CEBOS CLOUD PROGRAM DOCUMENT

This CEBOS Cloud Program Document establishes terms and conditions for Cloud Services ordered by Customer and provided by Vendor under an Order Document executed under a Cloud Services Agreement. Terms not otherwise defined herein shall have the meanings set forth in the Cloud Services Agreement.

Cloud Services

General Terms	
Subscription Terms	Upon Vendor's acceptance of Customer's order under an Order Document Vendor shall make the Cloud Applications available to Customer on a subscription basis and provide the other Cloud Services as described herein. Customer's usage of the Cloud Applications shall be limited to the subscription levels set forth in the Order Document. Customer shall not acquire any further rights in or to the Cloud Applications and Customer's right to access to the Cloud Applications shall cease upon termination of the Order Document. Customer shall not be provided with a copy of the Cloud Applications. Customer's subscription to the Cloud Applications is governed by the bundle definitions and metrics and related terms set forth in the Software and Cloud Services Terms posted at http://www.qad.com/legal.html and incorporated herein. The terms set forth in the Software Terms shall apply only to the extent applicable to the specific Cloud Applications subscribed for by Customer. Subsequent changes to these terms by Vendor shall not apply retroactively to Customer except as agreed by Customer. Customer's use of the Cloud Applications shall be subject to the following restrictions. Customer shall: • only use the Cloud Applications for its own business purposes. • restrict usage of the Cloud Applications to the purchased subscription levels. • use unique logon IDs for individuals, devices and processes (i.e. logon IDs shall not be shared). • not use any method, software or technology which hides or understates the actual number of users accessing the Cloud Applications (e.g. by circumventing the Cloud Applications log-on process). • not provide access to the Cloud Applications to third parties, except as explicitly permitted herein. • not use the Cloud Applications for timesharing, rental or service bureau purposes. Customer may permit a third party to access the Cloud Applications only if such third party forms part of the Customer's supply chain (i.e. the third party is a supplier or a customer of the Customer) and provided that such access is limited to the benefit of Customer. Customer shall be responsible for compliance with the terms of this Agreement by any third party granted access to the Cloud Applications by Customer.
Version Management	At the commencement of the Cloud Services the latest generally-available versions of the Cloud Applications shall be deployed unless otherwise agreed. Thereafter, Vendor shall in its discretion apply new versions, bug fixes, service packs and other updates in accordance with Vendor's standard operating procedures, provided, however, that (1) Vendor shall give reasonable advance notice and obtain Customer's consent prior to applying any such

	update; and (2) Customer may withhold consent if Customer reasonably believes that applying such update shall cause material disruption to Customer's business. In the event Customer withholds consent then Vendor shall not be responsible for any changes in software or system performance resulting from not applying such update. Notwithstanding the foregoing, Vendor may immediately shut down all environments if Customer withholds consent to an update and the absence of such update causes, in Vendor's reasonable opinion, material risk to the security of Vendor's systems.
Environments	As part of the Cloud Services, Vendor will provide one production environment and, on request, up to two non-production environments. Vendor may provide additional environments for additional fees. The service levels outlined in this Program Document apply to the production environment only (i.e. only to the environment that contains Customer's live data).
Environment availability commitment	Vendor warrants the availability of the production environment for 99.5% (ninety nine and five tenths percent) of the Scheduled Hours of Operation during Go-Live status, as set forth in the "Measuring availability" section below. This availability commitment does not apply to either Build status or Transition status. Environment availability statuses are defined as follows: • Build – the initial status, during which the environment is being built prior to release to Customer. • Transition – after the completion of the Build status, during which the environment is configured prior to Go-Live. • Go-Live – the status following the first production use of the environment per the scheduled Go-Live date mutually agreed by Vendor and Customer.
Scheduled Hours of Operation	The Scheduled Hours of Operation are defined as 24/7 (Monday through Sunday during 24 hours each day), minus Planned Maintenance Windows. A Planned Maintenance Window is a period during which the Cloud Services will be unavailable, downtime not to exceed eight (8) hours. Planned Maintenance Windows shall be announced in advance to Customer, the exact times to be agreed by parties and documented in writing. Information on Planned Maintenance Windows is available within the Customer's online collaborative share location or will be communicated in writing (by email or otherwise).
Measuring availability	Unavailability of the production environment is measured over a calendar month and is based on total outage time incurred by the Customer. Environment unavailability will exist when either (1) the environment is unable to transmit Internet Protocol data packets to the Vendor designated point of presence; or (2) the Cloud Applications are unavailable as measured by the key application component services determined by Vendor and tracked in reports available from Vendor. Environment unavailability is measured until the time Vendor determines that the affected service is again able to transmit and receive data and the Cloud Applications are again available. Vendor's commitment regarding Cloud Applications availability is conditioned on (A) the Cloud Applications must be within the General Availability, Functionally Stable or Mature phases under the Vendor Product Life Cycle Policy; and (B) the Cloud Applications must be deployed per the Vendor standard reference architecture. Customers are responsible for the connection between their sites (and users) and the Vendor data center. The Cloud Services rely on an Internet Protocol connection. If the connection is slowed or becomes unavailable, the Cloud Applications may become unresponsive or unusable. Inadequate performance by network connections and/or computer infrastructure not under Vendor's control is not covered by Vendor's environment availability commitment.

Service credits and conditions	If Vendor fails to meet this environment availability commitment for any calendar month and Customer provides Vendor with a written request within thirty (30) days of the last day of the month in which such failure occurred, Vendor will provide a service credit to Customer's account that may be applied against subsequent invoices equal to the fee for one (1) day of Cloud Services (excluding taxes, pass-through charges, credits, installation or other one-time charges) for each cumulative hour of unavailability or failure during the applicable month, exceeding 0.5% (five tenths of one percent) of the time, up to a maximum of the total Cloud Services fees charged by Vendor to Customer for such month. Service credits will not be available to Customer in cases where the environment is unavailable as a result of (a) the acts or omissions of Customer or its employees, contractors, agents or end-users; (b) the failure, malfunction, or limitation of throughput of equipment, network, software, applications or systems (including web services, ODBC and ftp locations) not owned or directly controlled by Vendor; (c) circumstances or causes beyond the control of Vendor, including, without limitation, events of force majeure and third-party attacks on the environment (such as ping and denial of service attacks); or (d) scheduled outages such as outages during Planned Maintenance Windows. Such credits will be granted only if Customer provides Vendor with all requested information in an expeditious manner and affords Vendor full cooperation to make necessary repairs, maintenance, testing, etc. THIS SECTION SETS FORTH CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR SERVICE INTERRUPTIONS, SERVICE RESPONSE ISSUES AND/OR SERVICE DEFICIENCIES OF ANY KIND WHATSOEVER.
Disk Space	Vendor shall provide sufficient space such that the production environment shall consist of 125 Gb of total available space for applications and data storage, and further, of the total 125 Gb the IIS server shall be allocated 55 Gb and the SQL server shall be allocated 70 Gb.
Backup	• Data to be backed up: all installed Vendor Application and database associated with the production environment. • Backup Schedule: incremental backup daily; full backup weekly. • Backup Storage: daily and weekly backups are replicated to off-site digital storage. • Backup Retention Schedule: incremental backups are retained for 3 weeks then are overwritten. Full backups are retained for 4 weeks. • Restoring Files: Customer may request restoration of data by opening a Vendor support ticket. Restore will be performed to the environment specified by the customer.
Environment and database refreshes	On Customer's request, Vendor shall refresh each of the test and development environments once per calendar month. On Customer's request, Vendor shall refresh the database twice per calendar month.
Disaster Recovery	<u>Vendor responsibilities</u> • A "Disaster" is defined as an unrecoverable event at the Vendor data center or Vendor network provider that causes the Customer's production environment at the primary site to be unavailable for eight (8) hours or more. • Vendor shall make the determination of when and if a Disaster has occurred. If an event or failure causes unavailability that Vendor determines will continue eight (8) hours or more, then Vendor shall declare a Disaster immediately. • Although the technical setup is designed for immediate up-time in case of a Disaster, Vendor will provide a Recovery Time Objective (RTO) of eight (8) hours after a Disaster has been declared by Vendor at the main hosting facility.

	• Although the technical setup is designed for zero data loss, Vendor will provide a Recovery Point Objective (RPO) of one (1) hour from when the unavailability initially occurred. • This service covers only the production environment. • Non production environments will be suspended when disaster recovery is enacted. <u>Customer responsibilities</u> • Customer must have an operational disaster recovery plan in place prior to implementation. • Customer must commit to review the disaster recovery plan every six months. • Customer must commit to test the disaster recovery plan annually (the Disaster Recovery Offering includes two person days Vendor assistance with testing). • The Customer will be responsible for the connectivity to the Vendor designated point of presence for the disaster recovery center, including network rerouting in the event of a Disaster. • Customer will be responsible for reconfiguring client configurations for connection the Vendor designated point of presence for the disaster recovery center. • A planned outage will be required to revert to the main hosting facility once the cause of the Disaster has been resolved. • Customer will be responsible for enabling and managing any third-party interfaces or third-party products in the event of a Disaster.
Role of Vendor Engagement Manager	• Provides initial orientation session with customer, reviewing Cloud practices and policies. • Acts as primary contact for Cloud service delivery.

Support for Environment Infrastructure

The following support service levels pertain only to the environment infrastructure described above. Service levels pertaining to the operation of the Cloud Applications are set forth in Vendor's Customer Support Guide.

Vendor will respond to Customer's request for support upon receipt of Customer's incident report. When Vendor receives the incident report, Vendor's support contact will respond to the designated person making the report. Response time goals for the various severity levels are outlined below along with resolution goal targets. These resolution goals are only set as targets to measure quality and provide continuous improvement metrics. Customer shall identify to Vendor up to three (3) individuals who are authorized to submit incident reports. Such individuals shall serve as the point of contact for the incident reports.

Severity level	Description	Vendor Response Goal	Vendor Resolution Goal
0	Highest priority available for cases. Business critical (down system or Cloud Applications not available to more than 1 user) condition in a production environment. No "work around" exists. Requires immediate solution.	Direct connection to support personnel or a response within 30 minutes.	8 hours from time call is answered. Resolution is understood as being provided with a work-around or a permanent solution that eliminates the business critical condition, with 90% of tickets resolved.

1	Critically impacts the customer's business operation. Production is operational (i.e. access to Cloud Applications is possible) or a "work around" exists, but severely restricting production.	2 Hours	2 days from time call is answered. Resolution is understood as being provided with a work-around or a permanent solution that eliminates the condition, with 90% of tickets resolved.
2	General product questions regarding the Cloud Applications. Production or non-production environments.	4 Hours	5 days Resolution is understood as being provided with a work-around or a permanent solution that eliminates the condition, with 80% of tickets resolved.
3	Informational or environment related questions about the Cloud Applications, and / or change requests. Production or non-production environments.	8 Hours	15 days Resolution is understood as being provided with a work-around or a permanent solution that eliminates the condition, with 80% of tickets resolved.

Standard Support Hours

Definition:	"Standard Support hours" are Monday through Friday, from 8:00 AM to 5:00 PM, public holidays excluded, local time zone for the Vendor support center.
Off Hours Support	Off hours support hours are provided to handle severity 0 cases. Issues of lower severity are deferred to the beginning of the following business day for follow-up. Vendor will make all reasonable efforts to respond to "Off Hours" support calls in the same response time as defined for normal and customary daily operations.

Security Procedures

Vendor shall be responsible for establishing and maintaining an information security program related to securing and protecting Customer's data and Customer's customers' data (collectively "Data") that is designed to: (i) ensure the security and confidentiality of the Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Data; (iii) protect against unauthorized access to or use of Data; (iv) ensure the proper disposal of Data; and, (v) ensure that all contractors / subcontractors of Vendor, if any, comply with all of the foregoing.

In addition to the above, and more specifically, Vendor shall meet or exceed industry accepted standards to comply with the following:

A. Personnel Security

1. Vendor shall perform background checks on all applicable employees prior to employment.

2. Vendor shall remove employee and contractor access rights from Vendor's systems, servers, and networks utilized in the performance of its obligations under this Agreement within twenty-four (24) hours of the termination effective date.

3. Vendor shall maintain a list of users with access to Customer's systems, and will provide a copy of this list to Customer upon request. Vendor shall notify Customer within a reasonable timeframe when a user no longer requires access, so that Customer may disable their access to Customer's systems.

4. Vendor shall provide security awareness training to its employees at least annually.

B. Physical and Environmental Security

1. Vendor shall have and implement access control policies and procedures for its facilities and data centers.

2. Vendor's data centers used in the Vendor's performance under this Agreement shall be equipped and configured to assure continuous operation. These data centers shall employ, at a minimum, uninterrupted power supply, redundant backup generators, smoke and heat alarm systems, water sensors, fire suppression systems, air conditioning and humidity controls, and monitoring.

C. Disaster Recovery/Business Continuity

1. Vendor shall have detailed and documented plans for responding to a disaster, emergency situation, or other unforeseen circumstances that include processes and procedures for resumption of business operations, which shall be tested and reviewed, at least annually.

D. Technical Controls

1. Access Controls

Vendor shall implement access controls that include the following:

a) Access that is authorized, unique for each user, authenticated, and assigned with least and minimum necessary privileges, current, and includes inactive time session timeout (at the application level) not to exceed 30 minutes.
b) Password controls with industry standard password strength and complexity, expiration and history, removal of vendor supplied passwords, and account lockout.
c) Logical or physical controls to segregate Customer's Data from data from Vendor's other customers.

2. Remote Access

a) Vendor shall control access from external sources by using password authentication.
b) Vendor shall follow Customer's remote access procedures when accessing Customer's network. Procedures include but are not limited to the execution of access agreements for each individual requiring access.

3. Network / Security Management

a) Firewall/router filtering - Vendor shall maintain a network environment that utilizes firewalls to protect all ingress and egress points. Vendor shall house all public or internet facing applications in a DMZ that separates the publicly facing servers from the internal network.

b) Protection against Malicious Code – Vendor shall implement automated tools to detect, prevent, remove and remedy malicious code on desktops, servers, e-mail and internet access. Servers shall be updated with security patches based on industry accepted standards and criticality. Vendor shall use supported versions of operating systems for which patches are actively deployed.

c) IDS / IPS – Vendor shall utilize intrusion detection/intrusion prevention (IDS / IPS) systems to monitor activity that occurs across the network, as the parties may agree pursuant to a separate services engagement.

d) Wireless technology - Vendor shall implement a standard at least as stringent as 802.11i, when utilizing wireless technology to transmit Data or to access systems or Data.

4. System Hardening

a) Vendor shall implement policies and technical standards to harden operating systems, networks, databases, and web services.

5. Logging

a) Vendor's systems, networks and applications shall maintain audit logs of key events as agreed by the parties (for example, logon attempts, account lockout, account administration and password resets),

and retain such logs for 30 days.

b) Vendor shall implement policies and procedures for monitoring security logs on a regular basis.

6. Software Development Life Cycle (SDLC)

a) Vendor shall follow a documented SDLC process that covers software design, development, and improvement. The development/test and production environments shall be physically separated. All development and testing must be performed in a development / test environment. Sensitive production Data shall not be used for testing purposes, unless de-identified.

7. Change Management

a) Vendor shall implement documented change management and problem management processes which require management review and approval. For example, changes to software code shall require management review and approval.

8. Software Security

a) Vendor shall implement secure coding practices, consistent with industry standards, so that software provided or utilized under this Agreement is not vulnerable to known exploits.

E. Data Security

1. Personal Devices

Vendor shall only store or process Data on / in assets owned or leased by Vendor. Except for back-up media, Vendor shall not store Data on storage devices such as flash drives, memory sticks, CDs, or DVDs.

2. Encryption

All Data that is transmitted between Customer and Vendor's data center through a VPN tunnel shall be encrypted. Data that is transmitted via email and support tickets and other means is not encrypted.

F. Data Destruction and Retention

1. Vendor shall implement policies and procedures around the physical destruction or secure deletion of hardcopy and electronic media based on industry accepted standards.

G. Incident Response

1. Vendor shall have a computer security incident response plan that is supported by a cross-functional response and recovery team that are on call 24x7, 365 days a year.

H. Audit and Monitoring

1. Vendor shall maintain certifications under the ISO 9001:2008 standard for quality management, the ISO 20,000:2011 standard for service management, the ISO 27001:2013 standard for information security management, and the SSAE-16 (SOC I – Type II) requirements for reporting and compliance controls (or the functional equivalent of such standards). Vendor shall, upon request, provide to Customer reports and evidence of such certifications.

Setup

Setup. Setup services, as may be ordered by Customer under an Order Document, is a fixed fee project-based service consisting of the following deliverables:

- Provision the hardware and install the Cloud Applications for the environments.
- Apply security standards for hardening systems.
- Configure on-site and off-site backup procedure.
- Configure disaster recovery procedure.
- Make available network connectivity to Cloud environment.

Exclusions

The following items are excluded from the scope of this Program Document. This list of excluded items is presented only for clarification and this list does not represent a comprehensive list of all excluded items. Certain of these items may be performed under a separate, chargeable project as may be agreed by the parties.

- Project-based services, including implementations (new modules, sites, etc.), upgrade projects, training, testing, configuration or process changes, and data migration. If applicable, Customer has all required source code to allow for re-compile on Vendor Cloud servers.
- Customizations, third-party products, interfaces and integrations are considered out of scope, except as may be expressly agreed by Vendor.
- On-site support.
- Penetration testing, stress testing and other vulnerability testing outside of standard Vendor practice is excluded. Any such activities conducted by Customer without Vendor's knowledge and consent is highly dangerous and will be treated as a cyber attack.
- Data cleansing or fixing of data integrity issues.
- Security of local area network and client machines is Customer's responsibility. Customer is responsible for any impact that a breach of local area network or client security may have on the service levels outlined in this document.
- Customer is responsible for complying with laws and regulations applicable to Customer, including laws and regulations governing the storage and use of personal credit information, and privacy laws and regulations applicable to Customer in its role as data controller.

# # #