MASTER SOFTWARE AS A SERVICE AGREEMENT

Version 1.0

This Master Software as a Service Agreement ("MSA") is entered into as of [Effective Date] by and between epp Technologies, Inc, a Delaware Corporation, having its principal place of business at 3423 Piedmont Rd NE, Atlanta, GA 30305 ("Provider"), and [Customer Legal Name] having its principal place of business at [Address] ("Customer"). Provider and Customer are each a "Party" and together the "Parties."

1. Agreement Structure

1.1 Services

Provider provides cloud-based software, artificial intelligence functionality, autonomous and semi-autonomous agents, APIs, integrations, applications, implementation services, support, and related technology and services collectively referred to as the "Services." Customer may purchase Services through one or more Order Forms executed by the Parties.

1.2 Contract Documents

The agreement between the Parties consists of this MSA, each applicable Order Form, the Data Processing Addendum ("DPA"), the Service Level Agreement ("SLA"), the AI & Autonomous Agent Security/Controls Schedule, applicable Statements of Work ("SOWs"), and any additional document expressly incorporated by reference.

1.3 Order of Precedence

In the event of a conflict: (1) the DPA controls with respect to Personal Data; (2) the AI & Autonomous Agent Security/Controls Schedule controls with respect to autonomous-agent security and authorization; (3) the Order Form controls with respect to commercial terms; (4) the SLA controls with respect to service levels; and (5) this MSA controls in all other respects. An Order Form modifies this MSA only when it expressly identifies the provision being modified.

2. Definitions

"Agent Action" means an action performed by an AI Agent through the Services on Customer's behalf. "AI Agent" means autonomous or semi-autonomous artificial intelligence functionality capable of reasoning, planning, recommending, communicating, invoking tools or APIs, or performing Agent Actions. "AI Features" means artificial intelligence, machine learning, generative AI, reasoning, recommendation, prediction, and autonomous-agent functionality included in the Services. "Authorized User" means an individual authorized by Customer to access the Services. "Customer Data" means all information, files, records, Personal Data, prompts, Inputs, configurations, instructions, and other content submitted to or processed through the Services by or for Customer. "Documentation" means Provider's then-current documentation for the Services. "Input" means information provided to an AI Feature. "Output" means information, recommendations, actions, communications, analyses, or other results produced by an AI Feature. "Personal Data" has the meaning given under applicable privacy laws. "Third-Party Service" means a third-

party software platform, CRM, API, database, identity provider, communications service, AI model, or other external service integrated with the Services.

3. Subscription Rights

Subject to this Agreement and Customer's payment of applicable fees, Provider grants Customer a limited, non-exclusive, non-transferable, non-sublicensable right during the applicable Subscription Term to access and use the Services for Customer's internal business purposes. Customer may provide access to Authorized Users within the limits stated in the applicable Order Form. Customer is responsible for Authorized User activity, account administration, maintaining appropriate user permissions, safeguarding credentials, and promptly notifying Provider of known unauthorized account access.

4. AI Features and Autonomous Agents

4.1 AI Functionality

The Services may use AI Features to analyze Customer Data, generate recommendations, generate communications or content, retrieve information, plan or execute workflows, interact with Third-Party Services, perform Agent Actions, and automate business processes.

4.2 Authorized Agent Actions

Customer authorizes Provider and its AI Agents to perform Agent Actions that Customer expressly enables through system configuration, user permissions, workflow configuration, API authorization, integration authorization, administrator settings, or direct Authorized User instructions.

4.3 Scope of Authority

Provider will design and operate AI Agents so that Agent Actions are limited to Customer-authorized systems, Customer-authorized functions, assigned identity and permission scopes, and configured workflow constraints. AI Agents will not intentionally expand their own access privileges.

4.4 Human Approval

Provider supports human-in-the-loop controls for designated Agent Actions. Customer may configure actions to require human approval before execution. Provider will enforce configured approval requirements before the applicable Agent Action is initiated.

4.5 Revocation

Customer administrators may disable or revoke AI Agent permissions and integrations. Provider will cease subsequent Agent Actions requiring revoked permissions after revocation is processed by the Services.

4.6 Auditability

Provider will maintain logging appropriate to the applicable Service for material Agent Actions, including available information concerning initiating user or process, execution time, connected system, action performed, and execution status.

4.7 AI Limitations

Customer acknowledges that AI technology may produce inaccurate, incomplete, unexpected, or non-unique Outputs. Customer is responsible for applying appropriate human judgment where required by law or reasonably appropriate to Customer's use case.

5. AI Training and Model Usage

5.1 No Generalized Model Training

Provider will not use Customer Data, Inputs, Outputs, or Customer Confidential Information to train generalized artificial intelligence or machine-learning models for use by other customers without Customer's prior written consent.

5.2 Third-Party AI Providers

Provider may utilize third-party AI model providers as subprocessors. Provider will maintain contractual protections requiring such providers to process Customer Data only to provide the applicable services to Provider. Provider will configure third-party AI services so that Customer Data submitted through Provider is not used to train generalized third-party AI models.

5.3 Aggregated Usage Information

Provider may use aggregated or de-identified operational information that does not reasonably identify Customer or an individual to operate the Services, maintain security, measure performance, improve functionality, and develop Service improvements.

6. Third-Party CRM, API, and Enterprise Integrations

Customer may connect the Services to Third-Party Services, including Salesforce, HubSpot, Microsoft Dynamics, Microsoft 365, Google Workspace, Slack, Microsoft Teams, identity providers, databases, enterprise APIs, and other systems supported by Provider. Customer authorizes Provider to read, transmit, create, update, or otherwise process information through Customer-enabled integrations according to configured permissions. Provider will use OAuth, API keys, service accounts, tokens, or equivalent authorization mechanisms as appropriate, follow least-privilege principles when designing supported integrations, and not intentionally expand an integration beyond permissions authorized by Customer.

7. Customer Data

Customer retains all right, title, and interest in Customer Data. Customer grants Provider a limited license to process Customer Data only as necessary to provide the Services, execute Customer-authorized Agent Actions, provide support, maintain security, prevent fraud and abuse, satisfy legal obligations, and fulfill Provider's obligations under the Agreement. Provider acquires no ownership interest in Customer Data.

8. Information Security

Provider will maintain a written information-security program containing administrative, technical, organizational, and physical safeguards appropriate to the nature of the Services and information processed. Provider's security program includes encryption of Customer Data in transit and at rest, least-

privilege access, role-based access controls, multi-factor authentication for privileged systems, logical tenant separation, security logging and monitoring, vulnerability management, penetration testing, secure software-development practices, code review, dependency management, incident-response procedures, backup and recovery, employee security training, personnel-access controls, vendor risk management, change-management procedures, and business continuity and disaster recovery.

9. SOC 2

Provider maintains controls subject to an independent SOC 2 Type II examination covering applicable Trust Services Criteria. Upon Customer's reasonable request and subject to confidentiality requirements, Provider will make its current SOC 2 Type II report available to Customer. Provider will use commercially reasonable efforts to remediate material control deficiencies identified through its SOC 2 program.

10. Penetration Testing and Vulnerability Management

Provider will conduct periodic vulnerability assessments of production infrastructure and arrange penetration testing by qualified independent security professionals at least annually. Upon reasonable request, Provider will provide Customer with an executive summary of its then-current penetration-testing results, subject to appropriate confidentiality restrictions. Provider will maintain a risk-based remediation program for identified vulnerabilities.

11. Enterprise Authentication

Provider supports enterprise identity and access management capabilities, including SAML 2.0, OpenID Connect where applicable, enterprise Single Sign-On, role-based access controls, multi-factor authentication, SCIM provisioning and deprovisioning where included in the applicable subscription, and customer-controlled identity-provider integrations.

12. Data Residency

Provider will host Customer's primary production data in the geographic region identified in the applicable Order Form. Provider will not materially relocate Customer's primary production data to another region without Customer authorization where Customer has purchased regional data residency. Limited cross-border processing may occur for subprocessors, security, support, or Service operation in accordance with the DPA and applicable law.

13. Security Incidents

Provider will maintain documented incident-response procedures. Provider will notify Customer without undue delay and, where reasonably practicable, within forty-eight (48) hours after confirming a Security Incident involving unauthorized acquisition of or access to Customer Personal Data. Provider will provide information reasonably available concerning the nature of the incident, affected systems or information, mitigation measures, remediation activities, and relevant updates. Notification is not an admission of liability.

14. Security Reviews and Audit Rights

Provider will reasonably cooperate with Customer's security and privacy assessment process. Provider may satisfy assessment requirements through SOC 2 reports, penetration-test summaries, security questionnaires, architecture documentation, policies, certifications, and other appropriate independent audit materials. If such materials are insufficient to satisfy a legal or regulatory requirement applicable to Customer, Customer may conduct an additional audit no more than once annually unless required following a confirmed material Security Incident. Audits must occur during normal business hours, be conducted on reasonable advance notice, preserve Provider and other customers' confidentiality, avoid penetration testing of production systems without written authorization, and not unreasonably interfere with Provider operations.

15. Confidentiality

Each Party will protect the other Party's Confidential Information using at least reasonable care, use Confidential Information only to perform or exercise rights under this Agreement, and disclose it only to personnel, contractors, advisers, and service providers who have a need to know and appropriate confidentiality obligations. Customer Data is Customer Confidential Information. Provider source code, non-public architecture, security information, models, algorithms, roadmaps, pricing, and proprietary technology are Provider Confidential Information. Customary exclusions apply to information publicly available without breach, independently developed, previously known without restriction, or lawfully obtained from a third party.

16. Intellectual Property

Provider retains all rights in the Services, software, source code, AI systems, algorithms, models, APIs, workflows, interfaces, Documentation, inventions, improvements, and Provider technology. Customer retains all rights in Customer Data. No implied intellectual-property rights are granted.

17. Feedback

Customer may voluntarily provide suggestions or feedback. Provider may use such feedback without restriction, provided that Provider does not disclose Customer Confidential Information or identify Customer as the source without authorization.

18. Acceptable Use

Customer will not use the Services to violate applicable law, infringe third-party rights, introduce malicious code, circumvent access controls, gain unauthorized system access, perform unauthorized security testing, reverse engineer the Services except where legally permitted, interfere with Service integrity, use credentials without authorization, or direct an AI Agent to perform an action Customer is not authorized to perform.

19. Fees and Payment

Customer will pay fees specified in the Order Form. Unless otherwise stated, subscription fees are invoiced annually in advance, usage-based charges are invoiced in arrears, invoices are due Net 30, undisputed fees are non-refundable except as expressly provided, Customer is responsible for applicable taxes other than

taxes on Provider's net income, and Provider may suspend Services for materially overdue undisputed amounts after written notice and a reasonable cure period.

20. Warranties

Provider warrants that it has authority to enter into the Agreement, the Services will materially conform to applicable Documentation, Provider will perform professional services in a professional and workmanlike manner, and Provider will not knowingly introduce malicious code into the Services. If Provider breaches the Service warranty and does not cure the breach within a reasonable period, Customer may terminate the affected Services and receive a prorated refund of prepaid unused fees for those Services.

21. Disclaimer

EXCEPT FOR EXPRESS WARRANTIES IN THE AGREEMENT, THE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." TO THE MAXIMUM EXTENT PERMITTED BY LAW, PROVIDER DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. PROVIDER DOES NOT WARRANT THAT AI OUTPUTS WILL ALWAYS BE ACCURATE, COMPLETE, UNIQUE, OR APPROPRIATE FOR CUSTOMER'S PARTICULAR PURPOSE.

22. Provider Indemnification

Provider will defend Customer against third-party claims alleging that Customer's authorized use of Provider's proprietary Services infringes a patent, copyright, trademark, or other applicable intellectual-property right and will indemnify Customer against damages finally awarded or settlements approved by Provider. Provider has no obligation for claims caused by Customer Data, unauthorized modifications, use contrary to Documentation, combinations not supplied or authorized by Provider where the combination causes infringement, or Third-Party Services. Provider may obtain continued usage rights, modify or replace affected functionality, or terminate the affected Service and refund prepaid unused fees.

23. Customer Indemnification

Customer will defend and indemnify Provider against third-party claims arising from Customer Data, Customer's unlawful instructions, Customer's unauthorized use of Third-Party Services, Customer's violation of third-party rights, or Customer's material violation of Section 18.

24. Limitation of Liability

Neither Party will be liable for indirect, incidental, special, exemplary, punitive, or consequential damages, or lost profits, revenue, or goodwill. Except for Excluded Claims, each Party's aggregate liability will not exceed the fees paid or payable under the applicable Order Form during the twelve months preceding the event giving rise to liability. For confidentiality breaches, data-protection obligations, Security Incidents caused by a Party's breach, and intellectual-property indemnification obligations, the aggregate liability cap will be two times (2x) the fees paid or payable under the applicable Order Form during the preceding twelve months. Nothing limits liability to the extent such liability cannot legally be limited, including fraud or willful misconduct.

25. Subscription Term and Renewal

Each Order Form will specify its Subscription Term. Unless otherwise stated, each subscription will expire at the end of the stated subscription term unless either Party provides written notice of interest to renew at least thirty days before expiration and the agreement has been reached with a newly executed order.

26. Termination

Either Party may terminate an affected Order Form for material breach if the breaching Party fails to cure within thirty days after written notice. A Party may terminate immediately if the other Party becomes insolvent, ceases business operations, or commits a material breach incapable of cure. Upon termination, Customer's Service access ends, unpaid accrued fees remain payable, Customer may export Customer Data during the applicable retention period, and Provider will delete Customer Data according to the DPA.

27. Enterprise Procurement

Provider will reasonably cooperate with customary enterprise procurement activities, including vendor onboarding, W-9 and tax documentation, insurance certificates, privacy questionnaires, security questionnaires, accessibility documentation, architecture reviews, and compliance assessments. Customer purchase orders, procurement systems, click-through terms, or vendor-portal terms are administrative only and do not modify the Agreement unless separately executed by Provider's authorized representative.

28. Insurance

Provider will maintain commercially reasonable insurance appropriate to its business, including commercial general liability, technology errors and omissions, and cyber/privacy liability coverage. Specific insurance limits may be stated in the applicable Order Form.

29. Publicity

Provider will not issue a press release identifying Customer without Customer's written approval. Provider may use Customer's name or logo in marketing materials only without Customer's prior written authorization.

30. Compliance With Laws

Each Party will comply with laws applicable to its performance under the Agreement, including applicable privacy laws, data-protection requirements, sanctions, export controls, anti-corruption laws, and AI-related legal requirements.

31. Assignment

Neither Party may assign the Agreement without the other Party's consent, except in connection with a merger, acquisition, corporate reorganization, or sale of substantially all relevant assets, provided the successor assumes the assigning Party's obligations.

32. Governing Law

This Agreement is governed by the laws of the State of Delaware, excluding conflict-of-law principles. The state and federal courts located in Delaware will have exclusive jurisdiction.

33. General

The Parties are independent contractors. The Agreement creates no partnership, joint venture, fiduciary, agency, or employment relationship. If any provision is unenforceable, the remainder remains effective. Failure to enforce a provision does not waive it. Amendments must be in writing signed by authorized representatives. Electronic signatures and counterparts are valid. The Agreement constitutes the entire agreement regarding its subject matter.

SIGNATURES

PROVIDER	CUSTOMER
epp Technologies, Inc	[Customer Legal Name]
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____