Technical & Organizational Measures for Data Protection

The Quorum Software group of companies ("Vendor") implements technical and organizational data security measures ("TOM") designed to meet the data protection principles in an effective manner and ensures that appropriate safeguards are integrated into the Vendor's data processing to meet appropriate industry standard data protection requirements and to protect the rights of data subjects. The purpose of this document is to describe the TOM, which the Vendor implements to protect customer data as data processor.

When referenced or attached, this document will apply to the Subscriptions and Services set forth in the applicable order form, order confirmation, statement of work, invoice, e-commerce confirmation or similar agreement issued by or accepted by the Vendor (each, in any form, an "Ordering Document") and is fully incorporated therein. In the event of a conflict between the terms and conditions of this document and the Ordering Document, the terms and conditions of this document will take precedence.

Additional product level security descriptions may be available upon request if not agreed to be part of the Ordering Document governing the processing of customer data. Customer specific security measures are agreed separately.

1. Information Security Program

The Vendor maintains an information security program that adopts the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"). The program will include, but is not limited to, the following components:

1. Information security policy framework
2. Program documentation
3. Auditable controls
4. Compliance records
5. Appointed security officer and information security personnel

2. Data Protection Executives; Notices

Each of the parties shall designate and notify the other party of its respective Data Protection Executive(s) responsible for the obligations set forth on this document. Any notices under this document should be communicated as follows:

1. Communications regarding the day-to-day obligations should be communicated in writing via email or other written notice to each of the Data Protection Executives (or their designees), and
2. The Vendor reserves the right to update this document periodically when deemed necessary. However, any updates shall provide at least the same, or better, level of protection for customer data.
3. Communications regarding any material changes to this document shall be provided with at least 30 days's notice (the means and mechnisms in providing such notice to be determined by the Vendor and as may change over time).

3. General Security Practices

The Vendor has implemented and shall maintain appropriate TOM to protect customer data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures and internal controls set forth in this document for its personnel and processors, equipment, and facilities at Vendor locations providing the Subscriptions and Services.

3.1 Shared Security Obligations

Customers are responsible for all transactions that occur on their account(s) or portal used to access the Subscriptions and Services ("Accounts") and it is their responsibility to ensure that they and their users use unique usernames and strong passwords for accessing the Subscriptions and Services. Customers are responsible for holding in confidence all Account usernames and passwords. Each Customer user must immediately change their username and/or password combinations that have been acquired by or disclosed to an unauthorized third party. Additionally, Customers must notify the Vendor promptly upon becoming aware of any unauthorized third-party access to any Account or Vendor data or systems.

4. Organization of Information Security

1. The Vendor has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.
2. Vendor personnel and processors with access to customer data are subject to confidentiality obligations and to adhering to policies and guidelines governing their handling of customer data and security practices.

4.1 Security Policies

The Vendor maintains and follows IT security policies and practices that are integral to the Vendor's business and mandatory for all Vendor personnel, including supplemental personnel. IT security policies are reviewed periodically and such policies are amended as the Vendor deems reasonable to maintain protection of services and content processed therein.

4.2 Security Awareness Training

Vendor Personnel, including all employees, temporary staff, vendor-supplied staff, consultants, contractors, and volunteers, complete security and privacy education annually and certify that they shall comply with the Vendor's ethical business conduct, confidentiality, and security policies, as set out in the Code of Conduct. Additional policy and process training may be provided to persons granted administrative access to security components that is specific to their role within the Vendor's operation and support of the service, and as required to maintain compliance and certifications.

The Vendor trains and communicates its defined information security principles and information security policies and standards to Vendor personnel in accordance with the following:

1. Vendor personnel are required to take trainings, both at hire and on a regular basis, covering information security practices, the proper handling of customer data, and the proper use of information processing systems and facilities to better identify and minimize possible security threats.
2. Vendor personnel are instructed to report any observed or suspected threats, vulnerabilities, or incidents to a designated point of contact.
3. Vendor information security personnel is made aware of reported information security threats and concerns and will support the Vendor information security policy in the course of their normal work.

4.3 Privacy by Design

The Vendor incorporates Privacy by Design principles for systems and enhancements. For example:

1. Our Subscriptions and Services strive to process the minimal personal data necessary for the purposes. Customers control the types and volume of personal data that are input into the Subscriptions and Services;
2. The Vendor considers pseudonymization, aggregation, and/or anonymization of personal data to the extent possible, such as to analyze activity within the Subscriptions and Services;
3. The Vendor grants internal access to customer-facing environments and customer data on a need-to-know basis on the principle of least privilege; and
4. The Vendor is transparent about its personal data processing practices, as reflected in its data processing agreements and posted privacy policies.

4.4 Risk Management

The Vendor assesses risks related to processing of personal data and creates action plans to mitigate identified risks.

4.5 Compliance with Laws

The Vendor has established and adheres to policies that comply with applicable laws. However, the Vendor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to the Vendor. The Vendor does not determine whether Customer data includes information subject to any specific law or regulation and compliance with any such law or regulation is the sole responsibility of the Customer.

To the extent a data protection or security law is applicable to Customer but not generally applicable to Vendor, prior to providing any regulated data to the Subscriptions and Services, Customer is responsible for notifying the Vendor of the applicable law and relevant legal requirements and proposing contractual language to satisfy the cited legal obligations. The Vendor will in good faith consider the proposed language and its ability to comply with new legal requirements.

4.6 Security Assessments

To the extent the Vendor performs an independent third-party assessment or certification with respect to the subject Subscription or Service (e.g. ISO 27001 and SOC 2), Customer may upon request review an available summary of the results of such security assessment for the Subscription or Services containing Customer data processed by Vendor. All information and documentation shared with Customer relating to such assessments or certifications shall be the

Vendor's confidential information and subject to the confidentiality obligations under the subscription or services agreement.

5. Access Control

5.1 User Access Management
The Vendor maintains proper controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications. Only personnel with a clear business need are provided access to systems, applications, databases and/or ability to download data within the Vendor network and are given only those privileges needed in order to complete its task in line with principles of least privilege. All Vendor systems must meet corporate IT security standards and employ security configurations and security hygiene practices to protect against unauthorized access to system resources.

All access requests shall be approved based on individual role-based access and reviewed on a regular basis for continued business need.

5.2 Logical Access & Identity Management Policy
A logical access and identity management policy is established, documented, and reviewed based on business and information security requirements. Any Vendor employee, contractor or data processor who processes customer data is subject to this policy or equivalent standards.

5.3 Access Record Keeping
The Vendor maintains a record of security privileges of its personnel and processors that have access to customer data.

5.4 Access Authorization
The Vendor maintains vendor account creation and deletion procedures, with appropriate approvals, for granting and revoking access to systems accessing or processing customer data at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

5.5 Least Privilege
The Vendor limits access to customer data to those Vendor personnel or subcontractors performing the Subscriptions and/or Services and, to the extent technical support is needed, its personnel or contractors performing such technical support.

5.6 Workstation Protections
The Vendor implements protections on vendor managed end-user devices and monitor those devices to be in compliance with Vendor security standards requiring passwords, screen saver, antivirus software, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations.

The Vendor securely sanitizes physical media intended for reuse prior to such reuse and destroys physical media not intended for reuse.

5.7 Authentication

The Vendor shall:

1. Use industry standard practices to identify and authenticate users who attempt to access information systems.
2. Use authentication mechanisms that are based on passwords and require passwords to adhere to a commercially reasonable information security standard password complexity policy including length, character complexity, and non-repeatability requirements.
3. Maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
4. Limit access to password and key management systems in which passwords and secrets may be stored.

5.8 Background Checks
Employment background checks serve as an important part of the Vendor's selection process. Verifying background information validates a candidate's overall employability or an employee's suitability for a particular assignment. Depending on the country and position at issue, to the extent as is customary and permitted by law, all Vendor background checks may include identification verification, prior employment verification, criminal background information, global terror/sanctions checks and education verification.

6. Operational Policy

The Vendor maintains policies describing its security measures and the relevant procedures and responsibilities of its personnel or contractors who have access to customer data and to its systems and networks.

6.1 Physical and Environmental Security
Vendor-provided Subscriptions and Services are housed in secure facilities protected by a secure perimeter, with industry standard security barriers and entry controls to physically protect them from unauthorized access, damage and interference, including:

1. Access to such facilities are logged and maintained.
2. Procedures are maintained for visitors and guests accessing such Vendor facilities.
3. The Vendor employees physical safeguards designed to protect Vendor provided services systems from security threats and environmental hazards.

6.2 Network Security
The Vendor configures network devices (e.g., firewalls, routers, switches) according to approved lockdown standards.

The Vendor segregates data center networks into separate logical domains with the network security controls approved by its security personnel.

6.3 Web and Application Security
The Vendor maintains reasonable security measures for internet-accessible applications, including:

1. Implementing processes for developing secure applications.
2. Performing pre-deployment and ongoing security assessments of internet-accessible applications. Including but not limited to such things as Open Web Application Security Projects (OWASP) development Guide
3. Validating the input, internal processing, and output of data in internet-accessible application(s)

The Vendor implements a change management process for documenting and executing operational changes in Services.

6.4 Availability & Resilience
The Vendor has implemented and maintains suitable measures to make sure that data is protected from accidental destruction or loss. Systems and applications are evaluated to apply appropriate backup processes based on the criticality of the system and are continuously monitored with regards to availability, functionality, safety, and utilization. This is accomplished by:

1. Redundant service infrastructure in production environments
2. Hosting through state-of-the-art cloud providers and data centers in order to minimize risk
3. Backups are designed and implemented for production environments to prevent the loss of data in the event of a technical malfunction or human error.
4. Business continuity and disaster recovery plans are established for Vendor infrastructure supporting service delivery to customers.

The Vendor shall use reasonable efforts to restore the Subscriptions and Services by having offline backups of application data, infrastructure components and configuration settings.

6.5 Log Monitoring & Alerting
The Vendor maintains logging and monitoring of security relevant events that include access to administrator and partner and API interfaces and data deletion, data change and data recovery events and other events defined in the logging and monitoring Policy that includes protections against log tampering.

6.6 Endpoint Protection
The Vendor implements industry standard endpoint security protections including antivirus, antimalware, threat detection, investigation and response, device management, and evolving zero-day threats.

The Vendor implements and configures anti-virus and anti-malware software on systems holding or processing customer data for regular signature updates.

The Vendor implements and maintans threat management capabilities designed to protect systems holding or processing customer data.

6.7 Change Controls & Validation
The Vendor maintains policies and procedures designed to manage risks associated with the application of changes to the systems managed by the Vendor.

For Customers with managed Services: Prior to deployment of changes to systems, networks and underlying components, changes shall be documented in a registered change request. These include a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Customer, expected outcome, rollback plan, and documented approval by authorized Personnel.

7. Communications Security and Data Transfer

The Vendor uses standard security mechanisms and certificates for communications and secure data transfers.

1. The Vendor encrypts Customer data when in transit externally and at rest including any data backups with reasonable encryption algorithms, except as noted below.
2. The Vendor uses encryption for Customer data being transmitted across the public Internet or wirelessly, and as otherwise required by applicable laws, except as noted below.
3. The Vendor (i) holds such encryption keys in the strictest of confidence, and (ii) limits access to only named individuals with a need to have access.

Customer acknowledges that certain Subscriptions or Services may offer Customer's users the option to communicate with the Vendor via SMS. For example, DaWinci users may elect to receive their travel itinerary by SMS. Customer further acknowledges that communications over SMS are not encrypted and Customer is solely responsible for communicating any restrictions on SMS communications to their users.

7.1 Media Handling

The Vendor implements protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures are implemented for mobile computing devices to protect personal data.

8. System Acquisition, Development and Maintenance

8.1 Security Requirements

The Vendor has adopted security requirements for the purchase or development of information systems.

The Vendor inventories applicable applications and network components and assess their business criticality.

The Vendor reviews critical applications regularly to ensure compliance with industry and reasonable security standards.

8.2 Development Requirements

The Vendor has policies for secure development, system engineering and support. The Vendor conducts appropriate tests for system security as part of acceptance testing processes. Occasional problem solving in production environments are carried out following the logical access and identity management policy.

8.3 Threat and Vulnerability Management

The Vendor maintains measures meant to identify, manage, mitigate and/or remediate vulnerabilities within Vendor computing environments. Security measures include:

1. Patch management
2. Anti-virus/anti-malware
3. Threat notification advisories
4. Vulnerability scanning (all internal systems) and periodic penetration testing (Internet facing systems) within remediation of identified vulnerabilities

9. Information Security Incident Management

The Vendor maintains an incident response plan and follows documented incident response policies and procedures that guide the Vendor's detection, analysis, containment, eradication, and recovery in connection with a security incident.

The Vendor has established relationships with experts to support its incident response, including reputable forensic investigators and outside legal counsel.

The data processing agreement between the parties details the Vendor's obligations in response to a security incident that impacts Customer's data.