QAD CLOUD EDI PROGRAM DOCUMENT

This QAD Cloud EDI 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 provide the Cloud Services, which under this Program Document consist of operating EDI translation and communication services as a value-added network and making such network available to Customer as provided herein. Customer's usage shall be limited to the subscription levels set forth in the Order Document and access shall cease upon termination of the Order Document. Customer shall not be provided with a copy of any software applications. Customer's use of the Cloud Services shall be subject to the following restrictions. Customer shall: • only use the Cloud Services for its own business purposes. • not use any method, software or technology which hides or understates the actual degree of usage. • not use the Cloud Applications for timesharing, rental or service bureau purposes. Customer may permit a third party to access the Cloud Services 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 Services by Customer.
Version Management	Vendor shall determine the version of applications used in the Cloud Services. Vendor shall also determine whether and when to implement bug fixes and service packs for the Cloud Services. If Vendor decides to upgrade such applications, Vendor shall give reasonable advance notice to Customer. If Customer requires additional services (e.g. training and consultancy), such services will be charged at the then current rates.
Environments	As part of the Cloud Services, Vendor will provide one production environment and, on request, one non-production environment. The service levels outlined in this Program Document apply to the production Environment only (i.e. only to the Environment that transactions Customer's live data).
Environment availability commitment	Vendor warrants the availability of the Environment for 99.5% (ninety nine and five tenths percent) of the Scheduled Hours of Operation during Go-Live status. 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 the Maintenance Windows and minus the Scheduled Emergency Downs. A Maintenance Window is a period during which the Cloud Services will be unavailable, downtime not to exceed eight (8) hours. Maintenance Windows shall be announced to Customer at least three days prior to the scheduled time of the Maintenance Window. A Scheduled Emergency Down is the period during which specific activities are performed, which cannot wait for the next Maintenance Window. Information on Maintenance Windows and Scheduled Emergency Downs is available within the Customer's Online collaborative share location or will be communicated in writing (by email or letter).
Measuring availability	Unavailability of the Environment is measured over a calendar month and is based on total outage time incurred by the Customer. Environment unavailability will exist when (i) the Environment is unable to translate or communicate EDI messages between the customer system and its trading partners; and (ii) the communication failure is not due to a connectivity issue caused by the customer systems or its trading partner systems and (iii) such failure is recorded in the trouble ticket system of Vendor. Environment unavailability is measured from the time the trouble ticket is opened until the time Vendor determines that the affected service is again able to transmit and translate data. Customers are responsible for the connection between their sites (and users) and the Vendor data center. Vendor Cloud relies on an Internet Protocol connection. If the connection is slowed or becomes unavailable, the Cloud Services may become unresponsive or unusable. Poor performance by network connections 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 two business days of the last day of the month in which such failure occurred, Vendor will provide a service credit to Customer's account that can 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 (1) 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); (d) scheduled outages such as outages during Maintenance Windows or Emergency Scheduled Downs, or (2) Customer is not in compliance with the Cloud Services Agreement. 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.
Disaster Recovery	Due to the nature of the service, daily backups do not provide the level of protection required for business continuity. Data is replicated to multiple devices across physically separate data centers in real time.

Support for Environment Infrastructure

These service levels pertain only to the above mentioned Cloud EDI Services. Service levels pertaining to the operation of the EDI eCommerce application or the rest of the Vendor's Applications are set forth in the Vendor's Customer Support Guide and Customer's separate license/maintenance agreement.

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.

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 9:00 AM to 11:59 PM Barcelona Spain, local public holidays excluded.
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.

Support for Cloud EDI Services ("R" indicates the party responsible)			
Task	**Frequency**	**Vendor**	**Customer**
Support for Cloud Services shall be provided in accordance with Vendor's Customer Support Guide.			
Access to Knowledge Management program; Vendor will make the following items available: • On-line training on industry and application content where available • On-line Qbits; video based training on specific topics within the application where available • Mastery tests at end of training discipline	As Needed	R	
Account review • Review Support process and tools that are available • Review customer's incident metrics	As Needed	R	
T1 - First point of contact • Provide basic troubleshooting • Determine incident severity • Coordinate issue resolution	As Needed	R	
T2 - Resolves complex issues related to the service • Deliver knowledge to T1 • Identify process improvements • Determine escalation priority • Assist in identifying data discrepancies	As Needed	R	
T3 - Provide bug fixes via service pack, bug fix or workaround	As Needed	R	
Monitoring of open incidents	As Needed	R	
Online incident management and reporting	As Needed	R	
Access to knowledgebase of Vendor	As Needed	R	
Provide qualified contacts for each business function to interface with Vendor Support	As Needed		R
Provide contact for overall responsibility of support relationship and meet regularly to review service levels and process improvements • This person will be responsible for coordinating all internal activities related to support requests	As Needed		R
All business data setup and data standards	As Needed		R
Review documented procedures	As Needed		R

Provide remote access to all supported services and systems via dedicated network site to site connection	As Needed		R
End user assistance in testing of installed ECO's, patches, service packs, or upgrades	As Needed		R
Support incidents entered with required information using Vendor's online help desk ticket system • http://www.qad.com/erp/Support	As Needed		R
All end user testing	As Needed		R
Communication of maintenance windows with reasonable time in advance to the Customer	As Needed	R	
Security of local area network and client machines. Responsible for any impact that a breach of local area network or client security may have on the service levels outlined in this document.	As Needed		R
Vendor will have access to Customer's business processes documents or personnel to understand the business implications of a solution	As Needed		R
Escalation process will be defined by both parties and with assigned personnel as escalation points	As Needed	R	R
All requests outside of Severity 0 will be received via the Vendor On-Line Support user interface	As Needed		R
All Severity 0 requests will be called into Vendor's emergency Support line	As Needed		R
Storage of credit card data and PCI (personal credit information) legal compliance are not supported. Customer is responsible for ensuring any required PCI legal compliance	As Needed		R

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 Trading Partners' 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 and its partners shall perform background checks on all applicable employees and contractors prior to employment or engagement.

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

C. Disaster Recovery/Business Continuity 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.
   b) Logical or physical controls to segregate Customer's Data from data from Vendor's other customers.

2. 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.

3. System Hardening Vendor shall implement policies and technical standards to harden operating systems, networks, databases, and web services.

4. 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.

5. Change Management 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.

6. Software Security 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 Destruction and Retention Vendor shall implement policies and procedures around the physical destruction or secure deletion of hardcopy and electronic media based on industry accepted standards.

F. Incident Response 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.

Exclusions/Quoted Requests

The following items are excluded from the scope of the QAD Cloud EDI program and will require the initiation of a separate, chargeable project. This list of excluded items is presented for clarification, however; this list does not represent a comprehensive list of excluded items. Each individual chargeable project will be quoted at the agreed to Vendor's resource rates.

- Project related activities
- On-site training and consulting
- Implementation, development, support or upgrade of enhancements/customizations to the QAD Cloud EDI translation and communication workflows
- Implementation, development, support or upgrade of any elements related to QAD EDI eCommerce, the 3PL Add-On Services Module, QAD Enterprise Applications or any customization of the applications mentioned
- Third party or home grown application customization, support or upgrades/migrations
- Changes required to QAD Cloud EDI due to third party or home grown software
- IT support other than what is outlined above in the Cloud Services section
- Data cleansing or fixing of data integrity issues
- Application or business process consulting
- Connection fees to VANs or private networks not currently interconnected to QAD Cloud EDI and that require a specific connection fee

# # #