Cloud Services Standards

IMPORTANT – READ CAREFULLY**: This Confidentiality Notice is a legal agreement between you and Quorum Business Solutions, Inc. ("**Quorum**") for access to this documentation ("**Documentation**"). **BY ACCESSING THE DOCUMENTATION, YOU AGREE TO BE BOUND BY THIS CONFIDENTIALITY NOTICE. IF YOU DO NOT AGREE, DO NOT ACCESS THE DOCUMENTATION, AND IMMEDIATELY RETURN OR DESTROY ANY RELATED INFORMATION RECEIVED.

The Documentation and Software described herein is protected by intellectual property laws and contains valuable confidential information proprietary to Quorum and/or its group companies. You are only allowed to access and use the Documentation on behalf of the Quorum group customer or partner having obtained a license to the Documentation. You may not reproduce or disclose the content of the Documentation or any portion thereof outside your organization and/or to any third parties such as subcontractors or partners without prior written consent from Quorum or except as permitted under a valid Software License.

The receipt or possession of the Documentation or any information included herein does not convey any rights to (i) remove or modify a copyright or other proprietary rights notice in the Documentation, (ii) disassemble, reverse engineer, or decompile the Software, (iii) develop, manufacture, use, or sell anything intended to be offered to third parties in competition with the Software, or (iv) create derivative works based on or otherwise modify the Documentation or Software. You acknowledge that the Documentation and Software may be subject to change and under no circumstances will Quorum, any of the Quorum group companies, or their respective officers, directors, employees, agents, or representatives be liable for any damages, whether direct, indirect, special, or consequential damages for lost revenues, lost profits, or otherwise, arising from or in connection with your access to the Documentation solely under this Confidentiality Notice.

Find out more about the Software and Quorum products and services at www.quorumsoftware.com or by asking your local Quorum representative.

Last Updated: October 16, 2023

Table of Contents

Section 1 – Introduction

Subject to an Order, the SaaS Subscription(s) provide cloud access to eligible Software for an agreed term.

The Cloud Services Standards ("**Standards**") outlined in this document describe the operational standards for SaaS Subscription(s). For information on Vendor's product and customer support standards, including contact information, case submission process, and service level objectives, refer to the Global Customer Care – Customer Support Policy.

Vendor may update or revise these Standards from time to time. Updates to the Standards will be made available within this document including the date of change as well as the changes made. New versions will enter into force immediately, except for any ongoing annual Subscription term, for which the previous version will apply until the end of such ongoing term. Customer should review the Standards prior to using the SaaS Subscription(s) to stay informed about the applicable operational standards. Capitalized terms are defined in these Standards, the Order, or the Agreement for the purchase of the SaaS Subscription(s).

Section 2 – Eligibility

Customer must pay all applicable fees and have a current SaaS Subscription to qualify for the support under these Standards.

Section 3 – Availability Commitment

"**Available** means the time (in minutes) in a calendar month that the applicable Software is accessible for Production Use. The "**Availability Percentage**" = ([Total minutes in a calendar month – Outage minutes] / Total minutes in a calendar month) x 100.
"**Excused Outage**" means a Maintenance Window, scheduled outage, or any time the Production Environment is not Available due to Exclusions (as defined below).
"**Maintenance Window**" means the period between 8PM and 6AM in the SaaS Subscription Customer region specified in the applicable Order, where scheduled maintenance will be performed.
"**Production Environment**" means the environment (software and supporting infrastructure) where the eligible Software is put into operation for its intended use by end users using Customer's actual business information and used for actual business purposes.
"**Production Use**" means that Customer can access the Software to perform mission-critical processes vital to the daily business operations of Customer's business in the Production Environment.
"**Outage**" means the period that the Software is unavailable in the Production Environment for reasons other than an Excused Outage, measured in minutes from the time an Incident (as defined in the Customer Support Policy) case is opened in Vendor's incident

management system and validated, until the time when Production Use has been restored, including through a resolution or workaround. If two or more outage events occur simultaneously, the event with the longer duration will be used to determine the total Outage minutes.

Availability Commitment

Vendor will as of completion of onboarding tasks under a SaaS Subscription, make the ordered Software available in the Production Environment at the percentages described below during each calendar month of the Subscription Term:

	Availability Percentage	Outage Percentage
Standard Availability	99.0%	1.0%

If the Order expressly states that High Availability is provided, the following percentages apply instead solely with respect to the subject SaaS Subscription:

	Availability Percentage	Outage Percentage
High Availability	99.50%	0.50%

Downtime Services Credit

If availability falls below the applicable Availability Percentage during any given calendar month and Customer notifies Vendor thereof and requests a credit (a "**Credit Notification**") within 30 days of such interruption, Vendor will grant Customer a prorated credit of the affected monthly SaaS Subscription fee. The credit or fee relief will be equal to the prorated SaaS Subscription fee based on a 30-day month, being charged per hour for each hour of a day of the system being unavailable less than the stated availability, which credit shall not exceed 30% of the monthly fees for a given month's SaaS Subscription ("**Maximum Credits**").

If a Credit Notification is received by Vendor prior to preparation and sending of an invoice, this credit shall appear on the invoice immediately following Vendor's receipt of the Credit Notification, and any such credit above the amount of said invoice shall be applied to future invoices until fully applied. Such credit shall be Customer's sole and exclusive compensation for any downtime or other unavailability of the Software in the Production Environment. Vendor shall have no other liability of any kind for any damages or loss arising because of such downtime or unavailability.

Exclusions

The Availability Commitment does not apply to non-production, development, or testing environments, or to any unavailability or performance issues caused by or that result from any of the following (each, an "**Exclusion**"):

a. Customer or third-party equipment, software, or other technology (other than third-party equipment provided, managed, and controlled by Vendor under the SaaS Subscription);

b. Customer's use of the SaaS Subscription in violation of the terms of the applicable Order or the Agreement;
c. Misuse by Customer's users (for example, unapproved hack or denial of service attack initiated by an authorized user);
d. Customer's failure or refusal to install, or to allow Vendor to install, security patches or third-party software patches;
e. Customer's failure or refusal to allow Vendor to install current applicable releases, updates, and upgrades for the SaaS Subscription which Vendor has identified and offered to Customer to resolve the underlying issue causing the SaaS Subscription downtime or service disruption;
f. Excused Outages, including downtime arising from upgrades or updates or for installation of security patches, scheduled maintenance performed within the Maintenance Window, or where Customer has been notified at least two weeks in advance, or emergency repairs;
g. Factors outside of Vendor's reasonable control, including (i) any force majeure event, (ii) telecommunication disruptions, packet loss, network, or internet outages, (iii) hardware, software, networks, or power systems not within Vendor's possession, reasonable control, or responsibility, (iv) denial of service attacks, viruses or hacking attacks for which there is no commercially reasonable known solution, or (v) any other events that are not within Vendor's control that could not have been avoided with commercially reasonable care; or
h. Suspension or termination of Customer's right to use the SaaS Subscription in accordance with the terms of the Agreement or Order.

Furthermore, Availability may be dependent on and subject to availability of public cloud infrastructure on which the SaaS Subscription is hosted. Public cloud availability is not covered by the service availability metrics set forth in these Standards. If the public cloud infrastructure is unavailable, and therefore the SaaS Subscription is unavailable, Customer's sole recourse pursuant to the Agreement is against Vendor and not the public cloud vendor. In such event, Vendor may have recourse against the public cloud vendor pursuant to Vendor's separate agreement with such public cloud vendor for restoring Availability and, to the extent permitted, will pass through to Customer the same remedies Vendor may have against such third party for any non-performance.

Section 4 – Disaster Recovery and Planning Options

A "**Disaster**" means a sudden, unplanned catastrophic event or emergency, like a disaster (natural or man-made), or any other business or technical disruption that results in the complete loss of Availability of the SaaS Subscription or Customer Data with no imminent hope of recovery.

Disaster recovery options are defined by RTO and RPO objectives:

- "**Disaster Declaration**" is the process to activate the disaster recovery plan after a Disaster occurs. Vendor has sole discretion to decide if, when, and under what circumstances a Disaster is declared.
- "**Recovery Time Objective**" or "**RTO**" is the time objective for a Production Environment to become operational (i.e., core business features are available but there may be features, such as historical reporting functions, that will only become available outside of this time window), measured from the time of a Disaster Declaration.
- "**Recovery Point Objective**" or "**RPO**" is the maximum acceptable level of data loss following a Disaster. The RPO represents the point in time, prior to the Disaster, to which lost data can be recovered.

Vendor will provide Disaster recovery services at the Disaster Recovery Level identified in the Order for the SaaS Subscription.

Disaster Recovery Level	RTO	RPO
Standard	As soon as reasonably possible	24 Hours
Extended	Up to 24 Hours	12 Hours

A security event that impacts Customer's SaaS Subscription will not be deemed a Disaster and, therefore, will not be subject to the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Section 5 – Stay Current Commitment

Customer will under a SaaS Subscription have access to updates, version releases, and upgrades to the Software that Vendor generally makes available as part of the subscription to all licensees of the Software and that are not designated as new products, modules, or add-ons for which additional licensing would be required.

Vendor will perform the Software packaging and deployment for such updates, releases, and upgrades to Customer's Production Environment as part of Customer's SaaS Subscription (the "**Technical Upgrades**"), but will not be responsible for upgrading, updating, or enhancing any modifications or extensions to the Software unless expressly included in the Order for the SaaS Subscription. Furthermore, services associated with migrating Customer from an existing on-premise installation to a SaaS Subscription are not included. Customer will provide the collaboration, as reasonably requested by Vendor, to test and accept the Technical Upgrades as applicable. Customer may also request additional Professional Services from Vendor to assist with user acceptance testing of a new Software release, configuration of new release features or business rules, or any other discretionary services. Such services will be contracted and performed under a separate Order.

Any Customer-developed code or interfacing applications must leverage Vendor-published or -approved APIs to access the Software. Vendor reserves the right to validate any Customer-developed code that will connect to or be incorporated in the Software. Unless otherwise agreed, Customer is responsible for all interface functionality affected by the Technical Upgrades that is not part of the Software.

Technical Upgrades may consist of new Software features (as described in the applicable Documentation and Order) and/or bug fixes for the correction of defects to the then-current version of the Software.

Technical Upgrade Type	Description	Time Frame
Unscheduled	At Vendor's sole discretion, unscheduled updates may be delivered into the Production Environment at any time without prior notification, but only to the extent the updates can be performed without creating system downtime for Customer.	As Needed
Emergency	Vendor reserves the right to perform emergency updates from time to time to rectify critical issues in the Software that cannot reasonably be postponed without causing a potentially negative impact to Customer's environment. During an emergency update, any user attempting to access the Software will be notified that the Software is unavailable due to an emergency update. Vendor will provide notifications of emergency updates via email as soon as reasonably practicable and will provide a root cause analysis of the emergency issue within 10 business days of the conclusion of the emergency update.	As Needed
Scheduled	Updates required to keep the Software and cloud infrastructure operating at optimal status. Standard updates typically address infrastructure performance, Software issue resolution or enhancement deployment, or security-related updates. Scheduled maintenance will be performed within the applicable Maintenance Window.	Scheduled with advance communication to Customer
Continuous Delivery	For enabled solutions, Vendor practices agile development and provides the delivery of updates on a continuous basis.	As needed

Section 6 – Shared Responsibility Model

Vendor takes data security seriously and implements various technical, organizational, administrative, and physical security measures to protect Customer's information as appropriate to the nature of the SaaS Subscription and sensitivity of data processed through the Services and as further described under the Quorum Technical and

Organizational Measures for Data Protection. However, no system can guarantee absolute security, and there are inherent risks associated with the transmission and storage of data over the internet or any electronic system. By using SaaS Subscriptions, Customer acknowledges and accepts these risks. The Shared Responsibility Model (as set forth below and as may be further elaborated in other portions of the Documentation) identifies the responsibilities of the Parties regarding security and management of applicable systems, software, and data.

Vendor is responsible for:

- Implementing reasonable measures to protect Customer data within the Vendor-operated environment(s)
- Enabling data encryption and usage of secure communication protocols (e.g. HTTPS for web endpoints)
- Provision of a facility to enable Customer to leverage multifactor authentication to authenticate against Vendor hosted applications.
- Informing Customer of any significant data or security events within a reasonable timeframe

Customer is responsible for:

- The data provided by Customer (or any user that Customer allows to access the Vendor software or services), including the legality, reliability, integrity, accuracy, consistency, and quality of such data
- Using and securing Customer's hardware, software, applications, data, and operating systems (which may include integration middleware), including by implementing appropriate updates and security patches
- Implementing appropriate measures to prevent unauthorized access to or use of the Vendor software or services by mandatorily installing multifactor authentication (MFA), either by Vendor if so agreed, or by Customer itself, including maintaining the confidentiality of users' credentials
- Any software applications developed by or for Customer for interaction with data generated by use of the Vendor software and services (if such applications are permitted under the Agreement between Vendor and Customer), including any updates necessary to access, communicate, or interoperate with the Vendor software and services
- Implementing appropriate measures to protect Customer data stored on Customer's own systems and other systems that are not operated by Vendor
- Use of any output from the Vendor software or services that is stored on Customer's own systems or other systems that are not operated by Vendor (including if such output was previously transmitted by Vendor to Customer)
- Use of any APIs that access, communicate, or interoperate with any Vendor software or services, including ensuring that any such APIs function as intended (or will continue to function as intended after a version change) or will be maintained (in each case, except to the extent that Vendor has expressly agreed in the Agreement between Vendor and Customer to maintain an applicable API)

- Identifying and implementing retention periods for Customer data that comply with Customer's legal and contractual obligations (including by, if the Software permits Customer to set retention periods, implementing any applicable retention periods within the Software)

Vendor will consider Customer's request to transmit Customer's data that is hosted or processed by Vendor to a secure system that is not owned or operated by Vendor. Once mutually agreed including applicable fees, Vendor will transfer such data using reasonable industry practices to secure the data in transit. After Vendor has transmitted any Customer data to Customer, Customer will be fully responsible for such data (including the protection and use thereof), and Vendor will have no further responsibility for such data.

Customer understands and acknowledges that while Vendor will use reasonable practices for its responsibilities described above, Customer data may not always be encrypted, such as in case of transmission of any mutually agreed SMS (Short Message Services) text messages.

Section 7 – Other Operational Standards

Acceptable Use	Customer is aware of and recognizes that Vendor may use public cloud platform providers as a subcontractor in performance of the Services and that Vendor is bound by their conditions. Customer also understands that its use of the SaaS Subscription and Services is subject to compliance with the publicly available acceptable use policies of the public cloud providers, breach of which will be deemed Customer's gross negligence or willful misconduct.
Backups	Unless otherwise stated in the Agreement (including the Documentation), backups of the Production Environment are taken daily and retained for 30 days.
Custom Development	Custom developed code, scripts, or other items are the responsibility of Customer. Such artifacts must be compliant with the extendibility capabilities of the Software at hand.
Data Storage	Data storage provided includes up to 700 gigabytes per application instance. Additional quantities will be handled on a request basis and subject to additional charges.
Data Transfer	Data Transfers "into" and "out" refer to transfers of data into and out of the Vendor cloud hosting environment(s). There will be no limit or additional charge for Data Transfers into the Vendor cloud hosting environment provided that these transfers are commercially reasonable for standard business use

	and functions of the Software being hosted. A total monthly aggregate allocation of Data Transfer out is provided as part of the base SaaS Subscription Fee. This monthly aggregate amount is equivalent to (a) the higher of (i) the base edit users or (ii) active users for the month multiplied by (b) 4 gigabytes. Additional increments of transfer-out data will be subject to additional charges.
Expansion of New Technology	Vendor reserves the right to change existing infrastructure, hardware, and underlying software used to provide the SaaS Subscription provided that the changes are not materially detrimental to the SaaS Subscription.
Software Environments	Quorum SaaS Subscriptions are provided either as dedicated or shared solutions. Customer will during the Subscription Term be provided with access to the Software on one Production Environment. In cases where a test or development environment is required on a permanent basis during the Subscription Term, it will be limited to one development and one test environment. Vendor is not required to provide any additional environments unless expressly stated in the Order for the SaaS Subscription as an additional option.
Security Management	At least once per calendar year, Vendor commits to perform or to have a third-party auditor perform an assessment of its security controls for technical, organizational, administrative, and physical security. Upon Customer's written request, which shall be no more than once per calendar year, Vendor shall provide a summary of the assessment(s) to Customer. The assessments shall be Confidential Information of Vendor.

Section 8 – Change Log

Date of Change	Details of changes
January 3, 2023	Initial Release
October 16, 2023	General wording clarifications, update of RTO for Standard Disaster Recovery, inclusion of Shared Responsibility Model and Quorum Technical and Organizational security commitments to improve readability and reflect stakeholder feedback
November 15, 2024	Update to Section 6, "Customer Responsibility" bullet 3