Data Processing Addendum

This Data Processing Addendum ("**Addendum**") supplements the FloQast Close Management Software Services Agreement (the "**Agreement**") entered into by and between Controller named below and FloQast, Inc. ("**Processor**" or "FloQast") (each a "**Party**" and collectively the "**Parties**"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

Controller: the applicable FloQast Customer.

1. Definitions

1.1. "**Applicable Law(s)**" means any state, federal or foreign law(s), rule(s) or regulation(s) applicable to the Addendum, the Agreement, or the Processing, including those concerning privacy, data protection, information security, availability and integrity, or the handling or processing of Personal Data. Applicable Laws expressly include, without limitation, if applicable

1.1.1. California Consumer Privacy Act (and superseding legislation, the "**CCPA**");

1.1.2. the United Kingdom Data Protection Act 2018 (and superseding legislation, the "**UK Data Protection Act**");

1.1.3. the General Data Protection Regulation (Regulation (EU) 2016/679) (and superseding legislation, "**GDPR**");

1.1.4. the United Kingdom General Data Protection Regulation (the "**UK GDPR**"); as well as

1.1.5. the laws, rules, and regulations of each nation in the European Economic Area ("**Member State Law(s)**" and the United Kingdom.

1.2. "**Authorized Employee**" means an employee of Processor or a Processor Affiliate who has a need to know or otherwise access Personal Data in order to enable Processor to perform its obligations under this Addendum or the Agreement.

1.3. "**Authorized Person**" means an Authorized Employee or Authorized Subprocessor.

1.4. "**Authorized Subprocessor**" means a third-party subcontractor, agent, reseller, or auditor engaged by Processor, or employee of same, that has a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement.

1.5. "**Data Subject**" means an identified or identifiable person to whom Personal Data relates.

1.6. "**Data Subject Rights**" means the rights recognized and granted to Data Subjects with respect to their Personal Data under Applicable Laws.

1.7. "**Data Protection Impact Assessment**" or "**DPIA**" means an assessment, conducted pursuant to Controller's Instructions, of the impact of one or more Processing operations on the protection of Personal Data and the privacy of Data Subjects that takes into account the nature, scope, context, and purposes of such Processing and includes, without limitation, an analysis of the necessity and proportionality of such Processing as well as the appropriateness of the Technical and Organizational Measures used in connection with such Processing.

1.8. "**Incident**" means a situation whereby Personal Data in either Processor's or any Authorized Person's systems or technical infrastructure, was lost with a low risk of potential harm or damage to Data Subjects.

1.9. "**Including**" and its derivatives (such as "include" and "includes") (whether or not capitalized) means "including, without limitation" unless expressly indicated otherwise.

1.10. "**Industry Standards**" means the then-current industry prevailing data protection and data processing practices relating to the Processing of the Personal Data.

1.11. **"International Data Transfer"** means any transfer of Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom, and includes any onward transfer.

1.12. "**Personal Data**" means any information relating to a Data Subject which Processor: (i) receives from or on behalf of Controller, or the Controller's Affiliates or (ii) accesses, for Processing in connection with the Services, and includes Sensitive Personal Information.

1.13. "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.14. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.15. "**Processor Affiliate**" means any entity that owns or controls, is owned or controlled by, or is under common control or ownership with Processor (where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by contract, exercise of voting rights, common management, or otherwise) and that assists or enables Processor to fulfill its obligations under the Agreement and Addendum.

1.16. "**Restricted Transfer**" means a transfer of Personal Data from the European Economic Area, United Kingdom or Switzerland to any country or recipient: (i) not deemed by the European Commission or the UK Information Commissioner's Office as providing an adequate level of protection for Personal Data, and (ii) not covered by or a suitable framework or certification recognized by the relevant Supervisory Authority as providing an adequate level of protection for Personal Data.

1.17. "**Sensitive Personal Information**" means a Data Subject's (including without limitation a Controller employee's, where applicable) (i) government-issued identification number (including social security number, driver's license number or state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; (iii) genetic, biometric or health data; (iv) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or sexual activity, or trade union membership; (iv) Personal Data relating to criminal convictions and offences (including commission of or proceedings for any offence committed or alleged to have been committed) and (v) any other Personal Data designated as sensitive or deserving of heightened protection under Applicable Laws.

1.18. "**Services**" shall have the meaning set forth in the Agreement.

1.19. "**Standard Contractual Clauses**" means the current clauses promulgated by the European Commission and UK Information Commissioner's Office for the transfer of personal data to processors established in third countries, and any successor clause as may be approved by Supervisory Authorities from time to time, with the options set forth here (as of November 1, 2021): set forth on https://floqast.com/wp-content/uploads/2022/02/FQ-SCC-Addendum.pdf .

1.20. "**Supervisory Authority**" means any other court, tribunal, or governmental or quasi-governmental entity or agency that has jurisdiction, under Applicable Law, over the Agreement or Addendum, the Personal Data or Processing, and/or Controller or Processor.

1.21. "**Technical and Organizational Security Measures**" means the measures taken by Processor and Authorized Persons as set out in Exhibit A, and as may be updated, varied or improved by the Processor from time to time, provided that the Processor shall ensure that any such updates, variations, or improvements provide no less security protection than those set out in Exhibit A

2. Processing of Data

2.1. Processor agrees to comply with this Addendum during the term of the Agreement. Any failure by Processor to comply with the obligations set forth in this Addendum, or any Personal Data Breach, will be considered a material breach of the Agreement, and Controller will have the right, without limiting any of the rights or remedies under this Addendum or the Agreement, or at law or in equity, to immediately terminate the Agreement for cause.

2.2. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Addendum 1 to this Addendum.

2.3. Processor acknowledges and agrees that it shall only Process Personal Data for the limited and specified purposes described in Addendum 1 and in compliance with the terms and conditions set forth in this Addendum.

2.4. Subject to Sections 2.4 and 2.5, the Processor shall process Personal Data only on documented instructions from the Controller which are set out in this Addendum or in the Agreement.

2.5. The Processor may process Personal Data other than in accordance with Section 2.3 if required to do so in order to comply with Applicable Law, in which case, the Processor shall inform the Controller of the relevant Applicable Law before it commences such Processing unless such Applicable Law prohibits the Controller from doing so;

2.6. The Processor shall not be required to comply with any instructions which would violate any Applicable Law; in which case, the Processor shall notify the Controller immediately of such Applicable Law.

2.7. Processor warrants that it will comply with all Applicable Laws.

3. Security of Data

3.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (collectively, "**Risks**"), Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data as set forth on Exhibit A.

3.2. Upon Controller's written request, or, upon the termination or expiration of the Agreement for any reason, Processor shall, and shall ensure that all Authorized Persons, (i) promptly and securely delete (in accordance with Exhibit A) or return to Controller in an encrypted format all copies of Personal Data, and (ii) promptly certify in writing to Controller when the measures described in subsection (i) hereof have been completed. Any disposal of Personal Data must ensure that such data is rendered permanently unreadable and unrecoverable. Processor and/or Authorized Persons shall be excused from performing the foregoing obligations only if, and solely to the extent that, Applicable Law(s) explicitly prevent them from doing so.

4. Authorized Persons

4.1. Controller acknowledges and agrees that Processor may in the future (i) engage Authorized Persons, including Subprocessors to access and Process Personal Data in connection with the Services and (ii) from time to time engage additional third Parties for the purpose of providing the Services, including without limitation the Processing of Personal Data.

4.2. The Controller acknowledges and agrees that the Processor currently uses the Authorized Subprocessors to access and Process Personal Data as set forth on Exhibit B, and hereby consents to the use of such Authorized Subprocessors. Processor may also retain any of its Affiliates to be subprocessors, and each Affiliate shall be deemed to be an Authorized Subprocessor.

4.3. Upon use of additional or replacement Subprocessors, Processor shall notify Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and shall give Controller the opportunity to object to the engagement of the new Subprocessors within 30 days after being notified. Controller may not unreasonably object to any proposed Subprocessor. If Processor and Controller are unable to resolve such objection, either Party may terminate the Addendum by providing written notice to the other Party; Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

4.4. If Controller does not object to the engagement of a third party in accordance with Section 4.2 after notice by Processor, such third party shall be deemed an Authorized Subprocessor for the purposes of this Addendum.

4.5. Processor shall ensure that all Authorized Subprocessors are subject to confidentiality obligations that prevent them from disclosing or otherwise Processing, both during and after their engagement by Processor, any Personal Data both during and after their engagement with Processor.

4.6. Processor shall ensure that every Authorized Subprocessor is subject to confidentiality obligations regarding the Processing of Personal Data that are no less protective than those to which Processor is subject under this Addendum.

4.7. Processor shall be liable to Controller for the acts and omissions of Authorized Subprocessors to the same extent that Processor would itself be liable under this Addendum had it conducted such acts or omissions.

5. Incident, and Personal Data Breach Notification

5.1. Processor shall notify Controller without undue delay upon becoming aware of an Incident or a Personal Data Breach and shall, in a written report, provide such information that is within the Processor's knowledge to reasonably enable Controller to comply with its obligations under Applicable Laws with respect to such Incident or Personal Data Breach. Such report will include, to the extent that the Processor is aware of such information (i) a description of the nature of the Incident or Personal Data Breach, (ii) the categories and approximate number of Data Subjects and Personal Data sets affected or alleged to be affected, (iii) the likely consequences of the Incident or Personal Data Breach, and (iv) any measures that have been or may be taken to address and mitigate the Incident or Personal Data Breach.

5.2. To the extent a Data Breach or Incident is caused by the Processor and/or any relevant Authorized Subprocessor, the Processor and/or Authorized Subprocessor shall use all reasonable endeavors to attempt to mitigate and remedy any Incident or Personal Data Breach, and prevent recurrence thereof, at Processor's own expense and in accordance with Applicable Laws.

5.3. Neither Processor nor any Authorized Subprocessor shall publicly disclose any information regarding any Incident or Personal Data Breach without Controller's prior written consent, *except that* Processor and any relevant Authorized Subprocessor may disclose any Suspected Incident, Incident or Personal Data Breach to (i) its own employees, advisors, agents, or contractors, or (ii) where and to the extent required by Applicable Laws, to applicable Supervisory Authorities and/or Data Subjects without Controller's prior written consent.

5.4. Processor shall, and shall use reasonable efforts to ensure that all relevant Authorized Subprocessors shall, at Processor's expense, reasonably cooperate with Controller and provide reasonable assistance necessary for Controller to comply with any obligations under Applicable Laws with respect to an Incident or Personal Data Breach, including obligations to report or notify an Incident or Personal Data Breach to Supervisory Authorities and/or Data Subjects.

6. Data Subject Rights

6.1. Subject to Clause 6.1, if required by Applicable Law of Processor, Processor shall assist the Controller using the technical and organizational measures made available via the Processor's platform at the time. Such assistance shall be provided strictly to the extent necessary to support Controller's response to requests by Data Subjects to exercise Data Subject Rights, including, specifically, a Data Subject's right under Applicable Law to: (a) confirm whether his or her Personal Data has been or is being Processed; (b) access a copy of all Personal Data of his or hers that has been or is being Processed; (c) rectify or supplement his or her Personal Data; (d) transfer his or her Personal Data to another Controller; (e) confirm that his or her Personal Data has been or is being subject to Processing that constitutes automated decision-making; (f) restrict or cease the Processing of his or her Personal Data; and (g) withdraw consent to the Processing of his or her Personal Data held by Processor or any Authorized Person.

6.2. To the extent that the Controller does not have the ability to respond to a request from a Data Subject using such technical and organizational measures, the Processor shall, if requested by the Controller, make commercially reasonable efforts to assist the Controller in responding to such Data Subject Rights, provided that the Controller shall be responsible for any reasonable costs or expenses arising from Processor's provision of any such assistance.

6.3. The Processor shall, without undue delay, notify Controller if Processor or an Authorized Subprocessor receives a request from a Data Subject to exercise Data Subject Rights) informing Controller in the event that Applicable Laws or any judicial, law enforcement, or Supervisory Authority operate to prevent Processor (or any Authorized Subprocessor) from performing the obligations described in this Section 6.3.

7. Transfers of Personal Data

7.1. Controller hereby authorizes Processor to perform International Data Transfers to any country subject to a valid adequacy decision of the Supervisory Authorities.

7.2. With respect to any International Data Transfers to any country that has not received a valid adequacy decision, the parties hereby agree to the Standard Contractual Clauses set forth at: URL.

7.3. The Parties acknowledge and agree that if in the future any Standard Contractual Clauses adopted by the Supervisory Authorities are updated, amended, or replaced, then the Parties shall enter into such updated, amended or replaced Standard Contractual Clauses with the Processor, pursuant to such notification (and, to the extent that the Standard Contractual Clauses provide for options, as determined Process).

7.4. All authorizations of International Data Transfers in this Section 7 are expressly conditioned upon Processor's ongoing compliance with the requirements of Applicable Laws applicable to International Data Transfers, and any applicable legal instrument for International Data Transfers. If such compliance is affected by circumstances outside of Processor's control, including circumstances affecting the validity of an applicable legal instrument, Controller and Processor will work together in good faith to reasonably resolve such non-compliance.

8. Actions and Access Requests.

8.1. Upon Controller's request, Processor shall reasonably make information available to Controller all information available to Processor and to Authorized Subprocessors to demonstrate compliance by Controller with its obligations under Applicable Laws (including in particular the GDPR, the UK GDPR or CCPA) relating to the Personal Data and the Processing conducted by Processor and Authorized Subprocessors.

8.2. Upon Controller's request, Processor shall provide all necessary assistance to Controller in connection with any Data Protection Impact Assessment that Controller must conduct or cause to be conducted in order to comply with Applicable Laws, to the extent that such DPIA(s) relate to the Processing.

8.3. Upon Controller's request, Processor shall provide all necessary assistance to Controller in connection with any consultation with a Supervisory Authority that Controller must undertake as a result of a DPIA, to the extent that such DPIA relates to the Processing.

8.4. Upon Controller's request, Processor shall provide all necessary assistance to Controller in the event of any investigation, action, or request made by a Supervisory Authority, to the extent that such investigation, action, or request relates to the Personal Data or the Processing.

8.5. Upon Controller's request, Processor shall provide Controller, and any Supervisory Authority with whom Controller is consulting or cooperating, with a designated contact for all queries and requests relating to the Processing of Personal Data.

8.6. In the event Processor determines that any Processing violates Applicable Laws (including the valid exercise of a Data Subject Right) or this Addendum, it shall immediately inform Controller and follow instructions for stopping such Processing and/or remediating the violation.

8.7. If so requested by Controller, Processor's reasonable costs (including compensation for time) and expenses for providing any of the assistance set forth in this Section 8 shall be reimbursable by Controller, due and payable thirty (30) days from invoice.

9. Records and Audit Rights

9.1. Processor shall maintain complete and accurate records in connection with Processor's performance under this Addendum, and shall retain such records for a period of three (3) years after the termination or expiration of the Agreement.

9.2. Upon Controller's written request and on at least 30 days' notice, Processor will provide Controller with documentation reasonably necessary to demonstrate Processor's compliance with this Addendum, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by Applicable Law, a duty of confidentiality, or any other obligation owed to a third party.

9.3. If required by the Supervisory Authority specific to Processor, Upon Controller's written request and on at least 30 days' notice, Processor shall permit an audit of its business operations provided: (a) the scope of the audit is limited solely to the subject matter required of the Supervisory Authority; (b) it takes place during Processor's normal business hours; (c) is completed on a timely basis; (d) Controller provides evidence of commercial general liability insurance of no less than $2,000,000 USD per occurrence naming Processor as an additional insured, waiving subrogation and worker's compensation insurance required by the authority having jurisdiction and employer's liability insurance of not less than $1,000,000 each

illness/injury; (e) the audit is conduced by the qualified third party subject to confidentiality obligations; (f) Controller is responsible for all costs of the audit, including, without limitation the time of all Processor personnel reasonably required to participate in the audit at a rate equal to twice their effectively hourly wage; (g) Processor shall not be obligated to conduct an audit of its business operations more than once per calendar month; (h) Controller may not initiate more than one audit per calendar year. Any foregoing requirements that are not permitted by Applicable Law shall not apply.

10. Limitation of Liability. The total liability of each of Controller and Processor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement. Any exclusions of liability set out in the Agreement shall also apply in respect of this Addendum.

11. California Consumer Privacy Act of 2018.

11.1. FloQast is a "Service Provider" as defined in CCPA Section 1798.140(v).

11.2. Customer discloses Personal Data to FloQast solely for: (i) a valid business purpose; and (ii) to permit FloQast to perform the Services.

11.3. FloQast is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data outside of the Addendum between FloQast and Processor.

11.4. FloQast understands the prohibitions outlined in Section 12.3.

12. Miscellaneous.

12.1. This Addendum will terminate simultaneously and automatically with the termination of the Agreement, except that all provisions intending to survive shall survive.

12.2. This Addendum may be amended or modified only by a writing signed by both Parties. Processor acknowledges and agrees that the Controller (whether it is acting as a controller or a processor on behalf of another controller) may disclose this Addendum to third parties (including other controllers, data subjects and regulators) for purposes of demonstrating compliance with Applicable Laws.

12.3. This Addendum shall be governed by the law of the same jurisdiction as the Agreement, except where and to the extent that Applicable Laws require that the Addendum be governed by the law of another jurisdiction.

Exhibit A

Security Measures

Processor will implement and maintain the security measures set out in this Exhibit A ("**Security Measures**"). Processor may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Architecture, Data Segregation, and Data Processing

The Service is operated within the AWS Cloud and is designed to segregate and restrict customer data access based on business need. The Service's systems are designed upon the principle of least privilege where logical components reside in segregated AWS VPCs separated by stateful AWS security group firewalls and stateless Network ACLs. The Service architecture additionally provides effective logical data separation by use of client specific unique identifiers.

FloQast has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by FloQast and its sub-processors.

Security Controls

The Service includes a variety of configurable security controls that allow FloQast customers to tailor the security of the Service for their own use. The FloQast system provides several access control roles based on the organizational structure of each individual customer. All FloQast application security controls abide by OWASP and NIST standards. The Service integrates with several Single Sign on Providers, and where applicable recommends use of Single Sign On authentication in their configuration of the Service's security settings.

Information Security Management Program ("ISMP")

FloQast maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of FloQast's business; (b) the amount of resources available to FloQast; (c) the type of information that FloQast will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

FloQast's ISMP is designed to:

- Protect the integrity, availability, and prevent the unauthorized disclosure by FloQast or its agents, of Customer Data in FloQast's possession or control;
- Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by FloQast or its agents;
- Protect against unauthorized access, use, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard information as set forth in any local, state or federal regulations by which FloQast may be regulated.

1. Security Standards. FloQast's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:

a. Internal risk assessments;

b. External pen testing;

c. NIST guidance; and

d. SOC1 Type II (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report") (FloQast will undergo its first SOC2 Type II audit in Quarter 3 of 2021, prior annual audits have been SOC1 Type 2).

2. Security Audit Report. FloQast provides its customers, upon their request, with a copy of FloQast's then-current Audit Report, including information as to whether the Security Audit revealed any material findings in the Service; and if so, the nature of each finding discovered.

3. Assigned Security Responsibility. FloQast assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:

a. Designating a security official with overall responsibility; and

b. Defining security roles and responsibilities for individuals with security responsibilities.

4. Relationship with Sub-processors. FloQast conducts reasonable due diligence and security assessments of sub-processors engaged by FloQast in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.

5. Background Check. Unless prohibited by applicable law, FloQast performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data.

6. Security Policy, Confidentiality. FloQast requires all personnel with access to Customer Data to acknowledge in writing, at the time of hire, that they will comply with the ISMP and protect all Customer Data at all times.

7. Security Awareness and Training. FloQast has mandatory security awareness and training programs for all FloQast personnel that address their implementation of and compliance with the ISMP.

8. Disciplinary Policy and Process. FloQast maintains a disciplinary policy and process in the event FloQast personnel violate the ISMP.

9. Access Controls. FloQast has in place policies, procedures, and logical controls that are designed:

a. To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;

b. To prevent personnel and others who should not have access from obtaining access; and

c. To remove access in a timely basis in the event of a change in job responsibilities or job status.

FloQast institutes:

a. Controls to ensure that only those FloQast personnel with an actual need-to-know will have access to any Customer Data;

b. Controls to ensure that all FloQast personnel who are granted access to any Customer Data are based on least-privilege principles;

c. Controls to require that user identifiers (User IDs) shall be unique and readily identify FloQast personnel to whom it is assigned, and no shared or group User IDs shall be used for FloQast personnel to access any Customer Data;

d. Password and other strong authentication controls that are made available to FloQast customers, so that customers can configure the Service to be in compliance with NIST guidance addressing locking out, uniqueness, reset, expiration, termination after a period of inactivity, password reuse limitations, length, expiration, and the number of invalid login requests before locking out a user; and

e. Periodic (no less than quarterly) access reviews to ensure that only those FloQast personnel with access to Customer Data still require it.

10. Physical and Environmental Security. FloQast maintains controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly- authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

a. Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;

b. Camera surveillance systems at critical internal and external entry points to the data center;

c. Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and

d. Uninterruptible Power Supply (UPS) modules and backup generators that provide back- up power in the event of an electrical failure.

11. Data Encryption.

a. Encryption of Transmitted Data: FloQast uses industry standard secure encryption methods to ensure all communications with the FloQast system is encrypted. All data is encrypted in transit using TLS 1.2 with ECDHE_RSA with P-256 as the key exchange and AES_128_GCM as the cipher.

b. Encryption of At-Rest Data: FloQast uses industry standard secure encryption methods designed to protect stored Customer Data at rest. FloQast utilizes transparent AWS EBS disk encryption, which uses the industry standard AES-256 encryption to secure all persisted live volume (disk) data. Encryption keys are managed by AWS KMS. Customer integration credentials, API keys and OAuth tokens are additionally encrypted at the application layer, using an application specific encryption key. Application level encryption employs the authenticated AES-256-CBC cipher.

c. Encryption of Backups: FloQast uses industry standard secure encryption methods designed to protect stored Customer Data at rest. FloQast utilizes transparent AWS EBS disk encryption, which uses the industry standard AES-256 encryption to secure all backup volume (disk) data. Encryption keys are managed by AWS KMS.

12. Disaster Recovery. FloQast maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

a. Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below

b. Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently annually;

c. RPO / RTO: Recovery Point Objective is no more than 1 hour and Recovery Time Objective is no more than 24 hours;

d. Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

13. Secure Development Practices. FloQast adheres to the following development controls:

a. Development Policies: FloQast follows secure application development policies, procedures, and standards that are aligned to industry-standard practices; and

b. Secure Design: FloQast employs a team of application architects and developers responsible for the secure design and instrumentation of application and cloud development practices. FloQast develops technologies which ensure all application teams develop the FloQast product in adherence to secure design practices.

c. Training: FloQast provides those employees who are responsible for secure application design, development, configuration, testing, and deployment of the FloQast application with external and internal security training relevant for their role.

14. Malware Control. FloQast employs industry-standard measures to test the Service to detect and remediate viruses, Trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service.

15. Data Integrity and Management. FloQast maintains policies that ensure the following:

a. Segregation of Data: The Service includes logical controls, including encryption, to

segregate each customer's Customer Data from that of other customers; and

b. Back Up/Archival: FloQast performs full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

16. Vulnerability Management. FloQast maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

a. Infrastructure Scans: FloQast performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis. FloQast installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

b. Application Scans: FloQast performs regular (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. Vulnerabilities are remediated on a risk basis. FloQast installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

c. External Application Vulnerability Assessment: FloQast engages third parties to perform network vulnerability assessments and penetration testing on an annual basis ("Vulnerability Assessment"). Reports from FloQast's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request.

Vulnerabilities are remediated on a risk basis. FloQast installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

17. Change and Configuration Management. FloQast maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

a. A process for documenting, testing and approving the promotion of changes into production;

b. A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c. A process for FloQast to perform security assessments of changes into production.

18. Secure Deletion. FloQast maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable NIST guidance and data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted using secure deletion methods including digital shredding of encryption keys and hardware destruction in accordance with relevant guidelines.

19. Intrusion Detection. FloQast monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. FloQast may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentication events, and to ensure that the Service functions properly.

20. Incident Management. FloQast has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by FloQast or its agents of which FloQast becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in FloQast's security incident response plan include:

a. Roles and responsibilities: formation of an internal incident response team with a response leader;

b. Investigation: assessing the risk the incident poses and determining who may be affected;

c. Communication: internal reporting as well as a notification process in the event of a Security Breach;

d. Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

e. Audit: conducting and documenting a root cause analysis and remediation plan.

FloQast typically notifies customers of significant system incidents by email to the listed admin contact, and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and FloQast's response.

21. Security Breach Management.

a. Notification: In the event of a Security Breach, FloQast notifies impacted customers of such Security Breach. FloQast cooperates with an impacted customer's reasonable request for information regarding such

Security Breach, and FloQast provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.

b. Remediation: In the event of a Security Breach, FloQast, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

22. Logs. FloQast provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. FloQast (i) backs-up logs on a daily basis, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with FloQast's data retention policy. If there is suspicion of inappropriate access to the Service, FloQast has the ability to provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.

Exhibit B

Authorized Subprocessors

Sub-Processors	
Name of Subprocessor and Location	**Nature of the Services**
FloQast Application-Related Sub-Processors	
Amazon Web Services - WA, US	Cloud Computing Services
Egnyte - CA, US	File and Email Hosting Services
MongoDB - NY, US	Hosting Services
Loggly - CA, US	Logging Services
Pendo.io - NC, US	User Analytics Services
Business-Related Sub-Processors	
FloQast UK Ltd - London, UK	Fully controlled FloQast, Inc. subsidiary providing Customer Support Services in EMEA
Google - CA, US	File and Email Hosting Services
WP Engine - TX, US	Hosting Services
Jira/Atlassian - Sydney, AU	Customer Support Services
Zendesk - CA, US	Customer Support Services
ZoomInfo - WA, US	Customer Support Services
Zoom - CA, US	Customer Support Services
Gong - CA, US	Customer Support Services
HubSpot - MA, US	Direct Marketing Services
Qualified - CA, US	Cloud Messaging Provider Services
Salesforce - CA, US	Customer Relationship Management Services
Influitive - Ontario, CA	Consumer Engagement Platform Services
Asana - CA, US	Project Management Services
NetSuite - TX, US	Billing and Accounting Services
MailChimp - GA, US	Transactional Email Services
SurveyMonkey - CA, US	Market Research Services
Skilljar - WA, US	LMS Hosting and Management Services