Oracle Global Business Unit Cloud Services-Pillar Document

Effective Date: December 2022

TABLE OF CONTENTS

SCOPE

This document applies to Oracle Global Business Unit (GBU) Cloud Services.

The Oracle Global Business Unit Cloud Services organization supports the cloud offerings provided by the following:

- Communications Global Business Unit (CGBU),
- Communication Applications Global Business Unit (CAGBU),
- Construction and Engineering Global Business Unit (CEGBU),
- Financial Services Global Business Unit (FSGBU),
- Food and Beverage Global Business Unit (FBGBU),
- Health Care Global Business Unit (HCGBU),
- Health Sciences Global Business Unit (HSGBU),
- Hospitality Hotel Global Business Unit (HGBU),
- Retail Global Business Unit (RGBU),
- Local Government Global Business Unit, and
- Energy and Water Global Business Unit.

This document supplements the Oracle Cloud Hosting and Delivery Policies. Its purpose is to account for exceptions and additional terms specific to the Oracle Global Business Units. This document's content takes precedence over the Oracle Cloud Hosting and Delivery Policies.

1 ORACLE CLOUD SERVICE LEVEL AGREEMENT

1.1 Service Availability

For the purposes of this section, the following definitions will apply:

Applicable Cloud Services Fees	• Refers to the Cloud Services fees that are paid to Oracle for the affected Oracle GBU Cloud Services for the monthly reporting period in which the applicable Target Service Availability Level (or Target Service Uptime) is missed and for which You are entitled to receive Service Credits in accordance with the *Oracle Cloud Hosting and Delivery Policies.* • If You have purchased Oracle GBU Cloud Services from an Oracle partner, You agree that any Service Credits will be issued to that partner and You acknowledge that You are solely responsible for ensuring that any Service Credits

	are passed on to You. You acknowledge that Oracle will have no liability to You, the applicable Oracle partner, or any other party if the full benefit of the credit is not passed on to You. ● Applicable Cloud Services Fees do not include the fees paid for other Cloud Services that met the defined Target Service Availability Level (or Target Service Uptime).
Available or Availability	For the purposes of calculating the service availability level of the Oracle GBU Cloud Services, “available” or “availability” means that You and Your users are able to log in and access the Online Transaction Processing (OLTP), Reporting, or Transactional portions of the Oracle GBU Cloud Services.
Measurement of Service Availability Level	As defined in in Section 3.2.1 of the *Oracle Cloud Hosting and Delivery Policies.*
Service Credits	● 2% of the monthly Applicable Cloud Services Fees for every .1% that the Service Availability Level of the affected Oracle GBU Cloud Services is below the applicable Target Service Availability Level (or Target Service Uptime) during a monthly reporting period. ● In no event may the quantity of Service Credits in a monthly reporting period exceed 10% of that month’s Applicable Cloud Services Fees.
Scheduled Downtime	Refer to Change Management Section 2.1 in this document.
Target Service Availability Level (or Target Service Uptime)	Target Service Availability Level objectives are as outlined in the Oracle Cloud Service Level Agreement Section 3.2 in the Oracle Cloud Hosting and Delivery Policies document, or in the applicable service description related to the specific Global Business Unit cloud service.

You will be entitled to receive Service Credits if the Service Availability Level of the affected Oracle GBU Cloud Services is below the applicable Target Service Availability Level (or Target Service Uptime) in 2 or more calendar months during any 6 month period. If You have more than one production instance within a Service, the Service Availability Level or Service Uptime will be calculated as an average across all such production instances for a monthly reporting period. Service Credits will be paid starting with the second month in which the applicable Target Service Availability Level (or Target Service Uptime) is missed during the applicable 6 month period (i.e., no Service Credits will be provided for the first month missed).

To receive Service Credits, You must submit a claim within 30 days from when You became eligible to receive such Service Credits. You will be entitled to receive only one amount of Service Credits per monthly reporting period in which the applicable Target Service Availability Level (or Target Service Uptime) is missed. The Service Credits will be provided only towards any outstanding balance for the affected Oracle GBU Cloud Services that, as of the date You receive the Service Credits, is owed to Oracle under the relevant order for such Cloud Services, and the provision of these Service Credits represents YOUR EXCLUSIVE REMEDY, AND ORACLE'S ENTIRE LIABILITY, for the missed Target Service Availability Level (or Target Service Uptime).

1.2 Termination for Unavailability

The Oracle Cloud Service Level Agreement establishes a Target Service Availability Level (or Target Service Uptime) and describes how Oracle defines, measures and reports service availability. If the Service Availability Level of the production Services environment for the Cloud Services fails to meet the Target Service Availability Level (or Target Service Uptime) for at least 3 consecutive months, You may, upon written notice to Oracle, terminate the applicable Cloud Services as of the termination date specified in such notice, provided that You notify Oracle within 30 days. Following the effective date of such termination, You will receive a refund for any fees that You prepaid to Oracle for the terminated Cloud Services for the period following the effective date of the termination.

2 ORACLE CLOUD CHANGE MANAGEMENT POLICY

2.1 Application Upgrades and Updates

Oracle requires all GBU Cloud Services customers to keep their GBU Cloud Services current with versions that Oracle designates as Generally Available (GA). GBU Cloud Service updates or upgrades will follow every GA release and are required to maintain GBU Cloud Service version currency. For certain GBU Cloud Services, Oracle will upgrade Your non-production environment to the latest GA version before upgrading the production environment.

Oracle Cloud Hosting and Delivery Policies, such as the Service Level Agreement, and the Support Policy, depend upon on You maintaining GA version currency. Oracle is not responsible for performance or security issues encountered with the Cloud Services that may result from running earlier versions. Oracle will provide prior notice for updates or upgrades that involve service interruption to You.

Oracle typically schedules application upgrades every 2nd and 4th Friday of the month between 21:00-06:00 (Saturday) data center local time. For some GBU Cloud Services, Oracle will schedule upgrades on a weekday to accommodate Your business operations.

If You are eligible to select Your own upgrade window, You will either be contacted by Oracle to coordinate the upgrade change window, or You will be able to select target hours and dates with the exception of blocked time periods that Oracle reserves for core system maintenance.

2.2 Application Changes

Access to production servers at the operating system and database level is restricted to Oracle Global Business Unit Cloud Services and Application Management groups. You may only change the GBU Cloud Service using defined user interfaces, web services, or standardized application programming interfaces, also referred to as "APIs." Alteration or extension of the underlying base GBU Cloud Service code is not permitted.

2.3 Core System Maintenance

Core system maintenance involves changes to hardware, network systems, security systems, operating systems, storage systems, or general supporting software of the cloud infrastructure. Core system maintenance may result in service interruption. Oracle works to limit any service interruption due to core system maintenance to less than 2 hours during a scheduled service period. Oracle may elect not to schedule a core system maintenance event.

Oracle typically schedules core system maintenance on Fridays between 21:00- 06:00 (Saturday) data center local time.

2.4 Routine Infrastructure Maintenance

Oracle manages routine infrastructure maintenance activities for the purpose of providing environment currency, capacity, and stability. Routine maintenance is not expected to result in a service interruption. When possible, routine infrastructure maintenance will be performed during the core system maintenance window.

2.5 Supported Versions and End of Life (EOL) for Oracle Global Business Unit Cloud Services

Oracle will provide You with no less than 12 months advance notice prior to the date when the Oracle GBU Cloud Services are no longer generally available as a service (i.e., Oracle will no longer support, or make available for use, any versions of the GBU Cloud Services).

Specific GBU Cloud Services have published Supported Versions and EOL practices information. Where applicable, the documentation is available here: https://www.oracle.com/corporate/contracts/cloud-services/service-descriptions.html.

3 ORACLE CLOUD SERVICE CONTINUITY POLICY

3.1 Disaster Recovery

Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Oracle, that leads to loss of a data center and corresponding service unavailability. For the purposes of this Policy, a “disaster” means an unplanned event or condition that causes a complete loss of access to the primary site used to provide the GBU Cloud Services such that Your production environments at the primary site are not available.

Recovery Time Objective: A Recovery Time Objective (RTO) is Oracle’s objective for the maximum period of time between Oracle’s decision to activate the recovery process to the secondary site, due to a declared disaster, and the point at which You can resume production operations in the secondary production environment. If the decision to failover is made during the period in which an upgrade is in process at the secondary site, the RTO extends to include the time required to complete the upgrade.

Recovery Point Objective: A Recovery Point Objective (RPO) is Oracle’s objective for the maximum possible length of time during which data could be lost in the event of a disaster. The RPO time excludes any data loads that may be under way when the disaster is occurring.

The RTO and RPO do not apply to customizations that depend on external components or third-party software. During active failover events or recovery operations, non-critical fixes and enhancement requests are not supported. You will be solely responsible for issues arising from third party software and customizations to GBU Cloud Services.

The RTO and RPO Level objectives are as outlined in the applicable service description related to the specific Global Business Unit Cloud Services.

Upon Oracle’s declaration of a disaster, Oracle will commence the Disaster Recovery Plan to recover production data to the most recent available state to reconstitute the production environments of the affected Cloud Services with the Recovery Time and Recovery Point Objectives as defined in the service description for the applicable Global Business Unit Cloud Services. Production services may operate in a degraded state of performance for the duration of the disaster event.

4 INFORMATION TRANSFER

4.1 Secure File Transfer Protocol (SFTP)

The secure file transfer protocol (SFTP) services, if used for Oracle Cloud Services, are limited-access systems for the purpose of uploading or downloading data files in a secure manner. SFTP downloads/uploads are recorded in an electronic audit log that includes: date and time, user name, and name of file up/downloaded.

Traceability of user requests for SFTP access and modifications to access rights is provided through change control processes.

4.2 Account Usage

Oracle reserves the right to restrict access, limit use of the SFTP Service, or remove access for any nonconforming users, sites, or customers, without prior notification, whenever the use of the service is not in compliance with the terms of use. Access is granted on each account to specific directories using the principle of least privilege. Customer accounts have full read-write access to the data in each directory to which the user has access.

Technical controls in place are designed to ensure confidentiality of data and to prevent unauthorized access to other accounts' data. Attempts to access directories not authorized for a given account are a violation of the terms of use, and the account may be suspended. Oracle is not responsible for unauthorized customer access to data within a directory by an account which has authorized and approved access.

4.3 Account Provisioning

Currently, SFTP accounts are created with a strong 10-character password. The account password will be sent in an email to the address associated with the account. For this reason, the email address associated with an account must be a valid individual email and may not be a shared account or company e-mail distribution list. Inactive accounts will be disabled, and then deleted under the following schedule:

Accounts that are inactive for 3 months will be disabled.

Accounts that are inactive for 6 months will be deleted.

You must submit a service request to terminate accounts that are no longer required or need to be revoked.

4.4 Account Authentication

Passwords are automatically generated and cannot be changed by the account holder or recovered by Oracle. If a password needs to be changed or reset, the account holder must submit a formal service request to have a new password generated. The updated account password will be sent in an email to the address associated with the account.

4.5 Account Authentication – Alternate Automation Methods

The SFTP service supports public key authentication: a method of automatic password-less login. Each account has a public key directory. By generating a local private and public key pair, uploading the public key file to this directory, and configuring the client software to use public key authentication, an account user can log in without being prompted for a password. Multiple public key files per account are supported by Oracle.

4.6 Acceptable Usage

All data transferred via the SFTP service must be for the specific business purpose and function of supporting Your hosted environment(s). The SFTP service may not be used for data backups, temporary storage, unlicensed copyrighted materials, or other illegal materials. Your integrations employing the use of automated data transfer agents or 'scripts' are permitted, however they should either run manually or on a periodic schedule not to exceed a SFTP connection rate of 10 times per hour. The use of automated processes that aggressively connect, or that do not properly connect, authenticate, perform an appropriate file transfer operation, or properly disconnect, is a violation of the terms of use.

4.7 Data Storage

Data stored on the SFTP server will automatically be deleted after 60 days. All incoming and outgoing SFTP data is considered transient data and not subject to backup retention. The only exception is that the directory structure and any ssh login key file information is retained and not automatically deleted.

4.8 Payload Encryption Requirements – Data-at-Rest

If the service offering is subject to external regulatory requirements such as PCI DSS that mandates data-at-rest encryption, the configuration of the Oracle SFTP service for the deployment will employ the use of whole disk encryption, or the service will be designed to accept incoming encrypted data files with an Oracle provided public key or x.509 certificate. Conversely, if the service offering has outbound data and file transfer integrations, then You must provide Oracle with a bonafide x.509 certificate for SFTP data integrations.

4.9 Encryption Requirements – Transport

Industry security standards and Oracle security policies mandate end-to-end (socket-to-socket) based transport encryption for data exchange. Use of FTP over SSL (FTPS) and FTP does not guarantee transport encryption is either properly enforced or negotiated during the initiation of the data connection, and the latter protocol (FTP) is completely lacking any transport encryption. Therefore, Oracle data transfer standards is limited to SFTP with the goal of ensuring confidentiality of data transfers between Oracle and You.

5 COMPLIANCE

5.1 Audit Reports

Audit reports and letters of compliance for Oracle Cloud Services are periodically published by Oracle's third party auditors. Reports and letters may not be available for all services or at all times. You may request a copy of the current published audit report or letter available for a particular Oracle Cloud Service, as applicable, by contacting the Oracle Sales Representative or designated Oracle account contact and providing the following information:

- Company name
- Contact name
- Title
- Recipient e-mail address
- Request justification (e.g., purpose and intended use description)

6 ORACLE UTILITIES OPOWER CLOUD SERVICES

For additional details regarding specific Oracle Utilities Opower Cloud Services, please refer to the Oracle Utilities Opower service descriptions.

6.1 Change Management

Application Upgrades and Updates

For Oracle Utilities Opower Cloud Services, Oracle schedules application upgrades between 11:00 – 15:00 Eastern US time every third Sunday. Customer notifications are sent 72 hours in advance of such upgrades.

Core System Maintenance

For Oracle Utilities Opower Cloud Services, Oracle schedules core system maintenance between 03:00 – 07:00 Eastern US time on the last Thursday of each month. Customer notifications are sent 72 hours in advance of such upgrades.

6.2 Access Control

Privilege Management

In lieu of a proxy server, Oracle administrative access to the Oracle Utilities Opower Cloud Services environment requires administrators to first connect to a trusted network to be able to access the systems.

Access to the trusted network requires physical access to the network or authentication to the network by means of a username and password. All access to the trusted network from remote locations requires multifactor authentication.

6.3 Communication and Operations Management

Backups

The Data Integration Platform components of the Oracle Utilities Opower Cloud Services include customer AMI (or “smart meter”) data which is not backed up to disk or tape. Instead, disaster resiliency for this component relies on a data replication strategy. Non-personally identifiable AMI data resident within this component is automatically replicated to a standby cluster within the same jurisdictional region on a daily basis.

Daily backups are used to recover Oracle Utilities Opower Services in the event of a disaster. Oracle operates only one data center in Canada. Backups for disaster recovery purposes are stored in an encrypted format at a secondary site in the United States.

6.4 Termination of Oracle Utilities Opower Cloud Services

For a period of 60 days upon termination of the Oracle Utilities Opower Cloud Services (the “Retrieval Period”), Oracle will make available, via secure protocols and in a structured, machine-readable format, Your Content (which may not include all content provided by parties which You have been invited to access the Oracle Utilities Opower Cloud Services or Your environment) residing in a production Oracle Utilities Opower Cloud Services environment, and will maintain the service system so that it remains accessible to You for data retrieval during the Retrieval Period. You should not use the environment for production activities.

If You need assistance from Oracle to obtain access to or to obtain copies of Your Content, You must create a service request in the Cloud Customer Support Portal applicable to the Your Oracle Utilities Opower Cloud Services.

Data retrieval and any related assistance by Oracle is not applicable for Oracle Utilities Opower Cloud Services that do not store Your Content. You are responsible for ensuring that if those Oracle Utilities Opower Cloud Services are dependent on separate Oracle Cloud Services (such as Storage Cloud Service or Database Cloud Services) for the storage of data, those separate non-Opower Oracle Cloud Services must have a valid duration through the end of the terminating non-Opower Oracle Cloud Service to enable data retrieval, or for otherwise taking appropriate action to back up or otherwise store separately Your Content while the production Oracle Utilities Opower Cloud Services environment is still active prior to termination.

Following expiration of the Retrieval Period, Oracle will delete or render unrecoverable Your Content from all production Oracle Utilities Opower Cloud Services environments (unless otherwise required by applicable law). Such processing may take up to 180 days.

6.5 Device Cloud Services

Oracle Utilities Opower Device Cloud Services (“Device Cloud Services”) consist of the following Cloud Services:

- Oracle Utilities Opower Device Control Cloud Service, Platform – 100 in Customer Count,
- Oracle Utilities Opower Device Control Cloud Service, Control Thermostat – 100 Utilities Devices, and
- Oracle Utilities Opower Device Control Cloud Service, Control Other Devices – 100 Utilities Devices

Sections 1.2, 1.6, and 6.1 of the Oracle Cloud Hosting and Delivery Policies are inapplicable to the Device Cloud Services.

Device Cloud Services are deployed by a third party environment provider and therefore, while security policies and software security assurance policies are in place, they may be different from Oracle's policies referenced in Sections 1.10 and 1.13, respectively, of the Oracle Cloud Hosting and Delivery Policies.

Notwithstanding Section 3.4.2 of the Oracle Cloud Hosting and Delivery Policies, You may not assess or test any components in Device Cloud Services, including non-Oracle applications, non-Oracle databases, other applicable non-Oracle software, code, or the use of data scraping tools.

6.6 Business Customer Engagement Portal Cloud Service

Oracle Utilities Opower Business Customer Engagement Portal Cloud Service consists of the following Cloud Service:

- Oracle Utilities Opower Business Customer Engagement Portal Cloud Service – 100 in Customer Count

Section 1.2 of the Oracle Cloud Hosting and Delivery Policies is inapplicable to the Business Customer Engagement Portal Cloud Service.

Business Customer Engagement Portal Cloud Service is deployed by a third party environment provider and therefore, while security policies and software security assurance policies are in place, they may be different from Oracle's policies referenced in Sections 1.10 and 1.13, respectively, of the Oracle Cloud Hosting and Delivery Policies.

Section 6.1 of this document is inapplicable to Business Customer Engagement Portal Cloud Service.

6.7 Video Generation

Oracle Utilities Opower Channel Fee – Video Generation consists of the following Cloud Service:

- Generation of video emails for Home Energy Reports (HER)

For clarity, sections 1.1, 1.2, 1.9, 1.13, 2, 3, 4.1, 5, and 6 of the Oracle Cloud Hosting and Delivery Policies are inapplicable to the Video Generation Cloud Service. Due to the nature of this Cloud Service, there is no retrieval period after the ninety (90) days of availability of the Video Home Energy Report.

Video Generation Cloud Service is deployed by a third party environment provider and therefore, while security policies are in place, they may be different from Oracle's policies referenced in the Oracle Cloud Hosting and Delivery Policies.

The third party supplier has its own methodology for building security into the design, build, testing, and maintenance of the Video Home Energy Reports, and the third party supplier manages backups of the Video Home Energy Reports.

Unless otherwise provided in Your order, no Service Level Agreement applies to the Video Generation Cloud Service.

For clarity, sections 1, 2, 3, 4.3, 5, 6.1 and 6.4 of this document are inapplicable to the Video Generation Cloud Service.

The maintenance window is Sunday from 6:00 AM to 12:00 PM Pacific Time. The application is maintained by the third party supplier. Audit reports are not available for the Video Generation Cloud Service.

7 ORACLE CONSTRUCTION AND ENGINEERING CLOUD SERVICES

7.1 Oracle Textura & Primavera Submittal Exchange Cloud Services

7.1.1 Change Management

Application Upgrades and Patches

- Oracle Textura Payment Management Cloud Services
  - For the Oracle Textura Payment Management Cloud Services US Instance, Oracle schedules *application upgrades* between 07:00 – 11:00 Eastern US time every first and third Sunday.
  - For the Oracle Textura Payment Management Cloud Services AU Instance, Oracle schedules *application upgrades* between 07:00 – 11:00 Eastern US time every first and third Sunday.
  - For the Oracle Textura Payment Management Cloud Services Europe Instance, Oracle schedules application upgrades between 16:00 – 20:00 Eastern US time every Monday following the US/AU application upgrade.
  - For the Oracle Textura Payment Management Cloud Services US Instance, Oracle schedules *application patches* between 00:00 – 01:00 Eastern US time (Monday – Friday).
  - For the Oracle Textura Payment Management Cloud Services AU Instance, Oracle schedules *application patches* between 09:00 – 10:00 Eastern US time (Monday – Friday).
  - For the Oracle Textura Payment Management Cloud Services Europe Instance, Oracle schedules application patches between 16:00 – 17:00 Eastern US time (Monday – Friday).
- Oracle Textura Pre-Qualification Management Cloud Services
  - For the Oracle Textura Pre-Qualification Management Cloud Services, Oracle schedules *application upgrades* between 23:30 – 03:30 Eastern US time on the Friday before the second Sunday of each month.

  - For the Oracle Textura Pre-Qualification Management Cloud Services, Oracle schedules *application patches* between 23:30 – 03:30 Eastern US time every Friday.
- Primavera Submittal Exchange Cloud Services
  - For the Primavera Submittal Exchange Cloud Services, Oracle schedules *application upgrades* between 20:00 – 23:00 Eastern US time every weekday.

Core System Maintenance

- Oracle Textura Payment Management Cloud Services
  - For the Oracle Textura Payment Management Cloud Services US Instance, Oracle schedules *core system maintenance* between 07:00 – 11:00 Eastern US time every first and third Sunday.
  - For the Oracle Textura Payment Management Cloud Services AU Instance, Oracle schedules *core system maintenance* between 07:00 – 11:00 Eastern US time every first and third Sunday.
  - For the Oracle Textura Payment Management Cloud Services Europe Instance, Oracle schedules core system maintenance between 16:00 – 20:00 Eastern US time every Monday following the US/AU core system maintenance.
- Oracle Textura Pre-Qualification Management Cloud Services
  - For the Oracle Textura Pre-Qualification Management Cloud Services, Oracle schedules *core system maintenance* between 07:00 – 11:00 Eastern US time every Sunday.
- Primavera Submittal Exchange Cloud Services
  - Oracle schedules *core system maintenance* between 09:00 – 11:00 Eastern US time every Sunday and 20:00 – 23:00 Eastern US time every weekday.

7.1.2 Termination Policy

Oracle Textura Cloud Services:

After termination or expiration of the Oracle Textura Cloud Services under Your order, or upon termination of the following retrieval period for such Oracle Textura Cloud Services, Oracle will disable Your access to the production Oracle Textura Cloud Services environment and will delete Your Personal Data (as that term is defined in the Data Processing Agreement for Oracle Cloud Services) relating to You residing in the production environment, except as may otherwise be required by law. Users and other third parties who are enabled to interact with Your production Oracle Textura Cloud Services environment may continue to access the environment and any data (including Your transactional data, Your invoice history, Your project history, etc.) that is not Personal Data relating to You.

For a period of no less than 60 days after the termination or expiration of the Oracle Textura Cloud Services under Your order, Oracle will make available Your production data via secured protocols, or keep Your access to the production Oracle Textura Cloud Services environment accessible, for the purpose of data retrieval by You. During this period, You should not use the environment for production activities. Oracle has no obligation to retain your data after this 60 day period.

Textura Payment Management

Following the date on which Oracle determines that both (i) all Projects, Contracts and Invoices managed on the cloud service have been paid in full and (ii) no Users from the related organization have logged in to Your production Oracle Textura Cloud Services environment for 180 days, Oracle will send an email notice to any User with administrator rights to the environment, indicating that all Personal Data, of any User, that is in the environment will be deleted or rendered unrecoverable unless a User logs in to the environment within 30 days from the date of the email notice. If no User logs in to the environment within 30 days of the date of the email notice, then all Personal Data, of any User, that is in the environment will be subsequently deleted, except as may otherwise be required by law.

Primavera Submittal Exchange Cloud Services

Following the data retrieval period, Oracle may retain Your data, including Personal Data, for at least an additional 180 days to allow for reasonable restoration or recovery of Your Primavera Submittal Exchange Cloud Services. Restoration of Your production Cloud Services may be requested by You, Your Users, or other third parties who were enabled to interact with Your production Primavera Submittal Exchange Cloud Services environment at the time of expiration of Your Cloud Service. Restoration of services may be subject to additional cost and fees. If no request(s) for restoration are received by Oracle within 180 days following the data retrieval period, all Personal Data, of any User, relating to the production environment will be deleted or rendered unrecoverable, unless otherwise required by law. Oracle has no obligation to retain Your data during this 180 day period. Any request for production Cloud Service restoration submitted to Oracle, even within the 180 day period following the data retrieval period, does not ensure the Cloud Service will be restored, and Oracle has no obligation to fulfill any such request.

7.1.3 Backups

Primavera Submittal Exchange data is backed up in real-time to a site separate from that at which the instance is running and may be used as recovery data in the event of a disaster. Backups of Database files are also synchronized to the same separate location site at least once an hour. All data is encrypted during synchronization.

7.2 Oracle Aconex and Conject Cloud Services

7.2.1 Change Management

Oracle Aconex Cloud Services

Oracle Aconex Cloud Services undergo scheduled maintenance every week. During this time the services are unavailable to users.

The regular maintenance windows listed below last for two hours. Oracle Aconex services teams will provide customer notifications 72 hours in advance of updates that require a maintenance window greater than 2 hours.

Not sure what your “instance” is? Click here for more information.

Note that the times given above reflect local time, whether or not daylight savings time is in effect.

Oracle Conject Cloud Services

Oracle Conject Cloud Services undergo scheduled maintenance regularly. The regular maintenance window starts every Saturday at 20:00 (Central European time) and lasts for 4 hours. During this time the services can be unavailable to users.

7.2.2 Support

The following features are not available until further notice:

- Chat services (Technical and Non-technical) are not provided
- Oracle Guided learning Starter Packs are not provided

7.2.3 Disaster Recovery

In the case where Your order states "Middle East", You acknowledge and agree that the disaster recovery Data Center Region may be Europe or Middle East.

7.2.4 Termination Policy

Termination of Oracle Aconex Cloud Services

This section replaces the 'Termination of Oracle Cloud Services' section or equivalent in the Oracle Cloud Hosting and Delivery Policy.

(a) For a period of at least 180 days from the expiry or termination of the applicable System Project on the Oracle Aconex Cloud Service or Your right to access the System Project ("Retrieval Period"), Oracle will upon Your request and subject to (i) You acquiring archive services through a separate order and the payment of any applicable fees or (ii) such request being made during the first 30 days of the Retrieval Period and only for that duration ("Initial Retrieval Period"), make available during the Retrieval Period (or the Initial Retrieval Period, as applicable), via secure protocols and in a structured, machine-readable format, Your Content (as it currently exists at the time of such access or retrieval) residing in the production Oracle Aconex Cloud Services environment for the applicable System Project(s), or make the service system for the applicable System Project(s) accessible, for the purpose of retrieval of the aforementioned data by You.

(b) Subject to section (f) below, following the expiry of the Retrieval Period, Oracle will delete Your Content from the Oracle Aconex Cloud Services environment(s) related to the applicable System Project unless (i) otherwise required by applicable law or (ii) if You or any entity other than You that participates in the System Project ("Participant") related to the System Project has a longer retention period or has a right for an archive service related to the System Project. Deletion will occur across all production instances and renders Your Content non-recoverable. Oracle may notify You within the Retrieval Period of the date for Your Content's deletion.

(c) Participants who are enabled to access or view Your Content may continue to access or view part or all of Your Content in the production Oracle Aconex Cloud Services environment for the applicable System Project(s) during the Retrieval Period.

(d) If during the Retrieval Period You need assistance from Oracle to obtain access to or copies of Your Content, You must create a service request in the Cloud Customer Support Portal applicable to Your Oracle Aconex Cloud Service (e.g. Aconex Support Central).

(e) Data retrieval and any related assistance by Oracle is not applicable for Oracle Cloud Services that do not store Your Content. You are responsible for ensuring that if those Oracle Cloud Services are dependent on separate Oracle Cloud Services (such as Storage Cloud Service or Database Cloud Services) for the storage of data, those separate Oracle Cloud Services must have a valid duration through the end of the terminating Oracle Cloud Service to enable data retrieval, or for otherwise taking appropriate action to back up or otherwise store separately Your Content while the production Cloud Services environment is still active prior to termination.

(f) Notwithstanding sections (a) and (b) above, Oracle will delete or render unrecoverable from the Global Directory Your User's data (including Personal Data) that You include in the Global Directory, provided that such User is (i) inactive on the Oracle Aconex Cloud Services for a continuous period of 12 months; and (ii) You are not a Participant in any active System Projects. Notwithstanding the prior sentence, Oracle reserves the right to delete or render unrecoverable Your Users' data (including Personal Data) from the Global Directory in the event all Your Users have not participated in any active System Projects within 90 days from Your registration on the Oracle Aconex Cloud Services. For the purposes of this section, the 'Global Directory' means the index of registered users on the Oracle Aconex Cloud Services that may be accessible to all users of the Oracle Aconex Cloud Service within the same data centre location.

Termination of Oracle Conject Cloud Services

This section replaces the 'Termination of Oracle Cloud Services' section or equivalent in the Oracle Cloud Hosting and Delivery Policy.

For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available, via secure protocols and in a structured, machine-readable format, Your Content (which may not include all content provided by parties which You have invited to access the Oracle Conject Cloud Service or Your environment) residing in the production Oracle Conject Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You. You should not use the environment for production activities.

If You need assistance from Oracle to obtain access to or copies of Your Content, You must create a service request in the Cloud Customer Support Portal applicable to the Your Oracle Conject Cloud Service (e.g. Aconex Support Central).

Data retrieval and any related assistance by Oracle is not applicable for Oracle Cloud Services that do not store Your Content. You are responsible for ensuring that if those Oracle Cloud Services are dependent on separate Oracle Cloud Services (such as Storage Cloud Service or Database Cloud Services) for the storage of data, those separate Oracle Cloud Services must have a valid duration through the end of the terminating Oracle Cloud Service to enable data retrieval, or for otherwise taking appropriate action to back up or otherwise store separately Your Content while the Production Cloud Services environment is still active prior to termination.

Following expiry of the retrieval period, Oracle will delete or render unrecoverable Your Content from all production Oracle Cloud Services environments (unless otherwise required by applicable law).

7.3 Oracle Preconstruction Bid Management Cloud Services

7.3.1 Termination of Oracle Cloud Services

This section replaces the 'Termination of Oracle Cloud Services' section or equivalent in the Oracle Cloud Hosting and Delivery Policy in relation to Oracle Preconstruction Cloud Services.

a. Oracle Preconstruction Bid Management General Contractor Cloud Service – Hosted Named User

For a period of 60 days upon termination of Your Oracle Preconstruction Cloud Services, Oracle will make available upon Your request, via secure protocols and in a structured, machine-readable format, Your Content residing in the production Oracle Preconstruction Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You. You should not use the environment for production activities. For clarity, some of Your Content may only be retrieved during the retrieval period by print to PDF, with the exception of Your Content in the Global Directory, which can only be retrieved manually by accessing the Global Directory during Your retrieval period.

If You need assistance from Oracle to obtain access to or obtain copies of Your Content during the retrieval period, You must create a service request in the Cloud Customer Support Portal applicable to the Your Oracle Preconstruction Cloud Services (e.g. Oracle Service Cloud).

Following expiry of the retrieval period, Oracle will delete or render unrecoverable Your Content from all production Oracle Preconstruction Cloud Services environments (unless otherwise required by applicable law or Your Content relates to Project Data that You submitted or received from another General Contractor in relation to that General Contractor's Bid Package). You acknowledge that Your Content (including any Project Data) once deleted cannot be retrieved by You and Oracle shall not be liable to You or any other party for any such deletion.

b. Oracle Preconstruction Bid Management Subcontractor Premium Cloud Service – Customer (also known as **'Premium Subcontractor - Preconstruction Bid Management'**)

Upon termination of Your Oracle Preconstruction Cloud Services, Your subscription will revert to the Basic Subcontractor - Preconstruction Bid Management cloud service and the terms and conditions related to such cloud service will apply. Please refer to the Basic Subcontractor - Preconstruction Bid Management section below in relation to the deletion policy applicable to such service.

If upon the termination of the Premium Subcontractor - Preconstruction Bid Management cloud service, You do not wish to revert to the Basic Subcontractor - Preconstruction Bid Management cloud service, for a period of 60 days upon such termination of the Premium Subcontractor - Preconstruction Bid Management cloud service, Oracle will make available upon Your request, via secure protocols and in a structured, machine-readable format, Your Content residing in the production Oracle Preconstruction Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You. You should not use the environment for production activities. For clarity, some of Your Content may only be retrieved during the retrieval period by print to PDF with the exception of Your Content in the Global Directory, which can only be retrieved manually by accessing the Global Directory during Your retrieval period. If You need assistance from Oracle to obtain access to or obtain copies of Your Content during the retrieval period, You must create a service request in the Cloud Customer Support Portal applicable to the Your Oracle Preconstruction Cloud Services (e.g. Oracle Service Cloud).

Following expiry of the above retrieval period, Oracle will delete or render unrecoverable Your Content from all production Oracle Preconstruction Cloud Services environments (except Project Data submitted to General Contractors or otherwise required by law).

Project Data will be deleted in accordance with the deletion policy and terms related to the applicable General Contractor's Your Content. Oracle is under no obligation to notify You prior to the deletion of Your Content within the Project Data. You acknowledge and agree that Project Data once deleted cannot be retrieved by You and Oracle shall not be liable to You for any such deletion by Oracle or the applicable General Contractor.

c. Oracle Preconstruction Bid Management Subcontractor Basic Cloud Service – Customer (Free) (also known as **'Basic Subcontractor - Preconstruction Bid Management'**)

After termination of Your Basic Subcontractor - Preconstruction Bid Management cloud service, for a period of 60 days, Oracle will make available upon Your request, via secure protocols and in a structured, machine-readable format, Your Content residing in the production Oracle Preconstruction Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You. You should not use the environment for production activities For clarity, some of Your Content may only be retrieved during the retrieval period by print to PDF with the exception of Your Content in the Global Directory, which can only be retrieved manually by accessing the Global Directory during Your retrieval period. If You need assistance from Oracle to obtain access to or obtain copies of Your Content during the retrieval period, You must create a service request in the Cloud Customer Support Portal applicable to the Your Oracle Preconstruction Cloud Services (e.g. Oracle Service Cloud).

Following expiry of the retrieval period, Oracle will delete or render unrecoverable Your Content from all production Oracle Preconstruction Cloud Services environments (except Project Data submitted to General Contractors or otherwise required by law).

Project Data will be deleted in accordance with the deletion policy related to the applicable General Contractor's Your Content. Oracle is under no obligation to notify You prior to the deletion of Your Content within the Project Data. You acknowledge and agree that Project Data once deleted cannot be retrieved by You and Oracle shall not be liable to You for any such deletion by Oracle or the applicable General Contractor.

7.3.2 Data Center Region

The order designates the Data Center Region for the Services. Your User login details may be hosted in the North America Data Center Region.

7.4 Primavera Cloud Services and Construction Intelligence Cloud Services

This section applies to Primavera Cloud and Construction Intelligence Cloud Services.

7.4.1 Data Center Region

For Primavera Cloud Services and Construction Intelligence Cloud Services where Your order states “Europe-United Kingdom”, You acknowledge and agree that Your User login details may be hosted in either the Europe-United Kingdom or Europe Data Center Region.

8 ORACLE HEALTH SCIENCES CLOUD SERVICES

8.1 Termination of Oracle Cloud Services and Pilot Environments

This section supplements the ‘Oracle Cloud Suspension and Termination Policy’ section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle Health Sciences Cloud Services.

Non-Production instances, modes, or environments of the Cloud Services, such as those for development, testing, training, or non-production pilots (“Non-Production Environments”) are not intended for production data. Upon termination of the Cloud Services, Your Content residing in Non-Production Environments will be deleted or otherwise render inaccessible and will not be available for retrieval.

8.2 Application Upgrades or Updates and Data Center Migrations

During application upgrades, updates, or data center migrations of certain Cloud Services, Oracle may be required to reconfigure and test applications or customizations, which may be subject to additional fees.

8.3 Oracle Health Sciences Argus Cloud Services

Oracle Argus Cloud Services Disaster Recovery testing follows a standard approach to testing the restoration of the production environment in a disaster recovery data center. Disaster Recovery testing uses a standard, pre-defined infrastructure assembly and standardized processes for the backup and restoration of the production environment and production data, achieving published RTOs and RPOs. The standard assembly and processes followed in the disaster recovery test plan are equivalent to the assemblies and provisioning and configuration processes used for deploying customer environments.

8.4 Oracle Health Sciences Site Select, Site Activate, and Site Analyze Cloud Services

8.4.1 Change Management

Application Upgrades

Single Tenant Applications

For upgrade of applications dedicated to the customer such as Site Activate, Oracle will work with the customer to identify a mutually agreed upon date and time when the upgrade will take place. This applies to Production and non-Production environments. Note: Upgrades may require downtime to the environment.

Multi-Tenant Applications

For upgrades to applications that are shared by multiple customers, Oracle will inform the customers the date and time when their environment will be upgraded. Notice will be provided at least five (5) business days in advance. This applies to Production and non-Production environments. Note: Upgrades may require downtime to the environment.

System Maintenance

The Oracle maintenance window is the 1st and 3rd Saturday of each month, 8:00 -11:00 PM Pacific US time. This window is used to do any system and infrastructure maintenance tasks like OS upgrades, applying security patches, database maintenance, etc.

8.4.2 Secure File Transfer Protocol (SFTP) Password Policy

For the purposes of file transfers of customer data, accounts in the Oracle SFTP server will be provisioned, upon submission of a ticket or service request, for customers to upload and download files to that sftp server. Such accounts are not intended for individual access, but rather for system integration to customer software instances. The credentials for accessing the sftp server will be sent via email to the customer's designated point of contact. The password for the sftp server will be at least 8 characters long with at least one of each of the following:

- lower case alphabet
- upper case alphabet
- number
- special character

When passwords are changed by Oracle, the change will be communicated to the customer in advance via email notification. When a customer requests the password to be changed, Oracle will communicate the new password, and date and time it will be changed, to the customer. Sftp accounts will be removed as part of the service termination or upon customer request.

In limited situations, Oracle will use the customer's sftp server. In such cases, the customer will communicate and manage the password policy and share it with Oracle. Changes to passwords will be communicated to Oracle in advance.

8.5 Oracle Health Science Clinical One Cloud Service - Access Management

8.5.1 Severity Levels

For the purpose of the Oracle Health Science Clinical One Cloud Service - Access Management Services, the Severity Definitions section and the Change to Service Request Severity Level section of the Oracle Cloud Hosting and Delivery Policies do not apply.

8.5.2 Hours and Languages

For the purpose of the Oracle Health Science Clinical One Cloud Service - Access Management Services, the Service Description takes precedence over anything to the contrary in the Oracle Cloud Hosting and Delivery Policies.

Phone support for the Access Management Services is available in the languages and during the hours specified in the Service Description.

9 NOR1 CLOUD SERVICES

9.1 Change Management

The Engineering team estimates the downtime for the upgrade or change and coordinates with the Account Management team to schedule a maintenance window. Maintenance windows are typically scheduled during off-peak hours, between 11pm and 2am Pacific. Hotel customers will be notified of the upcoming maintenance window by email and chat. Email distribution list is based on customer contacts in our database. Chat notifications pop-up when a hotel user signs into the Nor1 Hotel Portal.

10 ORACLE FOOD AND BEVERAGE CLOUD SERVICES

10.1 Oracle Food and Beverage Cloud Services

Oracle Food and Beverage Cloud Services (“FBGBU Cloud Services”) consist of the Cloud Services in the following Service Descriptions:

- Oracle Hospitality Food and Beverage Cloud Services—Service Descriptions and Metrics
- Oracle MICROS Food and Beverage Cloud Services—Service Descriptions and Metrics
- Oracle MICROS Payment Cloud Service - Service Descriptions

10.2 Oracle Food and Beverage Cloud Services Disaster Recovery

Notwithstanding anything to the contrary in this Section 3, for Oracle Food and Beverage Cloud Services, the following disaster recovery policy applies:

In the event of a declared disaster, Oracle may recover and restore the production environment of the affected FBGBU Cloud Service and work to restore production data using a recent backup made prior to the onset of the disaster. Oracle may elect to restore the production environment in an alternate, available data center of Oracle's choice. When using a backup for recovery and restoration of the production environment and production data, published RTOs and RPOs, if any, will not apply.

10.3 Oracle Food and Beverage Cloud Support Policy

For FBGBU Cloud Services, the following applies in lieu of the text in Section 5.1.3 of the Oracle Cloud Hosting and Delivery Policies:

- First Line Support: You are required to establish and maintain the organization and processes to provide "First Line Support" for the supported Cloud Services directly to your users. First Line Support shall include but not be limited to (i) a direct response to users with respect to inquiries concerning the performance, functionality or operation of the supported Cloud Services, (ii) a direct response to users with respect to problems or issues with the supported Cloud Services, (iii) a diagnosis of problems or issues of the supported Cloud Services, and (iv) a resolution of problems or issues of the supported Cloud Services.

For FBGBU Cloud Services, the following applies in lieu of the text in Section 5.3 of the Oracle Cloud Hosting and Delivery Policies

- Reasonable efforts will be made to respond to service requests per the Response Time Goals set forth in the guidelines below; however, Oracle's failure to adhere to the times stated will not constitute a breach by Oracle. The guidelines are for informational purposes only and subject to change at Oracle's discretion.

Severity Level	Response Time Goal	Update or Resolution Goal
Severity 1	5 minutes	1 hour
Severity 2	2 hours	6 hours
Severity 3	8 hours	24 hours
Severity 4	24 hours	48 hours

For purposes of the above table, the following definitions apply:

- **Severity 1:** Major system disruption (e.g., a major disruption in business-critical system operability or functionality, server crash or total system failure)
- **Severity 2:** Severe system disruption (e.g., A severe disruption in business-critical functionality that does not impact the entire system such as: significant number of workstations/terminals unable to perform or post transactions, loss of ability to perform payment functions, total Loss of reporting (local or hosted), loss of all printing, failure to reset totals or complete EOD/SOD/Night Audit, reposting for a given date or range of date, very slow page or image loading, or inaccessible tools interface
- **Severity 3:** Single function failure (e.g., a minor disruption in operability or functionality that does not impact the entire system such as: timekeeping issues, isolated printing failure, isolated workstation/terminal failure, failure to view a single report, password resets, or non-functional loyalty programs)
- **Severity 4:** Minor/Procedural issue or question (e.g., programming or configuration related questions, questions relating to functionality, operability, or formatting or cosmetic problems)

11 ORACLE HOSPITALITY CLOUD SERVICES

11.1 Oracle Hospitality Cloud Services

Oracle Hospitality Cloud Services (“Hospitality Cloud Services”) consist of the Cloud Services in the following Service Descriptions:

- Oracle Hospitality Hotel Cloud Services—Service Descriptions and Metrics

11.2 Oracle Hospitality Cloud Services Disaster Recovery

Notwithstanding anything to the contrary in this Section 3, for Oracle Hospitality Cloud Services, the following disaster recovery policy applies:

In the event of a declared disaster, Oracle may recover and restore the production environment of the affected Hospitality Cloud Service and work to restore production data using a recent backup made prior to the onset of the disaster. Oracle may elect to restore the production environment in an alternate, available data center of Oracle's choice. When using a backup for recovery and restoration of the production environment and production data, published RTOs and RPOs, if any, will not apply.

11.3 Oracle Hospitality Cloud Support Policy

For Oracle Hospitality Cloud, the following applies in lieu of the text in Section 5.1.3 of the Oracle Cloud Hosting and Delivery Policies:

- First Line Support: You are required to establish and maintain the organization and processes to provide “First Line Support” for the supported Cloud Services directly to your users. First Line Support shall include but not be limited to (i) a direct response to users with respect to inquiries concerning the performance, functionality or operation of the supported Cloud Services, (ii) a direct response to users with respect to problems or issues with the supported Cloud Services, (iii) a diagnosis of problems or issues of the supported Cloud Services, and (iv) a resolution of problems or issues of the supported Cloud Services.

For Oracle Hospitality Cloud, the following applies in lieu of the text in Section 5.3 of the Oracle Cloud Hosting and Delivery Policies

- Reasonable efforts will be made to respond to service requests per the Response Time Goals set forth in the guidelines below; however, Oracle’s failure to adhere to the times stated will not constitute a breach by Oracle. The guidelines are for informational purposes only and subject to change at Oracle’s discretion.

Severity Level	Response Time Goal	Update or Resolution Goal
Severity 1	5 minutes	1 hour
Severity 2	2 hours	6 hours
Severity 3	8 hours	24 hours
Severity 4	24 hours	48 hours

For purposes of the above table, the following definitions apply:

- **Severity 1:** Major system disruption (e.g., a major disruption in business-critical system operability or functionality, server crash or total system failure)
- **Severity 2:** Severe system disruption (e.g., A severe disruption in business-critical functionality that does not impact the entire system such as: significant number of workstations/terminals unable to perform or post transactions, loss of ability to perform payment functions, total Loss of reporting (local or hosted), loss of all printing, failure to reset totals or complete EOD/SOD/Night Audit, reposting for a given date or range of date, very slow page or image loading, or inaccessible tools interface
- **Severity 3:** Single function failure (e.g., a minor disruption in operability or functionality that does not impact the entire system such as: timekeeping issues, isolated printing failure, isolated workstation/terminal failure, failure to view a single report, password resets, or non-functional loyalty programs)
- **Severity 4:** Minor/Procedural issue or question (e.g., programming or configuration related questions, questions relating to functionality, operability, or formatting or cosmetic problems)

12 ORACLE NETSUITE FOR GOVERNMENT CLOUD SERVICE

12.1 System Access Controls

This section replaces the ‘1.3 System Access Controls’ section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

All remote access to the Oracle Cloud Network by Oracle personnel that have access to Your Content must be through one or more of the following: virtual private network, multi-factor authentication, mutual authentication, client trust scoring, machine identity verification, or other authentication methods with an equal or higher level of security. Oracle prohibits (through both policy and technical controls) the use of personal devices to access the Services environment for the Cloud Services. The controls described in this section are limited to access by Oracle personnel.

For Cloud Services hosted at Oracle: (i) log-ins to Cloud Services environments are logged and (ii) logical access to the data centers is restricted and protected.

12.2 Data Access Controls

This section supplements the ‘1.4 Data Access Controls’ section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

Oracle will act as though any electronic communications it receives under Your passwords, user name, and/or account number will have been sent by You. You shall use commercially reasonable efforts to prevent unauthorized access to or use of the Cloud Service and shall promptly notify Oracle of any unauthorized access or use of the Cloud Service and any loss or theft or unauthorized use of any User’s password or name and/or Cloud Service account numbers.

Oracle may access the Cloud Service to install and provide upgrades and patches for Oracle NetSuite for Government Cloud Service, monitor Oracle NetSuite for Government Cloud Service for performance, and to maintain the SuiteApp component of Oracle NetSuite for Government Cloud Service. You may not modify or revoke Oracle’s access to the Cloud Service which is required for Oracle to administer Oracle NetSuite for Government Cloud Service provisioned pursuant to Your order. Oracle’s access to the Cloud Service will be consistent with the terms of Oracle’s Hosting and Delivery Policies and this Oracle Global Business Unit Cloud Services – Pillar Document.

12.3 User Encryption for External Connections

This section supplements the ‘1.5 User Encryption for External Connections’ section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

In some cases, a third-party site that You wish to integrate with the Oracle Cloud Services, such as a social media service or a local government tax filing service, may not accept an encrypted connection or does not support up-to-date secure ciphers and protocols. Oracle will attempt to negotiate connections using the most secure protocols and ciphers supported by the target system. Where Your business requires You to communicate with a third-party service or application that does not accept an encrypted connection or does not support up-to-date ciphers and protocols, You agree to not hold Oracle responsible for any unauthorized data compromise or disclosures resulting from Your use of such integrations.

Without limiting Oracle's applicable security or confidentiality obligations under this section, Oracle will also not be responsible for any delay, loss, alteration, or interception during the transmission of any data across networks not owned and/or operated by Oracle, including, but not limited to, the Internet and Your local network.

12.4 Other Customer Security Related Obligations

This section supplements the ‘1.15 Other Customer Security Related Obligations’ section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

In managing client device security controls, You are also responsible for using encryption protocols and cipher suites for secure communications and connecting from secure client networks.

In addition, You will ensure that Your access and integrations to the Cloud Service meet, at a minimum, the changing requirements set forth by Oracle as provided to You via the support portal, User Guides, or other knowledge base for the Cloud Service, as the industry's security landscape evolves.

Oracle will not be liable for any service disruption or unauthorized disclosure, modification, or loss of Your Content caused by non-compliance with Oracle's requirements for access to or integrations with the Cloud Service.

12.5 Backup Strategy

This section supplements the '2.2 Oracle Cloud Services Backup Strategy' section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

A backup is typically retained online or offline for a period of at least 30 days after the date that the backup is made.

If assistance is required from Oracle to restore data lost through Your own actions, additional fees may apply.

12.6 Service Availability

This section replaces sections '3.2 Service Availability' and all of its subsections or equivalent in their entirety and '3.3 Definition of Unplanned Downtime' or equivalent in the Oracle Cloud Hosting and Delivery Policies and section "1 Oracle Cloud Service Level Agreement" and its subsections of this document in their entirety in relation to Oracle NetSuite for Government Cloud Service.

Please refer to the "Service Level Commitment" located at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html, or such other URL as specified by Oracle.

12.7 Customer Monitoring & Testing Tools

This section supplements the '3.4.2 Customer Monitoring & Testing Tools' section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

You may not, and may not cause or permit others to, perform any stress test, test of load failure, or load testing without prior written approval from Oracle.

The following statement does not apply to the Cloud Service: "The Oracle Cloud Services Program Documentation outlines when and how You may assess or test any components that You manage or create in

Oracle Cloud Services, including non-Oracle applications, non-Oracle databases, other applicable non-Oracle software, code, or the use of data scraping tools."

12.8 Emergency Maintenance

This section supplements the '4.1.1 Emergency Maintenance' section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

Please refer to the "Service Level Commitment" located at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html, or such other URL as specified by Oracle for additional information on Scheduled and Unscheduled Maintenance in relation to Oracle NetSuite for Government Cloud Service.

12.9 Major Maintenance Changes

This section replaces the '4.1.2 Major Maintenance Changes' section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

Please refer to the "Service Level Commitment" located at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html, or such other URL as specified by Oracle for applicable information on scheduled and unscheduled maintenance.

12.10 Termination Policy

This section replaces the '6.1 Termination of Oracle Cloud Services' section or equivalent in the Oracle Cloud Hosting and Delivery Policies in relation to Oracle NetSuite for Government Cloud Service.

You are responsible for taking appropriate actions to back up or otherwise store separately Your Content while Your access to the production Cloud Services environment is still active prior to termination. If You require account reactivation or other assistance from Oracle in retrieving Your Content post termination or to obtain access to or copies of Your Content, You must create a service request or a support case in the Cloud Customer Support Portal applicable to the Cloud Service. The availability of any such assistance is subject to the terms of this section and additional fees may apply.

For a period of 60 days upon termination of the Cloud Services (the "Retrieval Period"), upon Your request, Oracle may make available via secure protocols Your Content residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You. During this Retrieval Period, Oracle's Cloud Service Level Objective Policy or the Cloud Service's Service Level Commitment do not apply, and the Cloud Service may not be used for any production activities. Oracle has no obligation to retain Your Content after this Retrieval Period.

Upon termination of the Cloud Services, Your Content residing in the production Cloud Services environments is retained in disabled or inactive status during the Retrieval Period. Upon expiry of the Retrieval Period, any remaining access to Your Content and the Cloud Services are revoked, and Your Content is queued for deletion. Within ten (10) months following the expiration of the Retrieval Period, and except as may be required by law, Oracle will delete or render inaccessible Your Content in the production Cloud Services environments maintained by Oracle in providing the Cloud Services procured on Your order.

12.11 Change Management Policy

This section replaces sections '2.1 Application Upgrades and Updates' and '2.3 Core System Maintenance' of this document in relation to Oracle NetSuite for Government Cloud Service.

Please refer to the "Service Level Commitment" located at https://www.oracle.com/corporate/contracts/cloud-services/netsuite/contracts.html, or such other URL as specified by Oracle for information on Scheduled and Unscheduled Maintenance.

12.12 Disaster Recovery

This section replaces the third and fourth paragraphs of '3.1 Disaster Recovery' section of this document in relation to Oracle NetSuite for Government Cloud Service.

Upon Oracle's declaration of a disaster, Oracle will activate processes to recover the production environment of the affected Cloud Service from the most recent available backup made prior to the onset of the disaster. Although Oracle will work to recover the Cloud Service promptly, the nature of the disaster may affect the time period within which the Cloud Service can be recovered. Recovery Time Objective and Recovery Point Objective are not applicable for this Cloud Service.