# QENCODE

## DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "***DPA***") is incorporated into and supplements the Agreement between the Customer and Qencode, Corp. ("***Qencode***"), or other agreement between the Customer and Qencode governing the Customer's use of the Services (the "***Agreement***") and reflects the parties' agreement with regard to the Processing of Customer Data. This DPA is an agreement between you and the entity you represent (the "***Customer***") and Qencode. In the course of providing the Services to the Customer pursuant to the Agreement, Qencode may Process Customer Data (as defined below) on behalf of the Customer and the parties agree to comply with the following provisions with respect to any Customer Data, each acting reasonably and in good faith.

**1. Definitions**.

"***Adequacy Decision***" means a country, territory, or sector within a country which has been subject to a finding, and continues to be subject to a finding for the duration of this Agreement, of an adequate level of protection for Personal Data under the GDPR or UK GDPR as applicable to the Personal Data Processing activity.

"***Affiliate***" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity, where "***control***" means, for the purposes of this definition, an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question.

"***Agreement***" means Qencode's Website Use Agreement, or other written electronic agreement, which govern the provision of the Services to the Customer, as such terms or agreement may be updated from time to time.

"***Customer Data***" means any Personal Data that Qencode Processes on behalf of the Customer via the Services, as more particularly described in this DPA.

"***Data Breach***" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Data.

"***Data Controller***" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"***Data Processor***" means any natural or legal person, public authority, agency, or any other body which Processes Personal Data on behalf of a Data Controller or on the instruction of another Data Processor acting on behalf of a Data Controller.

"***Data Protection Laws***" means all applicable laws and regulations relating to the Processing of Personal Data and privacy that may exist in the relevant jurisdictions, including, where applicable, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the "***GDPR***"); Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019 (the "***UK GDPR***"); the California Consumer Privacy Act ("***CCPA***"); the Canadian Personal Information Protection and Electronic Documents Act ("***PIPEDA***"); the Brazilian General Data Protection Law ("***LGPD***"), Federal Law no. 13,709/2018; the Privacy Act 1988 ("***Cth***") of Australia, as amended ("***Australian Privacy Law***"); and any other privacy laws or regulations applicable to the Processing of Customer Data under the Agreement.

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

"***EU Standard Contractual Clauses***" means: (a) the standard contractual clauses adopted by the European Commission on 4th June 2021 for the transfer of Personal Data to third countries pursuant to the EU GDPR and where "MODULE TWO: Transfer controller to processor" therein is selected and applies where relevant; or (b) such other standard contractual clauses that are approved by the European Commission for Controller to Processor transfers of EU Personal Data to a third country which has not received an Adequacy Decision (and are subsequently incorporated into this Agreement);

"***Personal Data***" means any information relating to an identified or identifiable living individual, including information that can be linked, directly or indirectly, with a particular Data Subject.

"***Process***", "***Processing***" or "***Processed***" means any operation or set of operations which is performed upon Customer Data whether or not by automated means, according to the definitions given to such terms in the GDPR.

"***Restricted Transfer***" means a transfer of Personal Data to a country, a territory, or specified sector within a country that (but for the operation of this DPA): (a) has not been granted an Adequacy Decision; or (b) is not subject to any safeguards or derogations that would permit the transfer of the Personal Data to the country, territory, or sector in accordance with the GDPR or UK GDPR (as applicable to the Personal Data transfer).

"***Sensitive Data***" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences.

"***Services***" means all services provided by Qencode in accordance with, and as defined in, the Agreement.

"***Standard Contractual Clauses***" means (a) the EU Standard Contractual Clauses, (b) UK Standard Contractual Clauses, or (c) such other standard contractual clauses that are approved under applicable Data Protection Laws and apply to a Restricted Transfer of Personal Data under this Agreement.

"***Sub-processor***" means any sub-contractor engaged in the Processing of Customer Data in connection with the Services.

"***Supervisory Authority***" means any regulatory, supervisory, governmental, or other competent authority with jurisdiction or oversight over compliance with the Data Protection Laws.

"***UK Standard Contractual Clauses***" means: (a) the standard contractual clauses approved by the European Commission for the transfer of Personal Data from a Controller to a Processor (document reference number 2010/87/EU) for which references to the Directive 95/46/EC of 24 October 1995 therein shall be deemed to be replaced with respective provisions of the UK GDPR; or (b) such other standard contractual clauses that are approved under the UK GDPR for the transfer of UK Personal Data to a third country which has not received a UK Adequacy Decision (and are subsequently incorporated into this Agreement).

**2. <u>Appointment and Data Processing</u>.**

***2.1*** Subject to the terms of the Agreement, the Customer is the sole Data Controller of the Customer Data or has been instructed by and obtained the authorization of the relevant Data Controller(s) to enter into this DPA in the name and on behalf of such Data Controller(s). The Customer is responsible for obtaining all of the necessary authorizations and approvals to enter, use, provide, store, and Process Customer Data to enable Qencode to provide the Services.

***2.2*** The Customer, as the Data Controller, hereby appoints Qencode as the Data Processor in respect of all Processing operations required to be carried out by Qencode on Customer Data in order to provide the Services in accordance with the terms of the Agreement.

***2.3*** Qencode shall Process Customer Data, as further described in Annex A of this DPA, only in accordance with the Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing. The parties agree that the Agreement, including this DPA, along with the Customer's configuration of or use of any settings, features, or options in the Service (as the Customer may be able to modify from time to time) constitute the Customer's complete and final instructions to Qencode in relation to the Processing of Customer Data (including for the purposes of the Standard Contractual Clauses), and Processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

***2.4*** The Customer will ensure that Qencode's Processing of the Customer Data in accordance with the Customer's instructions will not cause Qencode to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Qencode shall promptly notify the Customer in writing, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any data Processing instruction from the Customer violates Data Protection Laws.

***2.5*** The Customer will not provide (or cause to be provided) any Sensitive Data to Qencode for Processing under the Agreement, and Qencode will have no liability whatsoever for Sensitive Data, whether in connection with a Data Breach or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

***2.6*** The Customer represents and warrants that (a) on an ongoing basis, there is, and there will be throughout the term of the Agreement, a legal basis for the Processing by Qencode of the Customer Data on behalf of the Customer in accordance with this DPA and the Agreement (including any and all Documented Instructions issued by the Customer from time to time in respect of such Processing); and (b) it will honor the rights of Data Subjects pursuant to Data Protection Laws. The Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which the Customer acquired Customer Data.

***2.7*** Except as expressly set forth in the Agreement and in this DPA, Qencode will not collect, use, retain, disclose, sell, or otherwise make Customer Data available for Qencode's own commercial purposes.

***2.8*** Qencode will maintain complete, accurate, and up to date written records of all Processing activities carried out on behalf of the Customer containing information required under any applicable Data Protection Laws.

**3. Sub-processors**.

***3.1*** The Customer acknowledges and agrees that Qencode may engage Sub-processors to Process Customer Data on the Customer's behalf. Qencode has entered into and will maintain a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the services provided by such Sub-processor.

***3.2*** The Sub-processors currently engaged by Qencode and authorized by the Customer, as of the execution of this DPA, are available here: https://cloud.qencode.com/qencode-list-sub-processors.pdf. Qencode shall notify the Customer of any proposed amendment(s) to the list of the Sub-processors (including any addition or any replacement to the list). The Customer shall notify Qencode within thirty (30) days of the date of its receipt of Qencode's notice whether it accepts the amendment(s) to the list of Sub-processors or whether it has any objections, in which case, the parties will meet to discuss the Customer's objections, acting reasonably and in good faith. If Qencode cannot reasonably accommodate a solution to the Customer's objection, then the Customer may terminate the Agreement and this DPA, by notice to Qencode. If the Customer does *not* object to the proposed change(s) within thirty (30) days of the date of its receipt of Qencode's, notice, then the amendment(s) proposed in the notice and the use of the new Sub-processor will be deemed accepted by the Customer.

***3.3*** Qencode will remain responsible for any acts or omissions of its Sub-processors to the same extent that Qencode would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

**4. Authorized Personnel**. Qencode shall ensure that all persons authorized to Process Customer Data are made aware of the confidential nature of Customer Data and have committed themselves to confidentiality (e.g., by confidentiality agreements) or are under an appropriate statutory obligation of confidentiality.

**5. Security Responsibilities**.

***5.1*** 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, Qencode shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, but not limited to, the security measures attached hereto in Annex B (the "***Security Measures***").

***5.2*** Qencode shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate: (a) the pseudonymization and encryption of Customer Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and (d) a Process for regularly testing, assessing, and evaluating the effectiveness of security measures.

***5.3*** The Customer is responsible for reviewing the information made available by Qencode relating to data security and making an independent determination as to whether the Service meets the Customer's requirements and legal obligations under Data Protection Laws. The Customer acknowledges that the Security Measures are subject to changes, from time to time, to reflect technological developments and industry best practices; *provided, always*, that such changes do not result in any objective degradation to the security of Customer Data, the manner in which the Services are provided, or which fall below the standard of any applicable law.

***5.4*** Notwithstanding the above, the Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials (if and as applicable), protecting the security of Customer Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to Qencode in connection with the Services.

**6. Data Breach Provisions**.

***6.1*** If Qencode becomes aware of a Data Breach, Qencode shall, without undue delay, (a) notify the Customer of the Data Breach; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Data Breach.

***6.2*** In the event of a Data Breach, Qencode shall provide the Customer with all reasonable assistance in dealing with the Data Breach, in particular in relation to making any notification to a Supervisory Authority or any communication to Data Subject. In order to provide such assistance, and taking into account the nature of the Services and the information available to Qencode, the notification of the Data Breach shall include, at a minimum, the following:

(a) A description of the nature of the Data Breach including the categories and approximate number of data records concerned;

(b) The likely consequences of the Data Breach; and

(c) The measures taken or to be taken by Qencode to address the Data Breach, including measures to mitigate any possible adverse consequences; and

***6.3*** Where, and insofar as, it is not possible for Qencode to provide such information at the time of the notice, then such notice shall nevertheless be made, in as complete a form as possible, and the remaining required information may be provided by Qencode, in phases and as it shall become available, without undue delay.

***6.4*** The Customer agrees that Qencode's obligation to report or respond to a Data Breach under this Section is not and will not be construed as an acknowledgement by Qencode of any fault or liability of Qencode with respect to the Data Breach.

**7. <u>Data Quality, Retrieval, Return, and Deletion</u>**.

***7.1*** Qencode will update, correct, or delete Customer Data on the Customer's request. Qencode will not collect or Process Customer Data beyond what is necessary to comply with the Customer's instructions and perform the Services on the Customer's behalf.

***7.2*** Upon termination of the Agreement (in whole or in part) or earlier upon the Customer's request, and at Customer's choice, Qencode will, unless any applicable law, competent court, Supervisory Authority, or regulatory body prevents Qencode from returning or destroying Customer Data: (a) destroy all Customer Data Processed and any copies thereof and certify to the Customer on request that Qencode has done so; or (b) if requested by the Customer, return all Customer Data Processed and the copies thereof to the Customer or another recipient identified by the Customer. If the Customer does not request the return of Customer Data within thirty (30) days following termination of the Agreement, Qencode shall destroy all Customer Data in accordance with <u>Section 7.2(a)</u> above.

***7.3*** On request from the Customer, Qencode will provide a portable copy of the Customer Data in accordance with the Data Protection Laws with respect to Personal Data.

**8. <u>Audits</u>**.

***8.1*** At the Customer's written request, Qencode will, not more than once annually, allow an audit to verify Qencode's compliance with obligations under Data Protection Laws and this DPA, to be carried out either (a) by an independent third party audit firm bound by a duty of confidentiality selected by the Customer and approved by Qencode (which approval will not unreasonably be withheld or delayed) and where applicable, in agreement with the competent Supervisory Authority, or (b) by a competent government authority. The audit will be carried out in close cooperation with Qencode's Data Protection Officer or Chief Information Security Officer. The parties will agree on the

scope of the audit in advance. The Customer will notify Qencode in writing with a minimum of 15 business days (in the country where the audit will be conducted) prior to any audit being carried out. The Customer will bear the costs of the audit unless the audit uncovers compliance deficits that are material, in which case Qencode will reimburse the Customer for the costs of the audit. If the Customer requests Qencode to incur out-of-pocket costs to assist the Customer in the audit, then Qencode is entitled to a reasonable, pre-approved reimbursement for its costs of the audit incurred by Qencode, to be paid by the Customer only if the audit does not uncover compliance deficits that are material.

***8.2*** Qencode will monitor and self-audit its own compliance with its obligations under Data Protection Laws and this DPA and will provide the Customer, upon written request, with periodic reports, no more than once annually, unless a prior audit revealed noncompliance or more frequent audits are required by law or a regulatory body.

***8.3*** In addition to the foregoing, Qencode shall respond to all reasonable requests for information made by the Customer to confirm Qencode's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon the Customer's written request to Qencode, provided that the Customer shall not exercise this right more than once annually.

**9. Assistance on Data Protection Impact Assessment**. To the extent required under applicable Data Protection Laws, Qencode will (taking into account the nature of the Processing and the information available to Qencode) provide all reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with any Supervisory Authorities, as required by such Data Protection Laws. Qencode shall comply with the foregoing by: (a) complying with Section 8; (b) providing the information contained in the Agreement, including this DPA; and (c) if the foregoing clauses (a) and (b) are insufficient for the Customer to comply with such obligations, upon request, providing additional reasonable assistance (at the Customer's expense).

**10. International Transfers**.

***10.1*** The Customer acknowledges that Qencode may transfer and Process Customer Data to and in the United States and anywhere else in the world where Qencode or its Sub-processors maintain Processing operations. Qencode will, at all times, ensure that such transfers are made in compliance with the requirements of all applicable Data Protection Laws.

***10.2*** The EU Standard Contractual Clauses shall apply to the transfer of Customer Data from the Customer acting the data exporter to Qencode acting as the data importer where the transfer of Customer Data is a Restricted Transfer to which the EU GDPR applies. The information required for the purposes of the Annexes of the EU Standard Contractual Clauses is provided in Annex A and Annex B respectively. For the purposes of the EU Standard Contractual Clauses, the laws of Ireland shall govern.

***10.3*** The UK Standard Contractual Clauses shall apply to the transfer of Customer Data from the Customer acting the data exporter to Qencode acting as the data importer where the transfer of Customer Data is a Restricted Transfer to which the UK GDPR applies. The information required for the purposes of the Appendices of the UK Standard Contractual Clauses is provided in Annex A and Annex B respectively. For the purposes of the UK Standard Contractual Clauses, the laws of England and Wales shall govern.

***10.4*** The parties agree and acknowledge the applicable Standard Contractual Clauses are incorporated into this Agreement, without further need for reference, incorporation, or attachment and that by accepting or by executing the Agreement the parties are deemed to have executed the applicable Standard Contractual Clauses. The parties agree that the applicable Standard Contractual

Clauses shall be directly binding between Qencode as the data importer (as defined therein) and the Customer as the data exporter (as defined therein) in relation to such Processing.

***10.5*** To the extent Qencode adopts another lawful mechanism for the transfer of Customer Data that is not described in this DPA ("***Alternative Transfer Mechanism***"), the Alternative Transfer Mechanism will apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism is approved by the appropriate Supervisory Authority). In addition, if and to the extent that a court of competent jurisdiction or Supervisory Authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Customer Data (within the meaning of applicable Data Protection Laws), Qencode may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of Customer Data.

**11. Data Subject Requests and Other Communications**.

***11.1*** Qencode shall, to the extent required by the Data Protection Laws, promptly notify the Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under the applicable Data Protection Laws. Qencode will advise the Data Subject to submit their request to the Customer and the Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

***11.2*** Qencode shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights (regarding information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under the Data Protection Laws.

**12. Permitted Disclosures of Customer Data**.

***12.1*** Qencode may disclose Customer Data to the extent such data is required to be disclosed by law, by any government or Supervisory Authority, or by a valid and binding order of a law enforcement agency (such as a subpoena or court order), or other authority of competent jurisdiction.

***12.2*** If any law enforcement agency government or Supervisory Authority sends Qencode a demand for disclosure of the Customer Data, then Qencode will attempt to redirect the law enforcement agency, government, or Supervisory Authority to request that data directly from the Customer and Qencode is entitled to provide the Customer's basic contact information to such law enforcement agency, government, or Supervisory Authority.

***12.3*** If compelled to disclose Customer Data pursuant to Section 12.1, then Qencode will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy.

**13. CCPA**. For purposes of the CCPA, the definitions of: "***Data Controller***" includes "***Business***"; "***Data Processor***" includes "***Service Provider***"; "***Data Subject***" includes "***Consumer***"; "***Personal Data***" includes "***Personal Information***"; in each case as defined under the CCPA. Qencode is a Service Provider and Customer is a Business. Qencode, as a Service Provider, will not (a) Sell Customer Data (as the term is respectively defined in the CCPA), or (b) retain, use, or disclose Customer Data for any purposes other than for the specific purposes set forth in the Agreement and this DPA. For the avoidance of doubt, Qencode will not Process Customer Data outside of the direct business relationship between Qencode and Customer. Qencode hereby certifies that it understands the restrictions and obligations set forth in this Section and will comply with them.

**14.** **Liability; Limitations**. Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA shall be subject to the exclusions and limitations of liability set forth in the Agreement to the extent permitted by applicable Data Protection Laws. Any claims made against Qencode or its Affiliates under or in connection with this DPA shall be brought solely by the Customer entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

**15.** **Relationship with the Agreement**.

***15.1*** This DPA shall remain in effect for as long as Qencode carries out Customer Data Processing operations on behalf of the Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7 above).

***15.2*** This DPA supersedes and replaces all prior representations, understandings, communications, and agreements by and between the Parties in relation to Customer Data and the matters set forth in this DPA.

***15.3*** In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the Standard Contractual Clauses; then (b) this DPA; and then (c) the Agreement.

***15.4*** Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

***15.5*** No one other than a Party to this DPA, its successors, and permitted assignees shall have any right to enforce any of its terms.

***15.6*** This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

# ANNEX A

## Details of Data Processing

**Subject Matter:** The subject matter of the Processing under this DPA is Customer Data.

**Duration of the Processing:** Qencode will Process Customer Data for the term of the Agreement plus the period until Qencode deletes all Customer Data in accordance with the Agreement or as otherwise required by applicable law.

**Nature and Purpose of the Processing:** The nature and purpose of the transfer and Processing of Customer Data is to (a) provide the Services to Customer and fulfil Qencode's obligations under the Agreement; (b) provide customer support to Customer and its end users; and (c) compliance with applicable law.

**Categories of Data Subjects:** The Customer Data transferred concern individuals about whom Personal Data is provided to Qencode via the Services by (or at the direction of) the Customer or the Customer's end users.

**Categories of Personal Data:** The data transferred is the Customer Data uploaded, submitted, or otherwise provided to Qencode by the Customer in connection with the Services, the extent of which is typically determined and controlled by the Customer in its sole discretion.

**Sensitive Data:** The Customer will not provide (or cause to be provided) any Sensitive Data to Qencode for Processing under the Agreement.

**Frequency of the Transfers:** The frequency of the transfer of Customer Data will be on a continuous basis for the duration of the Agreement.

**Subject Matter, Nature, and Duration of Processing by Sub-processors:** The subject matter and nature of the Processing by Sub-processors are specified in this Annex A. The duration of the Processing carried out by Sub-processors will be until the termination or expiration of the Agreement or as requested by Customer.

**Competent Supervisory Authority:** The Customer's competent Supervisory Authority will be determined in accordance with the GDPR.

# ANNEX B

## SECURITY MEASURES

**1. Servers and Networking**.

***1.1*** All servers that run Qencode software in production are recent, continuously patched Linux systems. Additional hosted services that we utilize, such as are comprehensively hardened.

***1.2*** Qencode's web servers encrypt data in transit using the strongest grade of HTTPS security (TLS 1.2) so that requests are protected from eavesdroppers and man-in-the-middle attacks. Our SSL certificates are 2048 bit RSA, signed with SHA256.

***1.3*** Internal tier-to-tier requests are signed and authenticated to prevent request forgery, tampering, and replay.

**2. Storage**. All persistent data is encrypted at rest using the AES-128 standards or similarly high standards.

**3. Employee Equipment and Employee Access**.

***3.1*** Qencode employee computers have strong passwords, encrypted disks, and firewalls.

***3.2*** Qencode follows the principle of least privilege in how it writes software as well as the level of access employees are instructed to utilize in diagnosing and resolving problems in the Qencode software and in response to customer support requests.

***3.3*** Access to administrative interfaces additionally enforce administrator permissions where applicable, and all administrative access is logged and auditable both in the form of traditional web server logs as well as via Qencode itself to make it easy to find and review any administrative activities with full fidelity.

**4. Code Reviews and Production Signoff**.

***4.1*** All changes to source code destined for production systems are subject to pre-commit code review by a qualified engineering peer that includes security, performance, and potential-for-abuse analysis.

***4.2*** Prior to updating production services, all contributors to the updated software version are required to approve that their changes are working as intended on staging servers.

**5. Service Levels, Backups, and Recovery**. Qencode's infrastructure utilizes multiple and layered techniques for increasingly reliable uptime, including the use of autoscaling, load balancing, task queues and rolling deployments. Due to the very large amount of data that Qencode stores, Qencode does not currently make point-in-time backups, although Qencode does use highly redundant data stores and/or rapid recovery infrastructure, making unintentional loss of received data due to hardware failures very unlikely.

**6. Product Security**.

***6.1*** Product security is of paramount importance at Qencode. Qencode uses a software development lifecycle in line with general Agile principles. When security effort is applied throughout the Agile release cycle, security oriented software defects are able to be discovered and addressed more rapidly than in longer release cycle development methodologies. Software patches are released

as part of Qencode's continuous integration process. Patches that can impact end users will be applied as soon as possible but may necessitate end user notification and scheduling a service window.

***6.2*** Qencode performs continuous integration. In this way, Qencode is able to respond rapidly to both functional and security issues. Well defined change management policies and procedures determine when and how changes occur. This philosophy is central to DevOps security and the development methodologies that have driven Qencode adoption. In this way, Qencode is able to achieve extremely short mean time to resolution for security vulnerabilities and functional issues alike. Qencode is continuously improving our DevOps practice in an iterative fashion.

**7.** **Corporate Security**. All Qencode personnel undergo regular security and privacy awareness training that weaves security into technical and non-technical roles; all employees are encouraged to participate in helping secure our customer data and company assets. Security training materials are developed for individual roles to ensure employees are equipped to handle the specific security oriented challenges of their roles

**8.** **Client and Server Hardening**.

***8.1*** Exposed server endpoints are recurrently tested for vulnerabilities using multiple types of scanning software as well as manual testing. Request-handling code paths have frequent user re-authorization checks, payload size restrictions, rate limiting where appropriate, and other request verification techniques. All requests are logged and made searchable to operations staff.

***8.2*** Client code utilizes multiple techniques to ensure that using the Qencode application is safe and that requests are authentic, including:

(a) IFRAME sandboxing;

(b) XSS and CSRF protection;

(c) signed and encrypted user auth cookies; and

(d) remote invalidation of extant sessions upon password change/user deactivation

**9.** **API and Integrations**. All access to Qencode REST API endpoints require an access key that can be regenerated on demand by customers.

**10.** **Customer Payment Information**. Qencode uses Stripe, Inc. for payment processing and do not store any credit card information. Stripe is a trusted, Level 1 PCI Service Provider.

**11.** **Incident Reporting and Ongoing Improvements**. Qencode encourages users to submit vulnerability reports. If you have a security concern or are aware of an incident, please send an email to security@qencode.com.