QAD CLOUD PROGRAM DOCUMENT

This QAD 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	
Access to the Cloud Services	Upon Vendor's acceptance of Customer's order under an Order Document Vendor shall make the Cloud Services available to Customer on a subscription basis and provide the other Cloud Services as described herein. Customer's usage of the Cloud Services 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 Services and Customer's right to access to the Cloud Services shall cease upon termination of the Order Document. Customer shall not be provided with a copy of the software incorporated within the Cloud Services. Customer's subscription to the Cloud Services is governed by the Application Bundle definitions (an Application Bundle is a collection of software modules made available in the form of a bundle) 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 and Cloud Services Terms shall apply only to the extent applicable to the specific Cloud Services subscribed for by Customer. Customer's use of the Cloud shall be subject to the following restrictions. Customer shall: ● only use the Cloud Services for its own business purposes. ● restrict usage of the Cloud Services 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 Services (e.g. by circumventing the Cloud Services software log-on process). ● not use the Cloud Services for timesharing, rental or service bureau purposes. During the term of any Order Document, Vendor may update the Cloud Services, the Documentation, the Support Service Catalog, the Product Lifecycle Policy, this Cloud Program Document or the Software and Cloud Services Terms to reflect changes in, among others, laws, regulations, rules, technology, security requirements, industry practices, patterns of system use, and availability of third party applications used by Vendor. Vendor commits that any such changes will not materially reduce the level of performance, functionality, security or availability of the Cloud Services during the term of such Order Document. When a new Order Document is signed or when an existing Order Document renews, the then current versions of the Cloud Program Document and associated documents shall apply.
Support Service Catalog	Vendor shall provide Cloud Services and application support and other services as set forth in Vendor's Support Service Catalog, which is published on Vendor's website.

Version Management	Vendor will update the Cloud Services software version at its discretion from time to time to maintain version currency. Vendor will deploy updated software versions to the Customer's production environment during a designated maintenance window that the Vendor will communicate to Customer. Customer is expected to facilitate and to cooperate with software updates and to test new versions to ensure all business processes and associated procedures will continue to be operational following the version deployment. Vendor's obligations under this Cloud Program Document are subject to the phase definitions and other terms of Vendor's Product Lifecycle Policy available at www.qad.com. Vendor is not responsible for performance, functionality, availability or security issues experienced with the Cloud Services that may result from deprecated technology. Vendor shall size Customer's production environment with disk space, compute capacity and other technical elements to achieve optimal system performance. In the event Customer's usage exceeds such disk space allocation or other parameters then Vendor may, with reasonable notice, charge additional fees for such excess usage.
Availability of Cloud Services	Vendor commits to provide availability of the Cloud Services for 99.5% (ninety nine and five tenths percent) of the Scheduled Hours of Operation. The availability commitment shall apply for the production environment only. The Scheduled Hours of Operation are defined as 24/7 (Monday through Sunday during 24 hours each day), minus Planned Maintenance. Planned Maintenance shall be announced to Customer as early as possible, but at least two business days in advance. Vendor will use all reasonable efforts to perform Planned Maintenance outside of regular business hours. Vendor, in its sole discretion, may take the Cloud Services down for emergency maintenance. If Vendor intends to take down the Cloud Services for emergency maintenance, Vendor will use its best efforts to notify the Customer in advance. Unavailability of the Cloud Services is measured over a calendar month and is based on total outage time of the Cloud Services minus Planned Maintenance (if applicable). Unavailability exists when there is a problem with the Cloud Services that prevents the Customer from logging in to, accessing or using the Cloud Services. Customer is responsible for the availability and performance of the infrastructure used to access the Cloud Services at the designated access point. Vendor's system logs and other documentation (e.g. announcements of Planned Maintenance) shall be used as the basis for calculating availability of the Cloud Services. Information on availability of the Cloud Services is available from the QAD Cloud Portal.
Service Credits	If Vendor fails to meet the availability commitment for the Cloud Services for any calendar month, Vendor shall provide, as the sole and exclusive remedy, a service credit based on the monthly Cloud Services fees paid for the impacted Cloud Services. To obtain the service credit, Customer shall provide Vendor with a written request within 30 days of the last day of the month in which such failure occurred. Once Vendor has verified the request, Vendor will provide a service credit to Customer's account that may be applied against subsequent invoices, equal to the fee for one 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.
Backup	Vendor regularly makes backups of Customer's data stored in the Customer's production environment for the purpose of minimizing data loss in the event of an incident. A production backup is typically retained for a period of at least 30 days after the date that the backup is made.

Disaster Recovery	Vendor maintains an ISO-compliant procedure for recovering Customer Data and restoring service to a secondary data center in the event the primary data center is declared by Vendor to be inoperable due to a catastrophic disaster. Vendor responsibilities ● 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. ● Vendor provides a Recovery Time Objective (RTO) of eight (8) hours after a Disaster has been declared by Vendor at the main hosting facility. ● Vendor provides 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. Customer responsibilities ● Customer shall establish an operational disaster recovery plan in place prior to implementation. ● Customer shall review the disaster recovery plan every six months. ● Customer shall test the disaster recovery plan annually (the Disaster Recovery Offering includes two person days Vendor assistance with testing). ● If Vendor has provided private networking access then 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 testing any third-party interfaces or third-party products in the event of a Disaster. ● If Customer does not fulfill the foregoing responsibilities then the RPO and RTO and other Vendor Disaster Recovery commitments may not be available.

Issue Resolution

Vendor shall provide support, as set forth in the Issue Resolution section of the Support Service Catalog, for reported issues that may impair or negatively affect the ability to operate Vendor solutions. Issue Resolution is provided on a 24x7x365 basis via a tiered prioritization of issues based on the impact and urgency to customer operations.

Vendor shall respond to reported issues within the response times set forth in the following table.

Severity	Definition	Response time
0	Showstopper, Major Business Impact, No Workaround available. A down production system making business operations unavailable.	Direct connection to support personnel (live channel / immediate) or a response within 30 minutes of incident report

1	Critical, Pervasive Business Impact, Workaround available. A pervasive issue with significant impact to business, affecting a production system and impeding normal business operations, but with the existence of a workaround.	2 hours from incident report
2	Moderate Business Impact, Workaround available. Typically reflects an isolated issue that is having a contained impact on business operations or an implementation effort, but with the existence of a workaround.	4 hours from incident report
3	Non-Critical, Minor Business Impact. Typically reflects a minor inconvenience on business operations or an implementation effort, but with the existence of a workaround.	8 hours from incident report
Stated response times are for solutions in the Generally Available phase per the Vendor Product Lifecycle Policy. Response times vary for later phases as set forth in the Support Service Catalog.		

Security Procedures

Vendor shall maintain an information security program, and a dedicated security organization, designed to protect the availability, integrity and confidentiality of the Customer Data. Vendor shall perform a risk assessment of the Cloud Services each year, which shall include an evaluation of risks to the Customer Data and a documented plan to correct or mitigate those risks. Specifically Vendor shall maintain the following controls or their function equivalents:

1. Personnel. Vendor personnel (including employees, contractors, and temporary employees) are subject to the Vendor information security practices and any additional policies that govern their employment or the services they provide to Vendor. Personnel who may have access to Customer Data are required to be bound by a confidentiality agreement, and to undergo security awareness training, and to undergo a background check upon hiring.

2. Data Storage and Handling. Storage medium or any equipment with storage capability, including mobile media, used to store Customer Data will be secured and hardened in accordance with industry standard practices, such as:

- Vendor shall maintain a reasonable asset management policy to manage the lifecycle (commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) of such media.
- Decommissioned media containing Customer Data will be wiped in accordance with industry standards.
- Customer Data will be logically segmented from Vendor and other Vendor customers' data.

3. Data Transmission. Customer's access to the Vendor Cloud Services is provided through a secure communication protocol using strong cryptography and security protocols consistent with industry standards.

4. Technical Controls.

- Server Operating Systems. Vendor servers will use a hardened operating system implementation customized for the Cloud Services. Vendor will maintain a risk-based prioritized patch management policy.
- Access Control and Privilege Management. Vendor employs systems and processes to limit physical and logical access based on least privileges and segregation of duties to ensure critical data can only be accessed by authorized Vendor personnel.
- User Accounts. Customer will have control over the creation, deletion, and suspension of user roles

within the Cloud Services..

- Password Policy. Customer shall apply industry-standard practices for password creation and safekeeping. Customer shall use unique logon IDs for individuals, devices and processes (i.e. logon IDs shall not be shared).
- Network Connectivity Security Requirements. Vendor will protect its infrastructure with multiple levels of secure network devices. All remote access to the Cloud Services environments by Vendor personnel that have access to Customer Data must be through one or a combination of the following: virtual private network, multi-factor authentication, mutual authentication, client trust scoring, or other authentication methods with an equal or higher level of security.
- Change Management. Vendor maintains a change management policy to ensure changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.

5. Data Center Environment and Physical Security.

- Physical Security Staffing. Each Vendor data center is staffed by onsite security personnel and monitored by a security organization responsible for continuous physical security functions.
- Physical Security Access Procedures. Formal access procedures exist for allowing physical access to the data centers.
- Physical Security Devices. Data centers employ electronic access control systems that are linked to a system alarm. Unauthorized activity and failed access attempts are logged by the access control system and investigated as appropriate.
- Redundancy. The data centers are designed with resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks. Infrastructure systems have been designed to eliminate single points of failure.
- Power. The data center electrical power systems are designed to be fully redundant and maintainable without interruption to continuous operations. Backup power is provided by various mechanisms including the use of batteries and generators. Backup power is designed to supply uninterruptible and consistently reliable power protection during utility brownouts, blackouts, overvoltage, undervoltage, and out-of-tolerance frequency conditions.

6. Software Security. Vendor shall maintain industry-standard procedures for building security into the design, build, testing, and maintenance of the Cloud Services, subject to the Vendor Product Lifecycle Policy.

7. Incident Response. Vendor shall monitor its systems for indications of compromise, and, in the event of a security incident involving an unauthorized disclosure of unencrypted Customer Data, Vendor shall promptly notify Customer in accordance with Vendor's obligations under applicable law.

8. Certifications and Audit. Vendor shall maintain certifications under, the ISO 20000:2018 standard for service management, the ISO 27001:2013 standard for information security management, the CSA-STAR (Cloud Security Alliance - Security, Trust, Assurance, and Risk) controls and the SSAE-18 (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.

Conditions and Exclusions

The following conditions and exclusions apply. This list is provided as examples only, and it not intended to comprehensively state all conditions and exclusions that may apply. Items excluded from the scope of this Program Document may be performed as a separate, chargeable project as may be agreed by the parties.

- Professional services are excluded from the scope of this Program Document. By way of example, professional services include the following activities:
    - implementation projects and upgrade projects;
    - development of enhancements and customizations;

    - development of or changes to configuration, processes, workflows and translation maps;
    - training, consulting, testing and validation services;
    - data migration, data conversion, data cleansing, and resolution of data integrity issues.
- No outside customizations, localizations, interfaces, integrations or other code or software products shall be deployed in any Cloud Services environments except by Vendor's express agreement. To the extent Vendor permits such outside elements Customer shall be responsible for the licensing and support of such elements and Vendor shall not be responsible for performance or security issues caused by such elements. Except as may be expressly agreed by Vendor, Vendor provides no support, release management, impact management, testing or quality assurance, or other services with respect to such outside elements.
- Customer acknowledges that proper operation of the Cloud Services depends in part upon implementation and other professional services being performed in accordance with Vendor's implementation guidelines and pre-go-live milestone quality assurance checks. To the extent that professional services are provided by any person other than Vendor, Vendor shall not be responsible for go-live delays or performance or security issues caused by a failure to adhere to such requirements.
- Customer is responsible for all infrastructure (including local area network, client machines, printers and access management thereto) outside of the data center infrastructure provided by Vendor, and Customer is also responsible for connections into the Vendor data center infrastructure.
- Penetration testing, stress testing and other vulnerability testing outside of standard Vendor practice is prohibited. Any such activities conducted by Customer without Vendor's knowledge and consent is highly dangerous and will be treated as a cyber attack.
- In the event Customer experiences a security incident within its own systems then Customer shall immediately notify Vendor and Vendor shall disconnect Customer systems from Vendor systems, and such systems shall remain disconnected until such time that Vendor has determined in its reasonable discretion that it is safe to reestablish connection.

# # #