Moat Analytics MSA
Data Processing Addendum

1. Scope, Order of Precedence and Term

1.1 These additional data privacy terms (the "**Data Processing Addendum**") apply to Oracle's Processing of Personal Data as part of Oracle's provision of Moat Services ("**Moat Services**"). The Moat Services are described in the Master Services Agreement by and between You and Oracle in which this Data Processing Addendum is referenced and all exhibits thereto (together the "**MSA**").

1.2 Except as expressly stated otherwise in the order, this Data Processing Addendum is incorporated into and subject to the terms of the MSA, and shall be effective and remain in force for the Term of the MSA.

1.3 Except as expressly stated otherwise in this Data Processing Addendum or the MSA, in the event of any conflict between the terms of the MSA, including any policies or schedules referenced therein, and the terms of this Data Processing Addendum, the relevant terms of this Data Processing Addendum shall take precedence.

1.4 You acknowledge and agree that (i) all rights and obligations under this Data Processing Addendum (including without limitation, audit rights and data processing instructions) shall be exclusively exercised by You and (ii) correspondingly, any notifications to be provided by Oracle under this Data Processing Addendum shall only be provided to You. In the event the applicable Master Services Agreement is the Oracle MSA for Moat Analytics (Agency), You shall ensure that appropriate contractual arrangements are put in place with Your Client(s) (as such term is defined in the MSA) in accordance with Applicable Data Protection Law. Notwithstanding the foregoing, Oracle has no obligation to ensure accuracy of instructions provided to Oracle by You and Oracle is not responsible for any incompatibility with instructions given by Your Clients to You.

2. Definitions

For the purposes of this Data Privacy Addendum:

2.1 "**Applicable Data Protection Law**" means (i) Directive 95/46/EC of October 24, 1995, as amended, on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data ('Directive') until such time that it is replaced by Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, applicable as of May 25, 2018; and (ii) any other data privacy or data protection law or regulation that applies to the Processing of Personal Data under this Data Processing Addendum;

2.2 "**You**" means the customer entity that has executed the MSA;

2.3 "**Data Subject**", "**Data Protection Impact Assessments**", "**Data Protection Officer**", "**Process/Processing**", "**Supervisory Authority**", **"Controller**", "**Processor**" and "**Binding Corporate Rules**" (or any of the equivalent terms) have the meaning set forth under Applicable Data Protection Law;

2.4 **"EU Model Clauses**" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision;

2.5 "**Oracle**" means the Oracle Affiliate that has executed the MSA;

2.6 "**Oracle Affiliate(s)"** means the subsidiar(y)(ies) of Oracle Corporation that may assist in the performance of the Moat Services as set forth in Section 3.4 below;

2.7 “**Personal Data**” means any information relating to a Data Subject that Oracle may Process on Your behalf as part of the Moat Services;

2.8 “**Third Party Subprocessor**” means a third party subcontractor, other than an Oracle Affiliate, engaged by Oracle and which may Process Personal Data as set forth in Section 3.4 below.

Other capitalized terms have the definitions provided for them in the MSA or as otherwise specified below.

3. Controller and Processor of Personal Data and Purpose of Processing

3.1 Unless Section 3.2 below applies, You are and will at all times remain the Controller of the Personal Data Processed by Oracle under the MSA. You are responsible for compliance with Your obligations as a Controller under Applicable Data Protection Law, in particular for justification of any transmission of Personal Data to Oracle (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Applicable Data Protection Law), and for Your decisions and actions concerning the Processing of such Personal Data.

3.2 In case You qualify as an agency and the applicable Master Services Agreement is the Oracle MSA for Moat Analytics (Agency) the following applies without prejudice to Section 1.4 above: (i) Your Client(s) will at all times remain the Controller of the Personal Data Processed by Oracle under the MSA, and (ii) Your Client(s) are responsible for compliance with their obligations as a Controller under Applicable Data Protection Law, in particular for justification of any transmission of Personal Data to Oracle (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Applicable Data Protection Law), and decisions and actions concerning the Processing of such Personal Data.

3.3 Oracle is and will at all times remain a Processor with regard to the Personal Data provided by You to Oracle under the MSA. Oracle is responsible for compliance with its obligations under this Data Processing Addendum and for compliance with its obligations as a Processor under Applicable Data Protections Law.

3.4 Oracle and any persons acting under the authority of Oracle, including any Oracle Affiliates and Third Party Subprocessors as set forth in Section 8, will Process Personal Data solely for the purpose of (i) providing the Moat Services in accordance with the MSA and this Data Processing Addendum (ii) complying with Your documented written instructions in accordance with Section 5, or (iii) complying with Oracle’s regulatory obligations in accordance with Section 13.

4. Categories of Personal Data and Data Subjects

4.1 In order to perform the Moat Services and depending on the Moat Services You have ordered, Oracle may Process some or all of the following categories of Personal Data: IP addresses and unique IDs collected from mobile devices network carriers or data providers (e.g., Mobile Advertising IDs).

4.2 Categories of Data Subjects whose Personal Data may be Processed in order to perform the Moat Services may include users of websites.

5. Your Instructions

5.1 Oracle will Process Personal Data on Your written instructions as specified in the MSA and this Data Processing Addendum, including instructions regarding data transfers as set forth in Section 7.

5.2 You may provide additional instructions in writing to Oracle with regard to Processing of Personal Data in accordance with Applicable Data Protection Law. Oracle will comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Moat Services, including assistance with notifying Personal Data breaches as set forth in Section 11, Data Subject requests as set forth in Section 6, and Data Protection

Impact Assessments (DPIAs).

5.3 Without prejudice to Oracle's obligations under this Section 5, the parties will negotiate in good faith with respect to any charges or fees that may be incurred by Oracle to comply with instructions with regard to the Processing of Personal Data that require the use of resources different from or in addition to those required for the provision of the Moat Services.

6. Rights of Data Subjects

6.1 If Oracle directly receives any Data Subject requests regarding Personal Data, it will promptly pass on such requests to You without responding to the Data Subject provided that the Data Subject has identified You as the Controller (acting on behalf of Your Client, as the case may be), unless otherwise required by Applicable Data Protection Law.

7. Personal Data Transfers

7.1 Oracle may access and Process Personal Data on a global basis as necessary to perform the Moat Services, including for IT security purposes, maintenance and performance of the Moat Services and related infrastructure, Moat Services technical support and Moat Service change management.

7.2 To the extent such global access involves a transfer of Personal Data originating from the European Economic Area ("EEA") or Switzerland to Oracle Affiliates or Third Party Subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national EEA data protection authority, such transfers are subject to (i) the terms of the EU Model Clauses incorporated into this Data Processing Addendum by reference; or (ii) other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Applicable Data Protection Law, such as approved Binding Corporate Rules for Processors. For the purposes of the EU Model Clauses if applicable, You and Oracle agree that (i) You will act as the data exporter on Your own behalf and on behalf of any of Your entities and Client(s) (if applicable), (ii) Oracle will act on its own behalf and/or on behalf of the relevant Oracle Affiliates as the data importers, (iii) any Third Party Subprocessors will act as 'subcontractors' pursuant to Clause 11 of the EU Model Clauses.

8. Oracle Affiliates and Third Party Subprocessors

8.1 Subject to the terms and restrictions specified in Sections 3.4, 7 and 8, You agree that Oracle may engage Oracle Affiliates and Third Party Subprocessors to assist in the performance of the Moat Services.

8.2 The Oracle Affiliates and Third Party Subprocessors are required to abide by the same level of data protection and security as Oracle under this Data Processing Addendum as applicable to their Processing of Personal Data. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Data.

8.3 Oracle remains responsible at all times for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Processing Addendum and Applicable Data Protection Law.

9. Technical and Organizational Measures, and Confidentiality of Processing

9.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data. These measures take into account the nature, scope and purposes of Processing as specified in this Data Processing Addendum, and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the Moat Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

9.2 In particular, Oracle has implemented the measures specified in the Information Security Program attached hereto as **Annex A** (the "**ISP**"). You are advised to carefully review the ISP to understand which specific security measures and practices apply and to ensure that these measures and practices are appropriate for the Processing of Personal Data pursuant to this Data Processing Addendum.

9.3. All Oracle and Oracle Affiliate staff, as well as any Third Party Subprocessors that may have access to Personal Data are subject to appropriate confidentiality arrangements. Oracle and Oracle Affiliate staff are required to periodically complete an information protection and confidentiality awareness training course.

9.4. Security Oversight and Enforcement. Oracle employs internal processes for regularly testing, assessing, evaluating and maintaining the effectiveness of the technical and organizational security measures described in this Data Processing Addendum and the MSA.

10. Audit Rights and Cooperation with You and Your Supervisory Authorities

10.1 You may audit Oracle's compliance with its obligations under this Data Processing Addendum up to once per year. In addition, to the extent required by Applicable Data Protection Law, including where mandated by Your Supervisory Authority, You or Your Supervisory Authority may perform more frequent audits. Oracle will contribute to such audits by providing You or Your Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Moat Services ordered by You.

10.2 If a third party is to conduct the audit, the third party must be mutually agreed to by You and Oracle (except if such Third Party is a competent Supervisory Authority). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

10.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions (for example, any request for information that could compromise Oracle security, privacy, employment or other relevant policies). Oracle will work cooperatively with You to agree on a final audit plan.

10.4 If the requested audit scope is addressed in a SOC1, SOC2, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

10.5 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

10.6 You will provide Oracle any audit reports generated in connection with any audit under this Section 10, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Supervisory Authority. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Addendum. The audit reports are Confidential Information of the parties under the terms of the MSA.

10.7 Any audits are at Your expense. The parties will negotiate in good faith with respect to any charges or fees that may be incurred by Oracle to provide assistance with an audit that requires the use of resources different from or in addition to those required for the provision of the Moat Services.

11. Incident Management and Personal Data Breach Notification

11.1 Oracle promptly evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or

Processing of Personal Data ("Incident"). All Oracle and Oracle Affiliates staff that have access to or Process Personal Data are instructed on responding to Incidents, including prompt internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence. Oracle's agreements with Third Party Subprocessors contain similar Incident reporting obligations.

11.2 In order to address an Incident, Oracle defines escalation paths and response teams involving internal functions such as Information Security and Legal. The goal of Oracle's Incident response will be to restore the confidentiality, integrity, and availability of the Moat Services environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident, Oracle may also involve and work with You and outside law enforcement to respond to the Incident.

11.3 To the extent Oracle becomes aware and determines that an Incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Oracle systems or the Moat Services environment that compromises the security, confidentiality or integrity of such Personal Data ("Personal Data Breach"), Oracle will inform You of such Personal Data Breach without undue delay but at the latest within 24 hours.

11.4 Oracle will take reasonable measures designed to identify the root cause(s) of the Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence. As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Oracle and to the extent permitted by law, Oracle will provide You with (i) a description of the nature and reasonably anticipated consequences of the Personal Data Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where possible, the categories of Personal Data and Data Subjects including an approximate number of Personal Data records and Data Subjects that were the subject of the Personal Data Breach; and (iv) other information concerning the Personal Data Breach reasonably known or available to Oracle that You may be required to disclose to a Supervisory Authority or affected Data Subject(s).

11.5 Unless otherwise required under Applicable Data Protection Law, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant Supervisory Authorities.

12. Return and Deletion of Personal Data upon Termination of Moat Services

12.1 Upon termination of the Moat Services or upon expiry of the retrieval period following termination of the Moat Services (if available), Oracle will promptly delete all copies of Personal Data from the Moat Services environment by rendering such Personal Data unrecoverable, except as may be required by law. Oracle's data disposal practices are described in more detail in the ISP.

13. Legally Required Disclosure Requests

13.1 If Oracle receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the Processing of Personal Data ("**Disclosure Request**"), it will promptly pass on such Disclosure Request to You without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

13.2 At Your request, Oracle will provide You with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for You to respond to the Disclosure Request in a timely manner.

* * *

ANNEX A
INFORMATION SECURITY PROGRAM

Oracle America, Inc.'s information is extremely valuable and must be treated as an asset that must be protected. Our objective, in the development and implementation of an Information Security Program and this Program ("**Program**"), is to create a plan designed to protect personal information and other sensitive information relating to our company, customers, users, employees, and business partners.

For purposes of this Program, "**personal information**" means any information relating to an identified or identifiable natural person that a customer or its end users provide to Oracle as part of the Moat services; an identified or identifiable natural person (a "data subject") is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

For purposes of this Program, "**proprietary information**" means all financial, business, legal and technical information which is developed, collected, learned or obtained by Oracle or in the course of its business activities or by its employees in the course of their employment, including information belong to or pertaining to Oracle's customers.

PURPOSE

The purpose of this Program is to establish processes and procedures designed to:

a) Protect the security and confidentiality of personal and proprietary information;

b) Protect against any anticipated threats or hazards to the security or integrity of all such information; and

c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of disclosure, identity theft or fraud.

HEAD OF SECURITY

Appointment and Responsibilities

Oracle has designated a Head of Security to implement, coordinate and maintain the Program. The Head of Security will be responsible for:

a) Initial implementation of the Program;

b) Training personnel;

c) Regular testing of the Program's safeguards;

d) Evaluating the ability of our third party service providers to protect, in the manner required by data security laws applicable to Oracle in its role a provider of cloud-based technology services ("applicable laws"), any personal information to which we have permitted them access and taking the steps reasonably necessary to ensure that any such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to such information under applicable laws;

e) Reviewing the scope of the security measures in the Program at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal and proprietary information; and

f) Conducting training sessions upon hire and biennially for all managers, employees and independent contractors, including temporary and contract employees, who have access to personal or proprietary information on the elements of the Program. Attendees must certify their attendance at the training and their familiarity with Oracle's requirements for protecting personal and proprietary information.

   Additionally, all new hires are required to receive Information Security Awareness Orientation before accessing any customer data or systems containing customer data.

Any questions or comments regarding the Program should be directed to the Head of Security. Following the earlier of the resignation or removal of the current Head of Security, a new Head of Security will be appointed as soon as reasonably practicable .

Breaches of Security

The Head of Security shall conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices if necessary relating to protection of personal and proprietary information following an incident involving a breach of security. The Head of Security shall document the foregoing and provide a report to executive management. "Breach of security" shall mean the misappropriation or unauthorized processing of personal information located on Oracle systems, including by an Oracle employee, that compromises the confidentiality, integrity or security of such personal information.

Routine Testing of Controls, Systems and Procedures

The effectiveness of the Information Security Program will be regularly evaluated and tested through the use of audits and operational testing where appropriate. Where possible and appropriate, security procedures will be tested and verified annually in a test or isolated environment. Oracle will reasonably monitor its systems for unauthorized use of or access to personal or proprietary information.

Evaluation and Adjustment

The Information Security Program will be reviewed at least annually or whenever there is a material change in business practices that may reasonably implicate the confidentiality, integrity or security of records containing personal or proprietary information to ensure that it contains administrative, technical, and physical safeguards designed to protect the confidentiality, integrity or security of the personal and proprietary information. In connection with such review, Oracle management will evaluate and adjust the Information Security Program as appropriate to address: (i) the current risk assessment, management and control activities; (ii) any new risks or vulnerabilities identified by Oracle management using the standards set forth above; (iii) any technology changes that may affect the protection of personal or proprietary information; (iv) material changes to our business, including to the size, scope and type of our business; (v) the amount of resources available to Oracle; (vi) the amount of personal or proprietary information stored or held by Oracle; (vii) any increased need for security of both consumer and employee information; and (viii) any other circumstances that Oracle management believes may have a material impact on the Information Security Program.

SCOPE OF PROGRAM

This Program applies to any activity that involves access to, or use or modification of, Oracle information and/or resources. This Program affects and encompasses Oracle's total information and physical environments.

Program Statement

Rights to use Oracle's information systems and computing resources will be based on each user's access privileges. Access privileges will be granted on the basis of specific business need (i.e. a "need to know" basis). Access controls must ensure that even legitimate users cannot access information unless they are authorized to do so. All Oracle resources, systems and applications will have access controls unless specifically designated as a public access resource.

Oracle's employees, temps, contractors, consultants, and other workers including all personnel affiliated with third parties, are responsible for participating in maintaining secure access to Oracle's information systems and computing resources and for ensuring that Oracle adheres to its posted Privacy Policy at http://www.moat.com/privacy. Oracle management will provide guidance in creating a secure access environment by establishing access management policies, approving roles and responsibilities, and providing consistent coordination of security efforts across the company. The Information Security Policies and Procedures listed below are approved by management and govern the information environment at Oracle.

Program Update and Notification

Oracle reserves the right to revise this Program at any time. Adequate notification of updates will be provided to all personnel. Personnel are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this Program.

SECURITY POLICIES AND PROCEDURES

Facilities Management

Access shall be restricted at each physical location where personal or proprietary information is stored to personnel and service providers who require access in order to perform their designated job functions or services. Where possible, storage areas containing personal or proprietary information will be protected against potential destruction or damage from physical hazards such as fire or floods. In furtherance of the foregoing, Oracle enforces the following restrictions:

- Hard copies of documents containing personal or proprietary information shall be stored in a locked room or cabinet, and access to such room or cabinet shall be restricted to the Chief Executive Officer, the Chief Financial Officer, the Head of Security and such other persons as may be approved by the Chief Executive Officer, the Chief Financial Officer or the Head of Security from time to time;
- Except as required by applicable building and safety codes, all access doors to Oracle's offices shall be locked at times when there is no receptionist on duty. When on duty, the receptionist shall escort all visitors to the appropriate locations within the office, or call someone else to do so.
- Terminated personnel are required to surrender all keys, IDs, access codes, badges, business cards and the like that permit access to Oracle's premises and/or systems. All Oracle property must be surrendered including work-from-home items such as headphones, monitors, etc.

Internal Computer Network Controls

Access to our computer networks, including wireless systems, and any files or programs containing personal or proprietary information is restricted to only those personnel who require such access to perform their job functions as determined by Oracle management. Such controls include the following:

- Oracle will retain at least one technician to provide support and routine maintenance of the network.
- Malware protection software must be installed on all employee workstations. All operating systems and applications will be upgraded with any currently available security patches or other security-related enhancements available from their providers in compliance with Oracle policy.
- Oracle's computer networks will be equipped with a firewall.
- All access to Oracle's computer networks and computers are subject to secure user authentication protocols set out below.
- Following the termination of employment of any of our personnel, steps are taken to prevent such terminated employee from accessing records containing personal or proprietary information, including by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.`
- To the extent that personnel are supplied with remote access devices, including, without limitation, laptops and handheld wireless access devices, Oracle will label them and take inventory at least annually.
- Personal or proprietary information stored on the network will be backed up on a regular basis. Any media containing backed-up personal or proprietary information must be secured in a locked room or file cabinet.
- To the extent technically feasible, Oracle will encrypt all records and files containing personal or proprietary information that will travel across public networks, all data containing personal or proprietary information to be transmitted wirelessly, and all personal or proprietary information stored on laptops or other portable devices.

USER AUTHENTICATION CONTROLS

Authenticating a User

<u>Restricted Access Devices</u>

Oracle information systems and/or computer resource usernames have an associated password with two-factor authentication to ensure that only the authorized user is able to access and utilize applications and/or systems.

Generic passwords should never be used. After a user's initial login, the user is required to change the password linked to the user's account for that information system or computer resource.

Invalid Login

In order to control user logons and maintain the effectiveness of access and authentication, user policies for all users on the Oracle domain must account for the following criteria:

- All Oracle user accounts are set to lockout the user after exceeding 5 invalid attempts. If a user attempts to logon to an Oracle domain incorrectly more than 5 times, the account will lock for 15 minutes.
- All lockout counters reset after no less than 15 minutes once a successful login is achieved.
- If access is required in less than 15 minutes, the user must contact the IT department.

Password policy

Oracle users shall follow the Oracle Password policy and ODC password standards. For mobile devices, such as smart phones and tablets, users shall follow the Oracle Mobile Device Management policy.

Users should immediately change their password if they suspect it has been compromised. Further, users must notify the appropriate security administrator when any access control mechanisms are broken or if they suspect they have been compromised.

Inactive Workstations

Inactive workstations are automatically locked after 10 minutes. Users are required to verify their identity as the last user of that workstation in order to unlock an inactive workstation.

System / Application Logging Requirements

Oracle maintains and appropriately store operator logs. These logs are subject to regular, independent reviews and should include:

- System logs
- Security logs
- Security alerts (from security appliances)
- Application logs
- Network equipment logs (including firewalls and wireless equipment)
- System errors and corrective actions taken (especially automated error recovery)
- Successful and unsuccessful logins

Security Fault Log

A log of all security faults involving Oracle information systems and services is maintained.

Standards - Logon Monitoring

User event logging systems contain at a minimum the following information:

- User ID
- Dates and times of logon and logoff
- Logon method, location, terminal identity (if possible), network address
- Records of successful and unsuccessful system access attempts
- Records of successful and rejected data access and other resource access attempts

Log Archiving

The length of retention should reflect the availability of resources and the need to track historical information and the possibility of providing evidence in future investigations. Storage and access to the logs should be sufficient to meet the requirements of evidence collection.

Access Audits

Access to Oracle's facilities and systems is audited on a quarterly basis. Oracle audits access levels to all corporate systems.

Enforcement

Users are responsible for all personal account usernames, passwords, tokens, and related personal identification numbers (PINs). Oracle users are not to share personal account information with any other individual for any reason. Sharing of account usernames, passwords, tokens, and/or PIN pertaining to any Oracle facilities, networks or applications is strictly forbidden and may be punishable by appropriate administrative action up to and including termination.

INTERNAL RISKS

To combat internal risks to the confidentiality, integrity or availability of any electronic, paper or other records containing personal or proprietary information, and evaluating and improving the effectiveness of current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

Internal Threats

- A copy of this Program must be distributed to each employee who shall, upon receipt of the Program, acknowledge in writing that he/she has received a copy of the Program and a copy will be retained by Oracle.
- The amount of personal or proprietary information collected must be limited to that amount reasonably necessary to accomplish Oracle's legitimate business purposes or necessary to comply with applicable laws and regulations.
- Access to records containing personal or proprietary information shall be limited to those persons who are reasonably required to know such information in order to accomplish a legitimate business purpose or to enable Oracle comply with applicable laws and regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access will be blocked.
- All persons are required to report any suspicious or unauthorized use of personal or proprietary information.
- All persons are prohibited from keeping open files containing personal or proprietary information on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing personal or proprietary information must be secured in a manner that is consistent with the Program's rules for protecting the security of personal or proprietary information.
- Access to electronically stored personal or proprietary information shall be electronically limited to those having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a ten minutes.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with applicable laws.

EXTERNAL RISKS

To combat external risks to the confidentiality, integrity and availability of any electronic, paper or other records containing personal or proprietary information, and evaluating and improving the effectiveness of current safeguards for limiting such risks, the following measures are mandatory:

External Threats

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the confidentiality, integrity and availability of personal or proprietary information, installed on all systems processing personal or proprietary information.

- There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal or proprietary information.
- To the extent technically feasible, all personal or proprietary information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly. Encryption here means the transformation of data using SSL or other industry-accepted encryption, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.

Mobile Computing

Only Oracle-approved portable computing devices may be used to access Oracle information resources. To access the Internet, the mobile device must be compliant with the IEEE 802.11b or IEEE 802.11g protocols. Mobile computing devices at Oracle must adhere to the following:

- All remote access connections made to the Oracle environment must be made through the approved remote access tools provided by Oracle.
- Remote access connections made to Oracle will include an industry-acceptable form of encryption, e.g. https with 2048-bit keys, SSL with 2048-bit key, or VPN.
- Non-Oracle computer systems that require network connectivity must conform to Oracle's IT standards.

HANDLING AND DISTRIBUTION OF DATA

Protection of Data

Acceptable Use

All Oracle personnel must use good business judgment in choosing the content and recipients of Internet messages such as e-mail or instant messages, responding in a timely manner, and deleting unneeded messages. Personnel shall not transmit personal or proprietary information over the Internet unless they are using an Oracle-approved transmission method and never using their personal email. Oracle personnel may not change the hardware or software configuration of any Oracle resources without specific permission from the IT team.

Backups

Backups of all essential Oracle electronically stored business data will be routinely created and properly stored to ensure prompt restoration. All data backed up to tape must be encrypted.

Environmental

Adequate environmental controls will be in place and monitored to prevent data loss due to preventable and/or treatable environmental threats.

Disposal of Data

Removable Media

When no longer required, the contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable state, federal, or internal business unit requirements.

Storage Devices

Prior to disposal or re-use, equipment containing storage media should be cleansed to prevent unauthorized exposure of data. Cleansing procedures should be used that will render all information unrecoverable. An "erase" feature (i.e. putting a document in the desktop recycle bin) is not sufficient.

Printed Material

When no longer required, all sensitive printed material shall be disposed of by an internal machine that will shred and dispose of all material in the bins on-site at an agreed upon frequency.

Destruction of Media

Prior to disposal, destroy defective or damaged media (USBs, CDs, tapes) containing sensitive information to render the information unrecoverable. Shred all hardcopy materials that contain sensitive information.

Standards - Secure Media Disposal

Dispose of worn, damaged, or otherwise no longer required media in a secure manner. To prevent the compromise of sensitive information through careless or inadequate disposal of computer media, consider the following controls:

- Media that may require secure disposal include: paper documents, recordings, output reports, magnetic tapes, removable disks or cassettes, optical storage media, program listings, test data, and system documentation.
- Dispose of media containing sensitive information by secure incineration or shredding.
- If planning to reuse magnetic or optical media, completely empty it of data through use of special software designed to securely erase and/or reformat the media. If software is unavailable, reformatting the media a minimum of three times is required.
- Use access restrictions to identify unauthorized personnel.
- Store media in accordance with manufacturer's specifications.

SERVICE PROVIDERS

Prior to engaging any third-party service provider who may receive personal or proprietary information, Oracle will take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal or proprietary information and will contractually require that all such third-party service providers implement and maintain appropriate security measures to protect personal or proprietary information.

EMPLOYEE MANAGEMENT AND TRAINING

Oracle will implement appropriate measures to ensure that all personnel are informed of and comply with the Information Security Program. Such measures will include the following:

- All Oracle employees are required to complete an information protection awareness course. 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 personnel will be trained to take steps to maintain the confidentiality, integrity and availability of personal and proprietary information, including: locking rooms and file cabinets where paper records are kept; using password-activated screensavers; using strong passwords; periodically changing passwords; disposing of personal and proprietary information in a secure manner; not keeping open files containing personal or proprietary information on their desks when they are not at their desks; and securing all physical and electronic files at the end of the work day in a manner consistent with this Information Security Program.
- Disciplinary measures will be imposed for breaches of the Information Security Program. In determining what action is appropriate in a particular case, Oracle management will take into account all relevant information, including the nature and severity of the violation, whether the violation was a single occurrence or repeated occurrences, whether the violation appears to have been intentional or inadvertent, whether the individual in question had been advised prior to the violation as to the proper course of action and whether or not the individual in question had committed other violations in the past.

OPERATING STANDARDS

1. An annual risk assessment must be performed by qualified personnel to properly identify security risks, threats and vulnerabilities.

2. This Information Security Program must be reviewed at least annually and updated as needed to reflect changes in the operating environment at Oracle.

3. Oracle should create a list of all devices, systems and applications used in processing, transmitting and/or storing sensitive Oracle data including customer payment information.

4. A formal security awareness plan should be documented, available and disseminated biennially and upon new hire or engagement.

5. A qualified incident response team should be formally assigned and responsible for crisis management including reporting theft and/or data breaches to the proper authorities and third parties.

6. A formal incident response plan should be documented and executable in the event of a crisis.

7. Business units should maintain a listing of third parties with access to Oracle information, including service providers.

8. All newly hired employees and contractors should review and sign the Oracle Information Security Program. The signed documentation should be filed and retained.

9. Terminated users' accounts to all applications, systems, resources and physical access shall be revoked, disabled and terminated immediately following exit.

10. Oracle information must be protected from unauthorized disclosure, modification, or destruction. Prudent information about security standards and practices must be implemented to ensure that the integrity, confidentiality, and availability of Oracle information are not compromised.

11. All hardware and software operated by business units of Oracle should be documented in compliance with all applicable company or business unit asset management standards.

12. Oracle has procedures to prevent and detect unauthorized access or damage to facilities that contain information systems.

13. Restricted areas within facilities that house sensitive or critical information systems will at a minimum utilize physical access controls designed to permit access by authorized users only.

14. To maintain the availability, integrity and confidentiality of information, computer and communications equipment should be secured from physical and environmental threats.

15. Prior to re-use, equipment containing storage media shall be cleansed to prevent unauthorized exposure of data.

16. Changes to all information processing facilities, systems, software, or procedures will be strictly controlled according to formal change management procedures.

17. Security incident management procedures should be established within each business unit to ensure quick, orderly, and effective responses to security incidents.

18. System capacity requirements should be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

19. System acceptance criteria for all new information systems and system upgrades must be defined, documented, and utilized to minimize risk of system failure, in addition, a clear back out method must be documented and available.

20. Security awareness, prevention, and detection controls should be utilized to protect information systems and services against malicious code.

21. Back-ups of all essential Oracle electronically stored business data will be routinely created and properly stored to ensure prompt restoration.

22. A log of all security faults involving Oracle information systems and services shall be maintained.

23. Oracle computing resources will be sufficiently monitored by appropriate business unit personnel to detect deviations from authorized use.