DATA SECURITY ADDENDUM

Last Updated: October 14, 2026

This Data Security Addendum (this "Security Addendum") is published by Patra Corporation ("Patra") and applies to Patra's safeguarding of Client Information that Patra accesses, receives, stores, transmits, or otherwise handles on behalf of each client ("Client") under a Master Services Agreement or other written or online agreement with Patra (the "Agreement"). This Security Addendum is incorporated by reference into the Agreement and supplements the Agreement with respect to information security. All capitalized terms not defined herein have the meanings ascribed to them in the Agreement or in the Data Processing Addendum (the "DPA").

This Security Addendum addresses the security of all Client Information, whether or not it constitutes Personal Data. To the extent Client Information constitutes Personal Data, the technical and organizational measures, Security Incident, Subprocessor, and data return and deletion provisions of the DPA also apply. To the extent this Security Addendum applies to Patra's AI Systems, the AI-specific security measures of the AI Addendum also apply. In the event of any conflict, the order of precedence in Section 9 governs.

1. DEFINITIONS Capitalized terms used but not otherwise defined in this Security Addendum have the meanings given to them in the Agreement or the DPA. "Security Incident" means any confirmed or reasonably suspected unauthorized access to, use, disclosure, alteration, or destruction of Client Information in Patra's possession or control, whether or not such Client Information constitutes Personal Data. "Security Measures" means the technical and organizational measures described in this Security Addendum.

2. INFORMATION SECURITY PROGRAM Patra shall implement and maintain a written information security program that includes appropriate technical and organizational measures designed to protect the confidentiality, integrity, and availability of Client Information against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access. Patra's Security Measures shall be consistent with the technical and organizational measures set forth in Section 3 of the DPA and shall include, at a minimum: (a) encryption of Client Information in transit and at rest; (b) access controls, including role-based access, multi-factor authentication, and least-privilege principles; (c) secure software development and change management practices; (d) regular security testing and vulnerability assessments; (e) comprehensive logging and monitoring; and (f) business continuity and disaster recovery plans with defined recovery objectives.

3. PERSONNEL SECURITY Patra shall ensure that all personnel with access to Client Information are subject to binding confidentiality obligations and receive appropriate security training commensurate with their role. Access to Client Information shall be restricted to personnel who require such access to perform the Services.

4. ACCESS CONTROLS AND SYSTEM SECURITY Patra shall maintain role-based and attribute-based access controls, multi-factor authentication, least-privilege access principles, and

segregation of duties for systems used to access or process Client Information, and shall maintain a secure software development lifecycle incorporating code review, security testing, supply-chain controls, and change management. Patra Systems used to access or process Client Information, including Patra-managed workstations and equipment, are configured and managed by Patra under its information security program, including application allowlisting and restrictions on the installation of third-party software. Patra does not install Client Software on Patra Systems except as approved by Patra in writing in its sole discretion, and any approved Client Software is subject to Patra's change management and segregation controls. Patra's decision not to install Client Software shall not constitute a breach of the Agreement or any SOW, or a violation of Client's access standards or information technology security policies. Client is responsible for the licensing, security, and configuration of any Client Software. "Client Software" means any software, agent, application, browser extension, certificate, or configuration change requested or required by Client or a third party with whom Client does business for installation on Patra Systems, including endpoint monitoring, antivirus or anti-malware, remote or device management, patch management, and locally installed management system clients. "Patra Systems" has the meaning given in the Agreement or, if not defined there, means Patra's information technology systems, equipment, software, and applications.

5. SECURITY INCIDENTS Patra shall notify Client of a Security Incident in accordance with Section 10 of the DPA. Where a Security Incident involves Client Information that does not constitute Personal Data, Patra shall notify Client without undue delay following Patra's confirmation of the Security Incident and shall cooperate with Client's reasonable requests in connection with the investigation, remediation, and notification obligations arising from such Security Incident. For the avoidance of doubt, the notification obligations and timing set forth in the DPA govern any Security Incident involving Personal Data, and nothing in this Security Addendum imposes a different or conflicting standard.

6. SUBPROCESSORS Patra's engagement of Subprocessors that access Client Information is governed by Section 4 of the DPA and, for the purposes of AI Systems, as further governed and defined by Section 8 of the AI Addendum. Patra shall impose data protection and security obligations on such Subprocessors that are no less protective of Client Information than those set out in this Security Addendum and the DPA, and Patra remains responsible for its Subprocessors' performance of those obligations.

7. CERTIFICATIONS AND AUDITS Patra shall maintain industry-standard security certifications, including as applicable SOC 2 Type II and ISO 27001, and shall make available to Client relevant audit reports and third-party certifications in accordance with Section 7 of the DPA.

8. RETURN AND DELETION Return and deletion of Client Information upon expiration or termination of the Agreement, or upon Client's written request, shall be handled in accordance with Section 9 of the DPA and the Effect of Termination provisions of the Agreement.

9. ORDER OF PRECEDENCE This Security Addendum supplements, and does not limit, the security obligations set forth in the Agreement, the DPA, and the AI Addendum. In the event of any conflict between this Security Addendum and the Agreement, an SOW, the AI Addendum, or the DPA, the order of precedence set forth in Section 15.1 of the DPA shall govern.

10. UPDATES This Security Addendum is an Online Document and may be updated or replaced by Patra from time to time in accordance with Section 7.i of the Agreement (Online Documents; Patra's Right to Amend).

ACCEPTANCE AND EFFECTIVE DATE By accepting the Agreement, or by accessing or using the Services after this Security Addendum is made available, Client acknowledges that it has read and understood, and agrees to be bound by, this Security Addendum.