deaths or resignations, Oracle will take actions to terminate network, telephony and physical access for such former employees. Oracle Corporate Security will periodically review accounts of terminated employees to verify that access has been terminated and that stale accounts are removed from the Oracle network.
VII. Additional Oracle Practices

Computer Virus Controls: Oracle maintains the following computer virus controls for 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 laptops to be loaded with virus protection software. Oracle 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 employees have the virus software installed and up to date virus definitions on all desktops and laptops.

Information Security Managers: Oracle Consulting & ACS have appointed an Information Security Managers (ISM) to coordinate with Oracle Global Information Security (GIS) by serving as a resource to help identify strategic and practical security issues within the organization. The ISM serves as an advocate within Oracle Consulting & ACS to communicate information security awareness to Oracle Consulting & ACS employees and management and work collectively with that group to help implement and comply with Oracle’s corporate security practices, policies and initiatives.

VIII. Human Resources Security

Personnel: All Oracle employees, independent contractors, and temporary employees are required to abide by the Oracle Code of Ethics and Business Conduct, which is available at http://www.oracle.com/us/corporate/investor-relations/cebc-176732.pdf.

Oracle places strong emphasis on reducing risks of human error, theft, fraud, and misuse of facilities. 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 and policies concerning the handling of confidential documentation.

Employee Security Requirements

- Oracle employees are required to take various measures to protect the security of the environments. Employee obligations include written confidentiality agreements and compliance with company policies concerning protection of confidential information (e.g., Oracle code of conduct, acceptable use and information protection policies). Employees also are required to take the following measures to protect your data:

  - Store materials containing data securely and share those materials internally only for the purposes of providing the services.
• Dispose of paper copies of confidential materials and materials containing data in shredding bins designated for confidential information, and not in non-secure recycling bins or trashcans (if shredders are available at client site).

**Subcontractors**

• Oracle will obtain a written confidentiality agreement from each subcontractor before the subcontractor provides services. In addition, subcontractors that require access to your environments are required to sign a services provider agreement and a network access agreement. Included in the services provider agreement are the Oracle Supplier Information and Physical Security standards, which require the subcontractor to implement physical, technical and administrative safeguards consistent with Oracle’s obligations under the order and these practices.

• Oracle is responsible for assuring that its subcontractors access, use, and protect the security of the environments in a manner consistent with the terms of the order and this document.

**Employee Training**

• All Oracle employees are required to complete an information protection awareness course upon hiring and every two years thereafter. The course instructs employees on their obligations under the various central Oracle privacy and security policies (such as the Information Protection Policy, Acceptable Use Policy, Security Breach Disclosure Policy and the Services Privacy Policy). The course also trains employees on data privacy principles as well as data handling practices that may apply to their jobs at Oracle and are required by company policy, including those related to notice, consent, use, access, integrity, sharing, retention, security and disposal of data.

• 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.
IX. Your Obligations

- You are responsible for all aspects of the collection of 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 sending any required notices and/or obtaining any required consents necessary for Oracle to perform the services. Oracle does not and will not collect data from data subjects or communicate with data subjects about their data.

- You will limit Oracle’s access to your data to the extent necessary for Oracle to perform the services. You will prevent Oracle from accessing any health, payment card or other sensitive data that requires protections greater than those identified herein unless the parties specify the security measures applicable to Oracle’s treatment of such data in the applicable order for services.

- You are responsible for managing Oracle’s access to your systems, including providing unique accounts and user IDs where necessary.