

ORACLE SUPPLIER/CONTRACTOR SECURITY STANDARDS

These Oracle Supplier/Contractor Security Standards identify the security standards and procedures that must be followed when accessing Oracle confidential information or Oracle's or an Oracle customer's networks. Contractor (as defined below) is responsible for compliance with the terms of these Standards by its employees and agents.

Terms not defined herein have the meaning in contractor's agreement with Oracle. Additional security requirements may be specified in an agreement between Oracle and contractor.

1. Definitions

The following definitions apply to these Standards:

"agreement" means an agreement between Oracle and a contractor under which (i) contractor performs services for Oracle or Oracle's client (e.g., Services Provider Agreement), or (ii) contractor is otherwise provided access to data or other confidential information or to a network or environment (e.g., Network Access Agreement).

"computer" means any desktop or laptop computer, mobile device (e.g., cellular phone, BlackBerry), server and/or storage device that (i) is involved in the performance of the services, (ii) may be used to access a network or environment, or (iii) may access or store data or other confidential information.

"confidential information" means all environments, passwords, personally identifiable information/PII, and data, as well as all other Oracle "Confidential Information" as defined in contractor's agreement with Oracle.

"contractor" means an entity (including its employees and agents) that (i) performs services for Oracle or as a subcontractor to Oracle, or (ii) is granted access to a network or environment.

"data" means any data or other confidential information (including without limitation any PII or other information about Oracle's vendors, suppliers, clients, employees, and partners) that resides on the network, in environments or on computers.

"environment" means any development, test, stage and/or production computing environments to which contractor is provided access under an agreement.

"network" means any computer network to which contractor is provided access in connection with an agreement and/or any of contractor's computer networks used to provide services to Oracle.

"personally identifiable information" or "PII" means any information to which contractor is provided access that could identify an individual, either directly or indirectly, including without limitation the individual's name; address; government identification/national identification number; phone number or e-mail address; passwords; or health, financial or employment information.

2. Physical Security

Contractor is required to maintain the following physical security standards to prohibit unauthorized physical access at its offices from which confidential information, networks or environments may be accessed (“service locations”):

- Access must be limited to contractor employees and authorized visitors.
- Contractor employees and authorized visitors must be issued identification cards that must be worn while on the premises.
- Visitors must be required to sign a visitor’s register and be escorted or observed when on the premises.
- Contractor must monitor and properly manage the possession of keys and access cards and the ability to access the premises.
- When visiting or working at Oracle’s facilities, contractor is required to abide by Oracle’s building security requirements and any direction provided by Oracle’s security staff. Contractor may not photograph or otherwise record Oracle facilities, computers or infrastructure.
- Any 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.

3. Use of Networks, Computers and Environments

Network Protocols

Contractor is required to take the following steps to protect its own network or when accessing an Oracle network or the environments:

- Employ an industry standard Network Intrusion Detection Systems (NIDS) to monitor and proactively block suspicious network traffic from reaching Contractor’s network or any environments.
- Manage and monitor all routers and firewall logs for unauthorized access to contractor’s network.
- Use router rules, access control lists and segmentation on any networks from which the environments or other confidential information are accessed.
- When accessing the environments over the Internet, contractor may use only (i) encrypted network traffic via industry standard Virtual Private Network (VPN) or equivalent technology, or (ii) other technology permitted by Oracle (e.g., direct dial-up or DSL if permitted) and specified in the agreement. Unless otherwise specified in the agreement, when connecting to the Oracle network in (i) above, contractor is required to use the Oracle Continuous Connection Network, which utilizes a Netscreen 5XT

Hardware VPN or a Cisco Software VPN, for internet-based connections to the environments.

- Contractor will use the access management and authentication measures provided by Oracle at all times for any logical connection to Oracle or customer networks. This includes, as applicable and without limitation, log-enabled access via Oracle's Continuous Connection Network, PowerBroker, Oracle Account Provisioning System, firewalls, load balancers, certificate stores, and encryption of network traffic.
- Contractor may not permit wireless access to networks, computers, or environments at any time.
- Contractor may transmit or make available confidential information over the Internet only in an encrypted format (e.g., using https or ftps).

Access to Networks and Environments

Oracle networks and the environments may be accessed only:

- if expressly permitted under contractor's agreement with Oracle;
- by contractor's employees and agents providing services under the agreement; and
- on a least-privilege basis for performance of the services.

Contractor will implement physical, administrative and technical measures that restrict the ability to download, copy and/or export data only to those authorized users who are required to process the data for the performance of the services.

Passwords

Contractor must maintain the following password standards for all computers, networks and environments:

- Passwords must conform to strong password standards that include length, complexity and expiration. Passwords must not be written down or stored on-line unencrypted.
- Passwords may not be shared. Each contractor employee or agent to whom access is granted must be provided a unique identifier and password for the networks and environments.
- Any passwords stored online must be stored using a minimum of 128 bit encryption.
- Contractor will change passwords on a regular basis; use of any one password may not exceed 90 days. No default passwords may be used.
- Contractor will abide by any further requirements for passwords on Oracle or client computers, networks or environments.

Use of Networks and Environments

Contractor may not use or permit use of the environments or networks for any purpose that may (a) menace or harass any person or cause damage or injury to any person or property, (b) involve the publication of any material that is false, defamatory, harassing or obscene, (c) violate privacy rights or promote bigotry, racism, hatred or harm, (d) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters, (e) constitute an infringement of intellectual property or other proprietary rights, or (f) otherwise violate applicable laws or regulations.

Terminating Access

Within 24 hours of termination, death or resignation of any contractor employee or agent, contractor must take appropriate actions to terminate his/her access to computers, networks, and environments, as well as physical access to service locations.

Logging

Contractor will retain security related logs for its computers and networks (including without limitation firewall, NIDS, operating system, VPN, and application logs) for at least 30 days.

4. Computer Protection

Virus Controls

Contractor will employ the following computer virus controls for all computers:

- Scan all e-mail sent both to and from any recipient for malicious code and delete email attachments that are infected with known malicious code prior to delivery.
- Use industry-standard virus protection software. Virus definitions must be updated regularly (in no event to exceed 7 days).
- Use automated virus updates, which may not be disabled.

Patches

Operating system security patches and software security patches must be applied promptly, when issued, on all computers. Computers should be configured to automatically receive operating system security patches and software security patches when issued.

5. Storage, Return and Deletion of Information

Storage

Contractor may not store PII, data, confidential information or environments on computers unless required for the performance of services under an agreement. Any such information must be deleted from a computer, in a manner that ensures that it cannot be accessed or read, as soon as such storage is no longer required for the performance of services.

Removable Media and Encryption

Contractor may not store PII, passwords, data or confidential information on removable media unless required for the performance of services under an agreement. Any such information on removable media must be stored using a minimum of 128-bit encryption. Any such information must be deleted from removable media, in a manner that ensures that it cannot be accessed or read, as soon as such storage is no longer required for performance of services.

Return and Deletion

Upon termination of services or upon Oracle's request, contractor must promptly (i) return to Oracle all PII, data and environments, and (ii) delete all PII, passwords, data and environments in Contractor's possession or control (on computer or in whatever other form or media) in a manner that ensures that they cannot be accessed or read. Contractor may retain one copy of the foregoing materials for so long as required by law, provided that any such copy is kept in encrypted format and is not used or accessed for any other purpose.

Contractor will dispose of documents containing PII, passwords, data or other confidential information only in secure shredding bins designated for confidential information, with appropriate processes to assure that documents destroyed in manner that ensures that they cannot be re-created, accessed or read.

6. Business Continuity and Disaster Planning/Response

Contractors that are required to store or process environments or data on their computers in connection with providing services to Oracle will maintain a comprehensive business continuity program for all facilities, networks and computers from which environments or data may be accessed. The program will be designed to ensure that computers and facilities can continue to function through an operational interruption and that Contractor can continue to provide services as specified in its agreement with Oracle. At a minimum, the program will include the following elements:

Backup Power Supply

Contractor will maintain an appropriate backup power supply system to guard against electrical outages. The solution will allow for controlled shutdown of systems used to process or store data, as well as ongoing power support for recovery and back-up systems.

Fire Detection and Suppression System

Contractor will implement appropriate fire detection and suppression systems.

Back-up and Retention of Data

Contractor agrees to complete back-up and retention of all data and environments as required for performance of the services. Rules for frequency of back-ups and retention cycles shall be made available to Oracle upon request. All back-ups must be stored securely.

Incident Notification and Support

Contractor shall notify Oracle promptly of any incident that requires execution of the business continuity program and affects the function of computers and/or the availability or integrity of data. Contractor will resume operations promptly after such an incident.

7. Confidentiality

The passwords for the networks and environments, and all PII and other data are Oracle confidential information. Contractor will provide its employees and agents access to the networks, environments and any confidential information only on a need to know basis, and may not disclose any confidential information to any third party without Oracle's prior written consent.

8. Privacy and Data Protection

Contractor agrees that it will take the following measures to assure the protection of personally identifiable information and other data:

- Access, use and process PII and other data only on behalf of Oracle and only for the purposes specified in Contractor's agreement with Oracle, in compliance with these Standards and such further instructions as Oracle may provide regarding the processing of such PII and other data.
- Inform Oracle promptly if contractor has reason to believe that legislation applicable to contractor (or changes in legislation applicable to contractor) prevent it from fulfilling the obligations relating to treatment of PII or other data under these Standards and/or contractor's agreement with Oracle.
- To the extent permitted by law, notify Oracle promptly and act only upon Oracle's instruction concerning:
 - any request for disclosure of the PII or other data by a law enforcement or other governmental authority;
 - any request by law enforcement or other governmental authority for information concerning the processing of PII or other data in connection with this Agreement;
 - any request received directly from an individual concerning his/her PII.
- Abide by all data privacy laws and regulations applicable to Contractor's access to PII, including those concerning onward and international transfer, and will act only on Oracle's written instruction concerning any such transfers.
- Execute European Union model contractual clauses or other similar terms as required by local law if necessary for Oracle's compliance with data privacy laws and regulations concerning the transfer of PII to Contractor.

The Oracle entity whose data is accessed pursuant to an agreement may enforce the terms of this Section 8 as required by local law.

9. Reporting and Responding to Security Incidents and Breaches

Contractor must immediately report to Oracle (i) any security or other event that creates reasonable suspicion of unauthorized access to PII, data, confidential information or an environment and/or misappropriation or alteration of any PII, data or confidential information, and (ii) the loss or theft of any computer. Contractor will take appropriate steps to immediately address such incident, and will follow any additional instructions Oracle provides with respect to such incident and/or remediation identified in response to such incident.

10. Personnel

All contractor employees and agents must be required to execute written confidentiality agreements that are consistent with the confidentiality obligations in these Standards and to comply with policies designed to prevent the disclosure of confidential information. Contractor is responsible for assuring that its employees and agents access, use, and protect the security of service locations, computers, networks, PII, data, environments and other confidential information in a manner consistent with the terms of its agreement with Oracle and these Standards.

Contractor will employ clean desk and clear screen policies (i.e., policies and practices designed to restrict physical and logical access to confidential information on a need-to-know basis) to protect all data and other confidential information.

11. Verification, Monitoring and Audit

Contractor will maintain a complete list of all individuals with permission to access the network, environments and/or data, including their geographic location and citizenship.

If requested, contractor will certify to Oracle in writing its compliance with the requirements of these Standards, and will provide written responses to any questions that Oracle submits to contractor about its security practices.

To the extent permitted by law, Oracle may monitor contractor's access to and use of the environments and networks. Oracle also may perform security audits upon reasonable notice to confirm compliance with these Standards.

12. Miscellaneous Requirements for Specific Services

- If contractor is storing, processing or transmitting credit card information as part of the services, contractor will ensure that it is and remains PCI certified for compliance with the current version of the PCI Data Security Standards during the performance of the services. Contractor will provide Oracle with its most recent PCI Report on Compliance performed by its third party Qualified Security Assessor at Oracle's request.