Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into by and between Content Square SAS on behalf of itself and its Affiliates (as defined below), including Hotjar Limited and Heap Inc. ("**Contentsquare**"), and [Vendor Name] ("**Vendor**") on behalf of itself and its Affiliates. Contentsquare and Vendor will hereafter be jointly referred to as the "**Parties**", and individually as the "**Party**".

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to Contentsquare's agreement with the Vendor (the "**Agreement**").

1. Definitions

In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth opposite each one of them:

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of at least fifty percent (50%).

1.2. "**Applicable Data Protection Law(s)**" means all applicable data protection, privacy and electronic marketing legislation, including the GDPR, CCPA, UK GDPR (the Data Protection Act 2018), the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Personal Data Protection Act ("PDPA") as well as any equivalent laws anywhere in the world - to the extent any such laws apply to Controller Personal Data to be processed hereunder by Processor.

1.3. "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer (as defined in the CCPA), which is processed by Vendor solely on behalf of Contentsquare, under this DPA and the Agreement between Vendor and Contentsquare.

1.4. "**Sensitive Personal Data**" is a subset of Personal Data, which due to its nature has been classified by applicable law or by Contentsquare as deserving additional privacy and security protection. Sensitive Personal Data consists of, in particular:

1.4.1. all government-issued identification documents and numbers (including Social Security numbers, driver's license numbers, and passport numbers);
1.4.2. all financial information, including any consumer, trading or spending habits, and any account numbers (bank and non-bank financial services account numbers, credit/debit card numbers, and other information if that information would permit access to a financial account);
1.4.3. any Personal Data pertaining to the categories specified in Articles 9-10 of the GDPR;
1.4.4. all employee, employment candidate and payroll information and data; and
1.4.5. any other Personal Data designated by Contentsquare as Sensitive Personal Data.

1.5. "**GDPR**" means EU General Data Protection Regulation 2016/679 and any subsequent amendments, replacements or supplements; The terms, "**Commission**", "**Data Subject**", "**Member State**", "**Personal Data Breach**", "**Special Categories of Data**", "**Process/Processing**", "**Controller**", "**Processor**", and "**Supervisory Authority**" shall have the same meanings given to them in the GDPR (or where the same or similar terms are used under another Applicable Law, the meanings given to such terms under such Applicable Law.

1.6. "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq, as amended, including by the California Privacy Rights Act, and any regulations issued thereto. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CCPA.

1.7. "**EU SCCs**" means the standard contractual clauses for the transfer of personal data pursuant to the European's Commission decision (EU) 2021/914 of 4 June 2021, as may be amended or replaced.

1.8. "**Controller to Processor SCCs**" means the standard contractual clauses for the transfer of personal data from controller to processor (module two) pursuant to the European's Commission decision (EU) 2021/914 of 4 June 2021, as may be amended or replaced.

1.9. "**Processor to Processor SCCs**" means the standard contractual clauses for the transfer of personal data from processor to processor (module three) pursuant to the European's Commission decision (EU) 2021/914 of 4 June 2021, as may be amended or replaced.

1.10. "**SCCs**" or "**Standard Contractual Clauses**" means together (i) the "EU SCCs", and (ii) the "U.K. SCCs" means the International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the U.K. Data Protection Act 2018, as amended from time to time.

1.11. "**Sub-Processor**" means any third party engaged directly by the Vendor to process any Personal Data pursuant to or in connection with the Vendor Services. The term shall not include employees or contractors of Vendor.

1.12. "**Customer Personal Data**" means the Personal Data of a Contentsquare Customer.

1.13. "**Vendor Services**" means any services provided by Vendor to Contentsquare, including, without limitation, any storage, software or platform services, pursuant to an agreement, purchase order, license or subscription.

2. Subject Matter

In the course of providing the Vendor Services to Contentsquare and its Affiliates, pursuant to the Agreement, the Vendor and its Affiliates may Process Contentsquare's Personal Data (which may include Customer Personal Data) on behalf of Contentsquare and its Affiliates. The Vendor agrees to comply with the provisions set out in this Addendum, as well as with Applicable Data Protection Laws with respect to any of Contentsquare's Personal Data, which is submitted by or for Contentsquare and its Affiliates to the Vendor Services, and/or is otherwise collected and Processed on behalf of or for the benefit of Contentsquare and its Affiliates by the Vendor and its Affiliates.

3. Scope of Processing

3.1. Vendor shall process Personal Data as described in **Annex 1** (*Details of Processing of Personal Data*) attached hereto. Other than with respect to Customer Personal Data (to the extent applicable), Vendor shall process Personal Data as a Data Processor ('Service Provider' as such is defined under the CCPA to the extent applicable) acting on behalf of Contentsquare as the Controller ('Business' as such is defined under the CCPA to the extent applicable) of such Personal Data. With respect to Customer Personal Data (to the extent applicable), Vendor shall process Customer Personal Data as a Sub-Processor ('Sub-Contractor' as such is defined under the CCPA to the extent applicable) acting on behalf of Contentsquare as the Processor of such Customer Personal Data.

3.2. Contentsquare hereby instructs Vendor to process Personal Data only for the limited purposes of providing Vendor Services and solely for the benefit of Contentsquare, including the pursuit of 'business purposes' as under the CCPA.

3.3. Vendor shall only process the Personal Data in accordance with, (i) the terms of this DPA, (ii) the terms of the existing agreement between the Parties, (iii) solely on Contentsquare's documented instructions, unless processing is required by Applicable Data Protection Laws, and (iv) in compliance with all Applicable Data Protection Laws.

3.4. Vendor shall notify Contentsquare without undue delay if Vendor determines that it can no longer meet Contentsquare's instructions or its obligations under this DPA.

3.5. Vendor acknowledges and confirms that it does not receive or process any Personal Data as consideration for any services or other items that Vendor provides to Contentsquare under the Agreement. Vendor shall not have, derive, or exercise any rights or benefits regarding Personal Data Processed on Contentsquare's behalf, and may retain, use, and disclose Personal Data solely for the purposes for which such Personal Data was provided to it, as stipulated in the Agreement and this DPA. Vendor represents and warrants that it understands the rules, requirements and definitions of the CCPA. Vendor agrees to refrain from selling or sharing (as such terms are defined in the CCPA) any Personal Data Processed hereunder,

without Contentsquare's prior written consent, nor taking any action that would cause any transfer of Personal Data to or from Vendor under the Agreement or this DPA to qualify as "selling" or "sharing" such Personal Data under the CCPA. Vendor shall not retain, use, or disclose Personal Data outside of the direct business relationship between the Parties to the Agreement, nor combine Personal Data that Vendor receives from, or on behalf of, Contentsquare with Personal Data that Vendor receives from, or on behalf of, another person or persons, or collects from its own interaction with the data subject, except where permitted under law. Contentsquare may, upon notice, take reasonable and appropriate steps to stop and remediate Vendor's unauthorized use of Personal Data.

4. Sub Processing

4.1. Vendor shall not subcontract any processing of Personal Data to any third party without a prior written consent of Contentsquare regarding each such subcontracting activity and third party.

4.2. Vendor shall ensure that the arrangement between the Vendor and the Sub Processor is governed by a written contract binding on the Sub Processor, which requires a Sub Processor to process Personal Data in accordance with this DPA. Contentsquare may object to the engagement of any Sub Processor at its sole and absolute discretion. In such case, Vendor shall not engage a Sub Processor for the provision of Vendor Services to Contentsquare, or Contentsquare may terminate or suspend its agreement with Vendor without penalty.

4.3. Where the Sub Processor fails to fulfill its obligations, Vendor shall remain fully liable to Contentsquare for the performance of that Sub Processor's obligations.

5. Vendor Personnel

5.1. Vendor shall conduct an appropriate background investigation of all employees or contractors ("**Vendor Personnel**") of Vendor who may have access to Personal Data, prior to allowing them such access. If the background investigation reveals that the Vendor Personnel are not suited to access Personal Data, then Vendor shall not provide the Vendor Personnel with access to the Personal Data.

5.2. Vendor shall ensure that all Vendor Personnel: (i) has such access only as necessary for the purposes of providing Contentsquare with Vendor Services and complying with Applicable Data Protection Laws; (ii) is contractually bound to confidentiality requirements no less onerous than this DPA; and (iii) is provided with appropriate privacy and security training.

5.3. Upon request, Vendor shall provide to Contentsquare a list of all individual employees and contractors (including former individual employees and contractors) who have (or have had) access to the Personal Data.

6. Security

6.1. The Vendor shall implement technical and organizational measures described in Annex 2 to ensure a level of security appropriate to the risk presented by the processing of Personal Data.

6.2. The Vendor shall keep records of its processing activities performed on behalf of Contentsquare, which shall include at least:

6.2.1. the details of the Vendor as Personal Data Processor, any representatives, Sub Processors, data protection officers and Vendor Personnel having access to Personal Data;

6.2.2. the categories of Processing activities performed;

6.2.3. information regarding cross-border data transfers, if any; and

6.2.4. description of the appropriate technical and organizational security measures implemented in respect of the processed Personal Data.

6.3. Upon request, Vendor shall provide copies of any existing relevant external information security certifications, audit report summaries and/or other documentation reasonably required by Contentsquare to verify Vendor's compliance with this DPA.

6.4. With reasonable prior notice, Contentsquare (or its appointed independent third-party auditor) may carry out an inspection of the Vendor's applicable controls, including, where applicable, an inspection of its facilities for the purposes of verifying Vendor's compliance with this DPA, or, where Contentsquare has reasonable concerns about Vendor's data protection compliance following i) a Personal Data Breach, ii) a request from a regulator or data protection authority, or iii) a material gap or deficiency identified in Vendor's answers to Vendor's security questionnaire.

7. Data Subject Rights

7.1. Vendor shall reasonably assist Contentsquare in responding to requests to exercise Data Subject rights under Applicable Data Protection Laws, including EU Data Protection Laws, including to opt-out of the sale of Personal Data, or the right not to be discriminated against for exercising any CCPA Consumer rights.

7.2. Vendor shall:

7.2.1. promptly notify Contentsquare if it receives a request from a Data Subject in respect of Personal Data;

7.2.2. provide full cooperation and assistance in relation to any complaint or request from a Data Subject regarding the Processing of Personal Data; and

7.2.3. ensure that it does not respond to that request except per the documented instructions by Contentsquare or as strictly required by Applicable Data Protection Laws to which the Vendor is subject;

7.2.4. maintain electronic records of complaints or requests from Data Subjects seeking to exercise their rights (under Applicable Data Protection Laws).

8. Legal Disclosure and Personal Data Breach

8.1. Vendor shall notify Contentsquare within 24 hours of Vendor becoming aware of:

8.1.1. any request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

8.1.2. any actual or suspected Personal Data Breach affecting Personal Data. Vendor shall provide Contentsquare with sufficient information to allow Contentsquare to meet any obligations to report or inform Data Subjects or Data Protection authorities of the Personal Data Breach under the Applicable Data Protection Laws. Other than as required by law, Vendor shall not make any public statements or other disclosures about a Personal Data Breach affecting Personal Data without Contentsquare's prior written consent, which may be provided at Contentsquare's discretion on a case by case basis, outside the signing of this DPA.

8.2. Vendor shall provide Contentsquare with the following details, as possible:

8.2.1. the nature of the Personal Data breach including the categories of Data Subjects concerned and the categories of Personal Data and data records concerned;

8.2.2. the measures proposed or taken by Vendor in cooperation with Contentsquare to address the Personal Data Breach;

8.2.3. the measures Contentsquare could take to mitigate the possible adverse effects of the Personal Data Breach;

8.3. Vendor shall take any actions necessary to investigate any suspected or actual Personal Data Breach and mitigate any related damages.

8.4. Vendor shall cooperate with Contentsquare and take such steps as are directed by Contentsquare to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Deletion or Return of Personal Data

9.1. Upon Contentsquare's written request or the expiration or termination of the provision of Vendor Services, Vendor shall promptly delete or return all copies of Personal Data, at Contentsquare's choice, except as required to be retained in accordance with Applicable Law.

9.2. Upon Contentsquare's prior written request, the Vendor's Data Protection Officer (or equivalent) shall provide written certification to Contentsquare that it has fully complied with this Section 9.

10. Data Protection Impact Assessment and Prior Consultation

10.1. Vendor shall provide cooperation and assistance to Contentsquare with any data protection impact assessments, and with prior consultations with a Supervisory Authority of Contentsquare and its Affiliates, which Contentsquare reasonably considers to be required under Applicable Data Protection Laws. The scope of such assistance shall be limited to the Processing of the Personal Data by Vendor.

11. Audit Rights

11.1. Vendor shall make available to Contentsquare, upon prior written request, all information necessary to demonstrate compliance with this DPA, including industry-standard third-party audit certifications.

11.2. Once annually or upon a security incident, Vendor shall allow for and contribute to audits, including inspections, by a reputable auditor mandated by Contentsquare. The scope, duration and methods of such audit will be determined by both parties in good faith. In any event, a third-party auditor shall be subject to confidentiality obligations.

12. Cross-Border Data Transfer

12.1. Vendor may transfer Personal Data only to such countries as shall be identified and agreed under **Annex 1** ("Approved Countries").

12.2. Personal Data may be transferred from Approved Countries which are part of the EU Member States, EEA member countries (collectively, "EEA") to Approved Countries that offer adequate levels of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, any Member States or the European Commission without any further safeguard being necessary ("Adequate Countries").

12.3. To the extent that Personal Data and/or Customer Personal Data is transferred from EEA to Approved Countries that are not deemed Adequate Countries, the following shall apply:

12.3.1. If Vendor is self-certified to the Data Privacy Framework and the Personal Data and/or Customer Personal Data transferred is within the scope of such certification, the DPF shall apply. Where the DPF does not apply to the Approved Countries, or the Vendor determines that it can no longer provide at least the same level of protection for such Personal Data and/or Customer Personal Data as is required by the DPF Principles, then the SCCs shall apply and be automatically incorporated into this DPA.

12.3.2. The parties agree that the SCCs (including Annexes I and II) shall be incorporated by reference where applicable and form an integral part of this DPA. Each party is deemed to have executed the SCCs by executing the Agreement incorporating this DPA. With respect to the SCCs, the following shall apply:

a) Contentsquare shall be the "data exporter" and Vendor shall be the "data importer";
b) Module Two of the EU SCCs shall apply to the extent that Contentsquare is a Data Controller and Module Three shall apply to the extent that Contentsquare is a Data Processor. The same shall apply with respect to Table 2 of the U.K. SCCs;
c) The optional Clause 7 of the EU SCCs shall apply and Affiliate(s) of both Contentsquare and Vendor may accede to the EU SCCs under the same terms, where applicable. The foregoing shall apply with respect to table 2 of the U.K. SCCs;
d) For purposes of Clause 9 of the EU SCCs, Option 1 ("Specific prior authorization") shall apply and the time period to submit the request for specific authorization Sub-processors prior to

the engagement of Sub-processors shall be thirty (30) days, and the same shall apply with respect to Table 2 of the U.K. SCCs;

e) The optional language in Clause 11 of the EU SCCs shall not apply;
f) For purposes of Clause 17 and Clause 18 of the EU SCCs, the Member State for purposes of governing law and jurisdiction shall be France. Part 2, Section 15(m) and Part 2, Section 15(n) of the U.K. SCCs regarding Clause 17 and Clause 18 of the EU SCCs shall apply;
g) The description of transfer of the EU SCCs and Table 3 of the U.K. SCCs shall be populated with the relevant information set out at Annex 1 (Details of Processing of Personal Data), Annex 2 (Technical Security and Organizational Measures) and Section 4 (Sub-Processing) to this DPA;
h) For the purposes of Annex I, Part C of the EU SCCs, the French Data Protection Authority will be the competent supervisory authority;
i) The measures set forth in Annex 2 (Technical Security and Organizational Measures) of this DPA will serve as Annex III of the EU SCCs;
j) The list referenced in Annex 1 of this DPA will serve as Annex III of the EU SCCs;
k) With respect to Table 4 of the U.K. SCCs, either the data exporter or data importer may terminate the U.K. SCCs prior to termination of the Agreement and this DPA.

12.3.3. Where Vendor determines that it can longer comply with its obligations under the DPF and the SCCs or use another valid transfer mechanism to safeguard the Restricted Transfer, Vendor shall notify Contentsquare immediately and work with Contentsquare to take reasonable and appropriate steps to remediate the non-compliance.

12.4. Where, and to the extent that, Vendor transfers Personal Data to a Sub-Processor listed in **Annex 1** and which is not located in Adequate Countries, the Vendor agrees to enter into Processor to Processor SCCs with the aforesaid Sub-Processor.

12.5. Where, and to the extent that, the SCCs are applicable pursuant to Section 12.3, if there is any conflict between this Agreement and the SCCs, the SCCs shall prevail.

12.6. For transfers from Switzerland or other countries that adopted and/or has determined the EU SCCs are adequate for Restricted Transfers, references in the EU SCCs shall be interpreted to include applicable terminology for those territories (e.g. 'Member State' shall be interpreted to mean 'Switzerland' for transfers from Switzerland).

12.7. Personal Data may be transferred from Australia (if agreed as an Approved Country) for processing by Vendor or Sub-Processor on its behalf who has declared to comply with the principles enshrined in the Australian Privacy Act 1988 or under other circumstances, in which the Data Subject has provided explicit consent.

12.8. Contentsquare may object to the transfer of Personal Data under this Section 12 on certain privacy and security grounds. In such case, Vendor shall not effectuate the transfer of Personal Data, or Contentsquare may terminate or suspend the provision of Vendor Services with immediate effect without penalty.

12.9. In any event, Vendor shall provide Contentsquare with all relevant information to enable Contentsquare to comply with its obligations in case of cross-border transfers.

13. Indemnification

13.1. Notwithstanding anything else to the contrary under the Agreement, Vendor shall indemnify, defend, and hold harmless Contentsquare, its Affiliates and their officers, directors, and employees, without limitation or cap, from and against all claims and proceedings and all liability, loss, costs, fines, and expenses (including reasonable legal fees), arising in connection with:

13.1.1. Vendor's unlawful or unauthorized Processing, destruction of, or damage to, any Personal Data;

13.1.2. Vendor's (including the Vendor Personnel) failure to comply with its obligations under this DPA, the existing agreement, any applicable law or any further instructions as to such Processing given in writing by Contentsquare in accordance to this DPA.

14. Miscellaneous

14.1. **Severance:** Should any provision of this DPA be determined invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

14.2. **Notice:** All notices required under this DPA shall be sent to Contentsquare by e-mail to: privacy@Contentsquare.com. Notices to Vendor shall be sent to: [Vendor Email]

14.3. **Order of Precedence:** In the event of any conflict between the terms of this DPA and other documents binding on Parties, the terms of these documents will be interpreted according to the following order of precedence: (i) Contentsquare's Privacy Policy; (ii) this DPA; (iii) terms of agreement, purchase order, license or subscription, pursuant to which Vendor's Services are provided.

15. Sanction

It is acknowledged by the Parties that in any case that a Party infringes any provision of an applicable Data Protection Laws, it may be subject to penalties and administrative fines, which may include, without limitation, concerning the GDPR, such administrative fines referred to paragraphs 4, 5 and 6 of Article 83. If applicable, the aforesaid administrative fines issued against either Party shall be subject to the conditions set out in the Section 13.

IN WITNESS WHEREOF, this DPA is entered into and becomes binding between the Parties with effect from the date first set out above.

Vendor: [Vendor Name]

Signature: _____

Name: _____

Title: _____

Date: _____

Content Square SAS

Signature: _____

Name: _____

Title: _____

Date: _____

Annex 1: Details of Processing of Personal Data

This **Annex 1** includes certain details of the processing of Personal Data.

Controller: Content Square SAS

Processor: _____

Description of Vendor Services: _____

Duration of the processing: _____

The nature and purpose of the processing: _____

Types of personal data processed: _____

Categories of data subjects: _____

Approved Countries: _____

List of sub-processors in the following format:

Name of Sub-Processor	Services Performed	Sub-Processor Location	Purpose of Processing	DPA with Sub-Processor? (Yes or No)

Annex 2

Technical Security and Organizational Measures

Vendor must implement the below Security Requirements in its systems, processes and policies, and ensure the applicability of these Security Requirements upon any of its third party providers.

All capitalized terms not defined in the Definitions provision below, shall have the meanings set forth in the Supplier Standards or the Agreement.

1. **Organization of information security**
    a. Vendor shall appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s), with responsibility and accountability for information security within the organization.
    b. Vendor shall ensure that all information security responsibilities are defined and allocated in accordance with Vendor's approved policies for information security. Such policies shall be published and communicated to employees and relevant external parties.
    c. Vendor shall have a risk management framework and conduct a yearly risk assessment of its environment and Systems to understand its risks and apply appropriate controls to manage and mitigate risks before offering its services.
2. **Human resources security**
    a. Vendor shall inform its personnel about relevant security procedures and their roles and ensure that personnel with access to any Systems and/or Scoped Data are subject to written confidentiality obligations.
    b. Vendor shall further inform its personnel of possible consequences of breaching Vendor's security policies, procedures and these Security Requirements, which must include disciplinary action and the ability to terminate the contract with such employee or third party provider upon such breach.
    c. Vendor personnel with access to any Systems and/or Scoped Data shall receive annual training covering these Security Requirements, additional privacy and security procedures that may be applicable to the services provided, prevention of unauthorized use or disclosure of Scoped Data and response to any Information Security Incidents.
    d. Vendor shall perform relevant and appropriate background checks on any of its personnel and third party providers with access to any Systems and/or Scoped Data, all in compliance with Applicable Laws and Regulations.
3. **Asset Management**
    a. Assets associated with any Systems and/or Scoped Data, including Vendor's information processing facilities shall be identified, and an inventory of these assets shall be maintained. Such inventory shall be provided to Contentsquare upon request.
    b. Vendor shall classify, categorize, and/or tag Scoped Data to help identify it and to allow for access to it to be appropriately restricted.
4. **Access control**
    a. Vendor shall restrict access to Scoped Data and Systems at all times solely to those individual personnel and third party providers whose access is essential to the Performance under the Agreement.
    b. Vendor shall immediately suspend or terminate the access rights to Scoped Data and Systems for any Vendor's personnel or third party providers suspected of breaching any of

the provisions of these Security Requirements or any Applicable Laws; and Vendor shall remove access rights of all employees or any third party providers immediately upon suspension or termination of their employment, contract, or agreement.

c. Vendor shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Scoped Data and/or Systems. Vendor shall use an enterprise access control system that requires its personnel and third party providers revalidation by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

d. Vendor shall maintain and update a record of personnel and third party providers authorized to access the Systems or any Scoped Data and Vendor shall review users' access rights at least every 6 months.

5. **Physical and Environmental Security**
   a. Vendor shall limit access to offices, where Scoped Data is processed, to authorized individuals and use a variety of industry standard systems to protect against loss of data.
6. **Operations security**
   a. Vendor shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to any Systems and/or Scoped Data and to its systems and networks. Vendor shall ensure the policies are communicated to all its personnel and third party providers involved in the processing or have access to any System or Scoped Data.
   b. The standards and procedures shall meet or exceed industry best practices and applicable regulations and laws, and include, without limitation: security controls; identification and patching of security vulnerabilities; change control process and procedures; problem management; and incident detection and management.
   c. Vendor shall maintain logs of administrator and operator activity and data recovery events
7. **Communication security and data transfer**
   a. Vendor shall, at a minimum, use the following controls to secure its networks which store or process Scoped Data:
      Network traffic shall pass through firewalls, which are monitored at all times. Vendor must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.
      Access to network devices for administration must utilize a minimum of 256-bit, industry standard encryption.
      Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 8 characters, upper case, lower case, numeral, special character).
      Initial user passwords are required to be changed during the first log-on. Vendor shall have a policy prohibiting the sharing of user IDs and passwords.
      Firewalls must be deployed to protect the perimeter Scoped data.
   b. When remote connectivity is required for processing of Scoped Data, Vendor shall use VPN servers for the remote access with the following or similar capabilities:
      Connections must be encrypted using a minimum of 256-bits encryption.
      The use of multi -factor authentication is required.
   c. Vendor shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to these Security Requirements. Such policies shall be designed to protect transferred information from interception, copying, modification, corruption, mis-routing and destruction.
8. **System Acquisition, Development, and Maintenance**

a. Vendor shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.
b. Vendor will perform annual penetration test on their internet perimeter network.
c. Vendor shall respond promptly to all reasonable security audit, scanning, discovery, and testing reports requested from Contentsquare, or from regulators (to the extent required by law) and shall cooperate and assist those regulators as required by law.
d. If any audit or penetration testing exercise referred to above reveals any deficiencies, weaknesses or areas of non-compliance, Vendor shall promptly take such steps as may be required to remedy those deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable in the circumstances.
e. Vendor shall keep Contentsquare informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Contentsquare as soon as may be practicable in the circumstances that all remedial actions have been completed.

9. Management of Information Security Incidents and Improvements

a. Vendor shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.
b. Vendor shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as possible. All Vendor employees and third party providers should be made aware of their responsibility to report Information Security Incidents as quickly as possible.
c. Vendor shall maintain a record of Information Security Incidents with a description of the incident, the consequences of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to correct future security incidents.

10. Information Security Aspects of Business Continuity Management

a. Vendor shall maintain emergency and contingency plans for the facilities in which Vendor information systems that process Scoped Data are located. To ensure that they are valid and effective during adverse situations, Vendor shall verify the established and implemented information security continuity controls at regular intervals.
b. Vendor's redundant storage and its procedures for recovering data shall be designed to reconstruct Scoped Data in its original state from before the time it was lost or destroyed.

11. Notification and Communication Obligations

a. Vendor shall immediately (i.e., within 48 hours) notify ContentSquare's security team (security@contentsquare.com) if any of the following events occur:
    any Information Security Incident or compromise of any System or Scoped Data;
    an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of information that is processed, stored and transmitted using a computer in connection with Scoped Data;
    failure or inability to maintain compliance with these Security Requirements or Applicable Laws