CONNECTED WORKFORCE CLOUD PROGRAM DOCUMENT

This Connected Workforce Cloud Program Document establishes terms and conditions for Connected Workforce 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 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 use of the Cloud Services shall be subject to the following restrictions. Customer shall: ● use the Cloud Services exclusively 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. ● not engage in or promote any illegal or abusive activity ● not engage in activity that is likely to damage, disable, disrupt, overload, interfere with, or impair the features, functionality, integrity, or performance of Software Services; ● not do any of the following: (a) circumvent any security or authentication feature, or access, or storage restriction of the Cloud Services, (b) scan, monitor, probe, or test the vulnerability of the Cloud Services, or (c) take any action that is reasonably likely to pose a threat to the security or operation of the Cloud Services or the network, computer systems, communications systems, software applications, or computing devices of Vendor or a third party. During the term of any Order Document, Vendor may update this Cloud Program Document 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 version of this Cloud Program Document.
Availability of Cloud Services	Vendor commits to provide availability of the Cloud Services for 99.9% (ninety nine and nine tenths percent) of the Scheduled Hours of Operation. The availability commitment shall apply for the production environment only, and excludes any beta, early adopter or free trial version of the Cloud Services.

	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 and for Planned Maintenance to be no more than one hour in the aggregate per month. 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. Availability is calculated as the overall uptime tracked on Vendor's status page (at https://status.rzsoftware.com/) and denoted as "Redzone Service". This status page will serve as the exclusive determinant of overall uptime. Customer is responsible for the availability and performance of the infrastructure used to access the Cloud Services at the designated access point.
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 0.1% (one tenth of one percent) of the time, up to a maximum of the total Cloud Services fees charged by Vendor to Customer for such month.

Issue Resolution

Vendor shall provide support 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 Priority to Customer operations. Customer must submit support requests through the Redzone App or through the 24/7 Knowledge Base *via* the built-in chat widget.

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

Priority	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	3 hours from incident report

	business operations, but with the existence of a workaround.	
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.	6 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.	12 hours from incident report

Artificial Intelligence

Customer acknowledges that certain features of the Services may incorporate artificial intelligence ("AI") technologies, which operate autonomously or semi-autonomously to generate outputs, including automated decisions, based on trained models and reference data sets that are built using Customer Data. To activate the Vendor AI-enhanced Services Customer must opt-in by using the settings within Vendor's software platform. AI-generated outputs are provided on an 'as-is' basis. Customer acknowledges that AI outputs may contain errors or inaccuracies and accordingly Customer agrees to implement appropriate human review processes before relying on such outputs for business decisions. By opting in Customer permits Vendor to collect, analyze, and otherwise use Customer Data internally to provide and further develop and enhance its AI-enhanced Services. Customer Data used to train AI models will be aggregated and anonymized so that it cannot be linked to Customer or any individual. Customer shall at all times retain ownership of its Customer Data and its own AI inputs and outputs. Customer may opt out of using the AI-enhanced Services by deactivating the AI feature within Vendor's software platform. Upon such opt-out Vendor shall cease further use of the Customer Data in connection with the AI-enhanced Services. Such opt-out shall not require or result in any alteration of Vendor's trained AI models. Additional background on the use of AI in QAD offerings is provided in the QAD Trust Center (https://www.qad.com/trust-center).

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 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 27001:2022 standard for information security management, the CSA-STAR (Cloud Security Alliance - Security, Trust and Assurance Registry) controls and the SSAE-18 (SOC I – Type II and SOC II - 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;
  - training, consulting, testing and validation services;
  - data migration, data conversion, data cleansing, and resolution of data integrity issues.
- 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.

# # #