DATA PROTECTION AND SECURITY AGREEMENT

This Data Protection and Security Agreement ("DPSA") made this _____, 2026 ("Effective Date") by and between OMH-HealthEdge Holdings, Inc., d/b/a Omega Healthcare Management Services, on behalf of itself and its subsidiaries (collectively, the "Controller"), and _____ (the "Processor") (together, the "Parties").

WHEREAS, Controller engages the Processor to provide certain services involving the Processing of Personal Data on its behalf; and other confidential information Processed in connection with the Services.[1] The Parties intend for this DPSA to establish a unified framework governing privacy, data protection, information security, and related compliance requirements

WHEREAS, the Parties seek to ensure that the Processing of Personal Data is performed in compliance with applicable Data Protection Laws; and

WHEREAS, this DPSA applies to the extent the Vendor Processes Personal Data or otherwise has access to such information in connection with the Services. If the Vendor does not Process Personal Data under the Agreement, only the provisions relating to information security, confidentiality, and incident response shall apply.

NOW, THEREFORE, the Parties agree as follows:

1. **Definitions.** Capitalized terms used herein have the meanings assigned to them in Data Protection Laws. In addition:

    1.1. **"Agreement"** means the agreement between the Parties governing the Services (e.g., master services agreement, purchase order form, statement of work, etc.), including schedules and all amendments thereto.

    1.2. **"Confidential Information"** means all non-public information disclosed by or on behalf of Omega to the Vendor, whether orally, visually, electronically, or in writing, including business, technical, financial, operational, customer, patient, or employee information; Personal Data; proprietary models, workflows, or systems; security information; and any information that is designated as confidential or that a reasonable person would understand to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information includes all data the Vendor accesses, stores, transmits, or processes on behalf of Omega, whether hosted in Covered Systems or Vendor systems.

    1.3. **"Covered Systems"** means any information systems, applications, networks, platforms, cloud environments, endpoints, or computing resources owned, operated, leased, managed, or otherwise used by Omega or its clients, including any systems that store, transmit, or process Confidential Information.

    1.4. "**Data Protection Laws**" means the data protection, privacy, and security laws that apply to the Processing of Personal Information under this Agreement, including the European Union General Data Protection Regulation ("GDPR"), the UK GDPR, Indian Digital Personal Data Protection Act ("DPDPA") 2023, Colombian Law 1581 of 2012, Philippines Data Privacy Act of 2012 (RA 10173), and applicable U.S. federal or state privacy laws.

    1.5. **"Personal Information"** or **"Personal Data"** means information relating to an identified or identifiable individual, including any information defined as "personal

[1] Capitalized terms herein shall have the same definitions as those provided in the Agreement unless otherwise defined herein.

information" or "personal data" under applicable Data Protection Laws. Personal Information does not include de-identified or aggregated information.

1.6. "**Primary Agreement**" means the agreement between the Parties governing the Services, including any statements of work, order forms, schedules, or similar documents incorporated into or executed under that agreement, and all amendments thereto.

1.7. **"Processing," "Process," "Processed,"** and **"Personal Data Breach"** have the meanings assigned under applicable Data Protection Laws.

1.8. "**Restricted Transfer**" means any transfer or remote access of Personal Data originating from the EEA, Switzerland, United Kingdom, India, Colombia, or Philippines to a country or territory that is not subject to an adequacy decision or its functional equivalent under applicable Data Protection Laws.

1.9. "**Subprocessor**" means any third party engaged by Vendor or Processor to perform Processing of Personal Data on behalf of Omega.

1.10. **"Vendor"** means "Processor", and is the counterparty to Omega under the Agreement that provides the Services and, to the extent it Processes Personal Data on Omega's behalf, acts as the Vendor under this DPSA.

2. Privacy Requirements

2.1 **Scope; Order of Precedence.** This DPSA supplements the Agreement. If there is any conflict between this DPSA and the Agreement, this DPSA controls for privacy, data protection, international transfers, and information security. The technical and organizational controls required of Vendor are set forth in the Security Measures attached to and incorporated into this DPSA as Exhibit A (the **"**Security Measures"). If the Parties have entered into a Business Associate Agreement ("BAA"), the BAA controls in the event of any conflict relating to the use, disclosure, safeguarding, or handling of Protected Health Information ("PHI") as required under the Health Insurance Portability and Accountability Act and its related rules and regulations ("HIPAA"). For all other information that is not PHI, the more protective requirement among the BAA, this DPSA, Exhibit A, and the Agreement shall apply.

2.2 **Compliance with Data Protection Laws.** Processor shall comply with all applicable Data Protection Laws in its Processing of Personal Data. Controller remains responsible for determining the lawful basis for Processing and for ensuring that Personal Data is collected and provided to Processor in compliance with applicable law.

2.3 **U.S. Service Provider/Contractor.** Processor will act as a "service provider"/"contractor" (as applicable) under U.S. state privacy laws. Processor will not sell or share Personal Information, use it for cross-context behavioural advertising, or retain, use, or disclose it for purposes other than performing the Services or as otherwise permitted by law or Omega's documented instructions. Vendor will not combine Personal Information except as permitted by applicable law and this DPSA.

2.4 **Omega Instructions from the Controller.** Processor shall Process Personal Data solely on documented instructions from Controller, including with respect to any transfer of Personal Data to a third country, except where Processing is required by applicable law. If Processor believes an instruction would violate Data Protection Laws or is required to disclose Personal Data under a legal obligation, it shall promptly notify Controller unless prohibited by law. Controller's documented instructions include the Primary Agreement, this DPSA, and any additional written instructions.

2.5 **Transfer and Location of Processing.** Controller authorizes Processor to Process Personal Data within the United States, India, Colombia, or Philippines, as applicable, and as necessary to provide the Services. Processor shall ensure that all Personal Data is stored within the United States, India, Colombia, or Philippines, as applicable, unless Controller provides prior written consent for storage in another jurisdiction. For clarity, remote access to Personal Data from locations outside the original geography in which it was collected or provided shall be considered Processing outside of the original geography, and may occur only where expressly authorized in writing by Controller and performed through secure, original geography-hosted environments that maintain appropriate technical and organizational safeguards. Where Controller provides such consent, Processor shall conduct all Processing consistent with the Primary Agreement, this DPA, applicable Data Protection Laws, and Controller's documented instructions.

2.6 **Restricted Transfers.** To the extent that Personal Data originating from the EEA, Switzerland, United Kingdom, India, Colombia or Philippines, as applicable, is accessed from or transferred to a location outside those jurisdictions that does not benefit from an adequacy decision or functional equivalent, such access or transfer shall constitute a Restricted Transfer under Data Protection Laws. Where a Restricted Transfer occurs, the Parties shall implement an appropriate and lawful transfer mechanism recognized under Data Protection Laws.

2.7 **Authorization.** Vendor shall not engage any Sub-processor without Omega's prior written consent. Omega may withhold or condition consent at its sole discretion.

2.8 **Due Diligence and Oversight.** Before allowing any Sub-processor to access Personal Data, Vendor shall perform documented privacy and security due diligence, including reviewing the Sub-processor's technical and organizational measures. Vendor shall monitor Sub-processor compliance on an ongoing basis, including through periodic assessments or audits, and promptly report any material non-compliance to Omega together with corrective actions taken.

2.9 **Flow-Down Requirements.** Vendor shall impose flow-down requirements on each Sub-processor, by written agreement.

3. **Security Requirements.** Processor shall implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, consistent with Article 32 of the GDPR, the DPDP, and good industry practice. Such measures shall include, at a minimum: access controls; authentication and authorization management; encryption of Personal Data in transit and at rest; network and system security controls, including vulnerability management and timely patching of critical systems; logging and monitoring; incident detection and response procedures; secure development practices; backup and recovery processes; and ongoing employee security and privacy training. Processor shall also comply with all terms contained in the most current version of the Omega Healthcare Management Services Vendor Security Requirements Addendum attached hereto. Processor shall regularly assess and validate the effectiveness of its security measures, including through internal assessments or independent third-party audits or certifications, including routine vulnerability assessment penetration testing. At Controller's request, Processor shall make available high-level documentation regarding such security measures, which may include SOC 2, ISO 27001, or equivalent certifications or reports. Processor shall ensure that any changes to its security measures do not materially reduce the level of protection afforded to Personal Data.

3.1 **Confidentiality.** Processor shall restrict access to Personal Data and Confidential Information to those personnel who require such access to perform the Services and shall ensure that such personnel are bound by written confidentiality obligations that survive the termination of their engagement. Processor shall ensure that all authorized

personnel receive appropriate training regarding the handling and protection of Personal Data and Confidential Information and are instructed to Process such information only in accordance with Omega's instructions and this DPSA. Vendor shall implement access controls and role-based permissions designed to ensure that only authorized personnel may access Personal Data and Confidential Information and shall periodically review such access rights.

3.2 **Information Security Program and Security Measures.** Processor shall maintain a written information security program that complies with industry standards and is reasonably designed to protect the confidentiality, integrity, and availability of Personal Data and Confidential Information. Such program shall align with widely recognized frameworks such as ISO 27001, the NIST Cybersecurity Framework, or CIS Controls, and shall include administrative, technical, and physical safeguards appropriate to the nature of the Processing. Processor shall implement and maintain technical and organizational measures consistent with Article 32 of the GDPR and at least those set out in the Security Measures. Processor shall ensure that all Subprocessors comply with the Security Measures. Processor shall not materially reduce the Security Measures without Omega's prior written consent. In the event of any conflict between the Security Measures described in this DPSA and Exhibit A, the more protective requirement shall apply.

3.3 **Security Incidents and Breach Notification.**

a. **Personal Data Breach.** Processor shall notify Omega without undue delay and in any event within seventy-two (72) hours after becoming aware of a Personal Data Breach, and in the case of the India-based PII, within six (6) hours under the DPDP. The notification shall include, to the extent reasonably available: (i) the nature of the Personal Data Breach, including the categories and approximate number of affected Data Subjects and records; (ii) the name and contact details of a point of contact at Processor; (iii) the likely consequences of the Personal Data Breach; and (iv) the measures taken or proposed to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Processor shall not notify any third party, including any supervisory authority or affected individuals, about a Personal Data Breach without Omega's prior written consent unless such notification is required by applicable law. Where notification to a third party is required by applicable law, Processor shall, where legally permitted, provide Omega with a copy of the proposed notification and consider any reasonable comments from Omega prior to making such notification.

b. **Security Breach of Confidential Information.** For any actual or reasonably suspected breach of security, confidentiality, or privacy affecting Confidential Information (including non-Personal Data), Processor shall notify Omega at legal@omegahms.com and compliance.QA@omegahms.com within twenty-four (24) hours after becoming aware of such breach and in the case of the India-based PII, within six (6) hours under the DPDP. Processor shall cooperate with Omega on investigation, containment, and mitigation, provide a written response plan for Omega's review, and, where applicable, permit Omega to observe discussions with regulators related to the incident to the extent permitted by law. The process and additional requirements for Security Incidents are further described in the Security Measures and shall be read as supplementing, and not limiting, this Section 3.3.

3.4 **Cloud Providers.** If Processor uses any cloud service provider to Process or store Personal Data or Confidential Information, Processor shall ensure such provider maintains security controls substantially equivalent to those required under this DPSA and the Security Measures and that appropriate written contractual obligations are in

place to protect such information, including confidentiality, security, incident notification, and audit rights (directly or via Processor).

3.5 **Testing, Vulnerability Management, and Patch Management.** Processor shall implement vulnerability management, testing, and patch management practices consistent with industry standards and, at a minimum, as set forth in the Security Measures. Without limiting the Security Measures, Processor shall conduct regular vulnerability scanning and periodic penetration testing of systems that Process Personal Data or Confidential Information and shall remediate identified vulnerabilities in accordance with the timeframes specified in the Security Measures or, where not specified, within commercially reasonable timeframes based on severity.

3.6 **Security Posture Changes.** Processor shall promptly notify Omega of any material changes to its information security program, Security Measures, subcontractor security posture, or hosting environment that could reasonably be expected to adversely affect the security of Personal Data or Confidential Information or Processor's ability to meet its obligations under this DPSA.

3.7 **Independent Assessments and Certifications.** Processor shall obtain, maintain, and renew, as applicable, independent third-party security assessments or certifications appropriate to the nature of the Services (for example, SOC 2 Type II, ISO 27001 certification or surveillance audits, or equivalent assurances). Upon Omega's reasonable request, Processor shall provide a summary of such assessments or certifications or relevant reports, which may be redacted to remove confidential commercial information not relevant to Processor's compliance with this DPSA.

3.8 **Assurance and Audit.** Processor shall maintain documentation necessary to demonstrate compliance with this DPSA and the Security Measures. Upon reasonable notice, Processor shall make available to Omega information reasonably necessary to verify such compliance, which may include summary security reports, SOC 2, ISO 27001, or equivalent certifications, results of relevant third-party assessments, and high-level descriptions of its information security program. Where such documentation is insufficient, or where there is a reasonable indication of non-compliance, Omega (or its designated auditor, bound by confidentiality) may conduct or mandate an audit, including an inspection of relevant facilities and systems, subject to reasonable scheduling, confidentiality obligations, and Processor's security requirements. Audits shall be conducted in a manner that minimizes disruption to Processor's operations. The Parties shall cooperate in good faith to agree on the scope and timing of any audit.

3.9 **Offshoring and Remote Access.** Processor shall not Process, Store, or Transfer Confidential Information outside the United States without Omega's advance written consent for the specific location and Processing, and any such offshoring shall be governed by a written offshore plan agreed by the Parties. Remote access to U.S.-hosted systems containing Personal Data or Confidential Information from locations outside the United States requires Omega's prior written approval and must comply with this DPSA, the Security Measures, and any additional requirements specified in the applicable offshore plan.

3.10 **Access Protocols.** Processor shall restrict access to Personal Data to those personnel who require such access to perform the Services and shall ensure that such personnel are bound by written confidentiality obligations that survive the termination of their engagement. Processor shall ensure that all authorized personnel receive appropriate training regarding the handling and protection of Personal Data and are instructed to Process Personal Data only in accordance with this DPSA, applicable privacy laws and Controller's instructions. Processor shall implement multifactor authentication ("MFA"), access controls and role-based permissions designed to

ensure that only authorized personnel may access Personal Data and shall periodically review such access rights.

4. **Sub-processors.** Controller agrees that Processor may engage Sub-processors in connection with the provision of the Services, consistent with the Primary Agreement, unless otherwise restricted therein. Processor shall remain responsible for the acts and omissions of all Sub-processors to the same extent as if such Processing were undertaken directly by Processor. Processor shall provide Controller, upon request, with a current list of Sub-processors involved in the Processing of Personal Data. Processor shall notify Controller in advance of any intended addition or replacement of a Sub-processor where the Primary Agreement requires such notice, and Controller may object on reasonable data-protection grounds. The Parties shall work in good faith to address any such objection.

5. **Sub-processor Obligations.** Where Processor engages a Sub-processor to carry out specific Processing activities on behalf of Controller, Processor shall impose on the Sub-processor, through a written contract or other binding legal instrument, data protection obligations that provide a level of protection for Personal Data no less protective than those required under this DPA and applicable Data Protection Laws. Each Sub-processor must provide sufficient guarantees to implement appropriate technical and organizational measures so that the Processing meets the requirements of Data Protection Laws. Processor shall conduct reasonable due diligence on each Sub-processor prior to allowing it to Process Personal Data, including an assessment of the Sub-processor's security controls and privacy practices. Processor shall monitor Sub-processor compliance on an ongoing basis, and where Processor becomes aware of a material failure by a Sub-processor to meet the requirements of this DPA, Processor shall promptly notify Controller and take appropriate corrective action, which may include suspension or termination of the Sub-processor's Processing. Processor shall remain fully liable for the performance of each Sub-processor's obligations.

6. **Data Subjects' Requests.** Processor shall implement and maintain technical and organizational measures necessary to enable Controller to respond to Data Subject requests under applicable Data Protection Laws, including requests to access, correct, delete, restrict Processing of, or port Personal Data. If Processor receives a Data Subject request directly, it shall notify Controller without undue delay and in any event within five (5) business days. Processor shall not respond to any Data Subject request except on Controller's written instructions or where required by law, in which case Processor shall notify Controller prior to responding unless prohibited by law. Controller is responsible for determining whether any exemptions or restrictions apply to a Data Subject's request.

7. **Recordkeeping.** Processor shall maintain records of Processing activities as required under Data Protection Laws and shall make such records available to Controller upon request to the extent necessary for Controller to comply with an inquiry or request from a supervisory authority. As part of this obligation, Processor shall maintain information regarding the categories of Personal Data Processed, the purposes of Processing, the categories of Data Subjects, Sub-processor involvement, data disclosures or transfers, and the technical and organizational measures used to protect Personal Data.

8. **Cooperation.** Processor shall provide reasonable assistance to Controller in connection with Controller's compliance obligations under Data Protection Laws, including with respect to Data Protection Impact Assessments, consultations with supervisory authorities, and assessments related to security or cross-border transfers. Processor shall make available information reasonably necessary to support such assessments, considering the nature of the Processing and the information available to Processor.

9. **Government and Third-Party Requests.** If Processor receives a request, subpoena, warrant, or other legal or regulatory demand that may require disclosure of Personal Data, Processor shall promptly notify Controller, unless legally prohibited, and shall provide Controller with a copy of the request where permitted. Processor shall cooperate with Controller's efforts to limit,

challenge, or protect against such disclosure to the extent reasonably possible and permitted by law. Processor shall not disclose Personal Data in response to such requests unless required by law.

10. **Retention.** Processor shall retain Personal Data only for as long as necessary to perform the Services or as required under applicable law. Processor shall implement data retention controls to ensure that Personal Data is not maintained longer than necessary for Processing activities conducted under the Primary Agreement. Where retention is required by law, Processor shall continue to apply appropriate safeguards to such Personal Data.

11. **Return and Deletion or Return.** Upon Controller's written election, Processor shall return or securely delete all Personal Data at the termination or expiration of the Services and shall instruct its Sub-processors to do the same. Processor shall delete any remaining copies unless retention is required by applicable law. Upon request, Processor shall provide written confirmation of the completion of such deletion.

12. **De-identified Data.** Processor shall not attempt to re-identify any de-identified, aggregated, or anonymized data that Omega provides or that Processor derives in connection with the Services. Processor may not create de-identified or aggregated data using Personal Data except as expressly permitted by the Agreement or Omega's written instructions.

13. **Inability to Comply.** Processor shall promptly notify Omega if Processor determines that it can no longer meet its obligations under this DPSA or Data Protection Laws. Upon such notice, Omega may require Processor to take reasonable and appropriate steps to stop or remediate the non-compliant Processing.

14. **Data Segregation.** Processor shall store and Process Personal Data in logically or physically segregated environments such that Omega's Personal Data is not commingled with data of other customers unless authorized in writing by Omega.

15. **Notice.** Any notices or communications to be given pursuant to this Agreement shall be made to the addresses given below:

If to Controller, to:

OMH-HealthEdge Holdings, Inc. d/b/a
Omega Healthcare Management Services
Attn: Chief Legal Officer
2424 N. Federal Highway, Suite 205
Boca Raton, FL 33431
legal@omegahms.com

If to Processor:

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

Controller:	**Processor:**
OMH-HealthEdge Holdings, Inc.	_____
_____	_____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Exhibit A – Security Measures

Vendor shall implement and maintain at least the following Security Measures. These Security Measures supplement, and do not limit, Vendor's obligations under Section 2 of the DPSA. If there is any inconsistency between the Security Measures and the body of the DPSA, the stricter or more protective requirement shall apply.

1. Scope. Vendor shall implement administrative, technical, and physical safeguards to protect Personal Information and Confidential Information, consistent with the Agreement, the DPSA, and this Exhibit. These Security Measures apply to all Processing of Personal Information or Confidential Information performed by Vendor or its Personnel, and to any access to Covered Systems used in connection with the Services. Vendor shall ensure that all safeguards and controls required under this Exhibit apply equally to Processing activities and to access to Covered Systems, regardless of whether such systems are hosted, owned, or managed by Omega, Vendor, or a third party engaged in connection with the Services.

1.1 International Data Protection Regulation. Vendor shall comply with all applicable international data protection laws.

1.2 U.S. Data Protection Regulation. Vendor shall comply with all applicable U.S. federal and state privacy laws governing Personal Information.

1.3 Personal Information Use and Security. Vendor shall use Personal Information only as permitted under the Agreement and shall maintain safeguards to preserve its confidentiality, integrity, and availability.

1.4 Personal Information Incident Reporting. Vendor shall report any actual or reasonably suspected unauthorized acquisition, access, use, disclosure, or destruction of Personal Information in accordance with the incident-notification requirements of the DPSA and this Exhibit.

2. Operational Provisions.

2.1 Adequate Safeguards. Vendor shall maintain a written information security program aligned with recognized security frameworks (e.g., ISO 27001, NIST CSF), reasonably designed to protect Confidential Information and Vendor systems supporting the Services.

2.2 Data Centers. Vendor shall maintain hosting environments that use industry-standard physical, environmental, and access controls and that provide levels of availability and resiliency appropriate to the Services.

2.3 Audit. Vendor shall maintain documentation sufficient to demonstrate compliance with this Exhibit and the DPSA and shall provide Omega with access to SOC/ISO reports or equivalent assurances upon reasonable request.

2.4 Infrastructure and Platform Security. Vendor shall maintain industry-standard technical and operational controls to protect systems, networks, applications, and infrastructure used to Process Confidential Information, including any third-party systems or services used in connection with the Services. At a minimum, Vendor shall implement the following:

2.4.1 Network Security. Vendor shall maintain a secure network architecture, including firewalls, network segmentation, intrusion detection and prevention systems ("IDS/IPS"), and configuration hardening consistent with industry practices.

2.4.2 Patch Management. Vendor shall apply security patches promptly based on severity (i.e., Critical within forty-eight (48) hours, High within one (1) week, and Medium within thirty (30) days) or shall implement documented compensating controls where timely patching is not feasible.

2.4.3 Malware Controls. Vendor shall deploy endpoint detection and response (**"EDR"**) or equivalent malware protection on systems used for the Services, including capabilities to prevent, detect, and recover from ransomware.

2.4.4 Portal and Internet-Facing Application Security. Vendor shall implement appropriate security controls for internet-facing applications, including multi-factor authentication, web application firewalls, bot detection and mitigation, rate limiting, and periodic security testing.

2.4.5 Mobile and Endpoint Security. Vendor shall ensure that any device used to access Confidential Information is protected through full-disk encryption, endpoint security controls, and secure connectivity mechanisms.

2.5 Identity and Access Management. Vendor shall restrict access to Confidential Information and Covered Systems to authorized personnel based on least-privilege principles and documented business need. At a minimum, Vendor shall implement the following:

2.5.1 User Identification and Password Controls. Vendor shall assign unique user IDs, enforce password complexity requirements, prohibit the sharing of credentials, and revoke access promptly upon personnel role changes or departures.

2.5.2 Multi-Factor Authentication. Vendor shall require multi-factor authentication for access to all devices and/or systems, administrative interfaces, and any remote or elevated access involving Confidential Information.

2.5.3 Access Controls and Reviews. Vendor shall apply least-privilege and role-based access controls, maintain approval workflows for access requests, and perform periodic reviews of access rights.

2.5.4 Privileged Access Management. Vendor shall restrict administrative and privileged access to the minimum required roles, shall require multi-factor authentication for all such access, shall record or administer privileged sessions where feasible, and shall review privileged roles on a regular basis.

2.5.5 Authorized Personnel and Background Checks. Vendor shall limit access to Confidential Information to personnel with a documented business need and shall perform appropriate background checks, including OIG, SAM, and OFAC screenings where applicable, removing any personnel with disqualifying histories or sanctions

2.6 Data Protection and Information Lifecycle. Vendor shall protect Confidential Information throughout its lifecycle, including creation, use, storage, transmission, and destruction. At a minimum, Vendor shall implement the following:

2.6.1 Data Loss Prevention. Vendor shall implement controls designed to prevent the unauthorized transfer or exposure of Confidential Information, including data-loss-prevention technologies or equivalent egress monitoring measures.

2.6.2 Data Encryption. Vendor shall encrypt Confidential Information both in transit and at rest using industry-standard protocols and algorithms.

2.6.3 Segregation of Customer Data. Vendor shall segregate Confidential Information from data belonging to other customers through logical or physical separation.

2.6.4 Minimum Necessary Processing. Vendor shall limit the Processing of Confidential Information to the minimum necessary to perform the Services and comply with the Agreement.

2.6.5 Portable and Removable Media. Vendor shall prohibit the storage of Confidential Information on portable or removable media by default and shall allow exceptions only where such media are encrypted and specifically approved by Omega in writing.

2.6.6 Secure Data Destruction. Vendor shall permanently delete Confidential Information when no longer required using recognized sanitization standards and, upon request, shall provide Omega with certificates of destruction describing the date, method, and materials destroyed.

2.6.7 Databases. Vendor shall maintain secure configurations for databases containing Confidential Information, shall limit access to authorized roles, shall log administrative and privileged access, and shall review database privileges regularly.

2.7 Logging, Monitoring, and Detection. Vendor shall maintain logging, monitoring, and alerting capabilities sufficient to detect, investigate, and respond to security-relevant events affecting Confidential Information or Covered Systems. At a minimum, Vendor shall implement the following:

2.7.1 Detection and Monitoring. Vendor shall monitor networks and systems for malicious activity, including malware detection, security event monitoring, and real-time alerting of suspicious or anomalous events.

2.7.2 Monitoring Tools and Automated Alerts. Vendor shall maintain tools that log and monitor system activity and shall automatically generate alerts or trouble tickets for failures or suspicious security-relevant events.

2.7.3 Logging and Retention. Vendor shall maintain audit logs of system, network, and database access, shall review critical events, and shall retain security logs for at least 12 months in an accessible form.

2.8 Workforce Governance and Acceptable Use. Vendor shall maintain governance controls to ensure that personnel understand and comply with security obligations applicable to the Services. At a minimum, Vendor shall implement the following:

2.8.1 Acceptable Use Policy. Vendor shall maintain and enforce an acceptable use policy that governs the use of systems and personnel involved in providing the Services.

2.8.2 Security Policies, Training and Sanctions. Vendor shall maintain and enforce appropriate written information security policies; shall provide personnel with onboarding and periodic training, including annual phishing and social-engineering testing; and shall enforce disciplinary policies and/or appropriate sanctions for violations of its policies or this Exhibit.

3. Vendor Contact. Vendor shall designate a single point of contact with authority to act on privacy and security matters on Vendor's behalf, including coordination of Security Incidents.

4. Subcontracts. Vendor shall ensure that all subcontractors involved in Processing Confidential Information are bound by written obligations that are at least as protective as the requirements of this Exhibit and the DPSA. Vendor shall provide Omega with a current list of such subcontractors upon request.

5. Trouble Ticketing System. Vendor shall maintain an electronic system to record, track, and manage security-related issues affecting systems used to Process Confidential Information.

6. Offshoring. Vendor shall not Process, Store, or Transfer Confidential Information outside the United States without Omega's prior written approval and a jointly agreed offshore plan describing authorized locations, permitted Processing, and applicable safeguards.

7. Hard Copy Materials. Vendor shall secure hard-copy materials containing Confidential Information, shall limit access to such materials to authorized personnel, and shall confidentially destroy such materials when no longer required.

8. Legal Compliance. Vendor shall comply with all applicable federal, state, and international laws governing the privacy and security of Confidential Information and shall cooperate with Omega in meeting any legal obligations related to such information.

9. Security Incident and Breach Response.

9.1 Prior Incidents. Vendor represents that, to its knowledge after reasonable inquiry, it is not aware of any significant prior breach affecting systems relevant to the Services.

9.2 Incident Management Program. Vendor shall maintain a written incident-response plan that addresses identification, containment, eradication, investigation, remediation, and recovery from Security Incidents, including ransomware readiness.

9.3 Notification. Vendor shall notify Omega within twenty-four (24) hours after becoming aware of any actual or reasonably suspected Security Incident involving Confidential Information or Personal Information.

9.4 Investigation and Response. Vendor shall promptly investigate any Security Incident, shall mitigate its effects, shall identify the data reasonably believed to be affected, and shall provide Omega with drafts of any notices that may be required by applicable law.

9.5 Regulatory Involvement. In connection with any Security Incident involving Confidential Information, Omega may observe Vendor's communications with any regulator to the extent permitted by applicable law or the regulator's procedures.

9.6 Mitigation. Vendor shall take all appropriate measures to reduce the adverse effects of any Security Incident and shall coordinate such mitigation with Omega, subject to Omega's approval where appropriate.

10. Disaster Recovery and Business Continuity. Vendor shall maintain disaster-recovery and business-continuity capabilities sufficient to meet a recovery point objective (RPO) of no more than four hours and a recovery time objective (RTO) of no more than 24 hours. Vendor shall test such plans at least annually, shall provide Omega with reasonable advance notice of any test that may affect the Services, and shall make high-level test results available to Omega upon request.

11. Certifications. Vendor shall maintain any certifications required under the Agreement, including SOC 2 or ISO certifications where applicable, and shall notify Omega of any failures or material deficiencies identified by any certifying entity.

12. Testing. Vendor shall conduct internal and external periodic security testing, including vulnerability scanning, penetration testing, and social-engineering or phishing testing, and shall remediate identified findings in timeframes appropriate to their severity.

13. Audits. Vendor shall notify Omega in advance of any third-party audit or inspection of systems relevant to the Services (subject to confidentiality requirements) and shall provide Omega with copies of any resulting audit reports upon request.

14. Responses. Vendor shall provide timely, accurate responses to Omega's questionnaires, assessments, and documentation requests related to Vendor's security controls and its Processing of Confidential Information.

15. Secure Software Development. Vendor shall use secure software-development practices, including code scanning, dependency management, environment segregation, change control, and pre-release security testing.

16. Artificial Intelligence. Vendor shall notify Omega in advance of using artificial-intelligence or machine-learning tools in connection with the Services and shall not use any such tools to Process Confidential Information without Omega's prior written approval and appropriate safeguards.