Evently

EXHIBIT A - AI & AUTONOMOUS AGENT SECURITY/CONTROLS SCHEDULE

Version 1.0

This AI & Autonomous Agent Security/Controls Schedule ("AI Controls Schedule") forms part of the Master Software as a Service Agreement and applies to AI Agents capable of performing Agent Actions on behalf of Customer.

1. Purpose

The purpose of this Schedule is to establish authorization boundaries, identity and access controls, human-approval controls, logging requirements, integration security, credential protections, data-use limitations, operational safeguards, and accountability for autonomous Agent Actions.

2. Agent Authorization Model

An AI Agent may perform an Agent Action only where the action is authorized through one or more of the following: Customer administrator configuration, Customer-authorized integration permissions, Customer-created workflow, direct Authorized User instruction, preconfigured business rule, or other Customer-approved authorization mechanism. Provider will not intentionally permit an AI Agent to independently increase its authorization scope.

3. Principle of Least Privilege

AI Agents will be designed to use the minimum permissions reasonably necessary to perform configured functions. Where an integration supports granular permission scopes, Provider will request permissions appropriate to the applicable integration functionality.

4. Identity and Authentication

Agent access to Third-Party Services will use supported secure authentication mechanisms, which may include OAuth 2.0, signed tokens, API keys, service accounts, scoped credentials, or equivalent secure mechanisms. Provider will not intentionally expose integration credentials to unauthorized users.

5. Credential Protection

Provider will maintain controls designed to protect authentication credentials, including encrypted transmission, secure storage, access restrictions, secrets management, logging of administrative credential access where appropriate, and credential revocation capabilities. Provider personnel will not access Customer integration credentials except where necessary for authorized operational or support purposes.

6. Human-in-the-Loop Controls

Provider supports configurable human approval for designated Agent Actions. Customer may require approval before actions such as sending external communications, modifying material records, deleting records, changing schedules, initiating consequential workflows, making external API writes, or other Customer-designated actions. When approval is required, the AI Agent will not intentionally execute the applicable action until the required approval has been obtained.

7. High-Risk Actions

Customer is responsible for determining whether particular business processes constitute high-risk activities. Provider will make controls available to limit autonomous execution of designated actions. Unless expressly supported and authorized in writing, Customer will not use AI Agents as the sole decision-maker for decisions that legally require human review.

8. Agent Action Logging

Provider will maintain appropriate records of material Agent Actions. Logs may include date and time, initiating user or automated workflow, AI Agent identifier, action type, affected connected system, target object or record identifier, execution result, approval state where applicable, and error status. Logging detail may vary by Service and connected system.

9. Audit Trail Access

Where supported by the applicable Service, Customer administrators may access audit records through administrative interfaces, dashboards, reports, API access, or support requests. Provider will maintain audit logs according to its applicable retention policies.

10. Integration Boundaries

AI Agents will interact only with Third-Party Services that Customer has authorized. Provider will not intentionally enable one Customer's AI Agent to access another customer's environment or data. Provider will maintain logical tenant separation.

11. API Controls

Provider will implement commercially reasonable API security practices, including as applicable authentication, authorization, scope restrictions, encrypted transport, request validation, rate limiting, error handling, and monitoring.

12. Data Minimization

AI Agents will be designed to process Customer Data reasonably necessary for the configured workflow. Customer controls the data and systems made available through its integrations and configurations.

13. AI Model Data Controls

Provider will not submit Customer Data to third-party AI providers for generalized model training. Third-party AI providers used by Provider will be contractually restricted from using Customer Data for generalized model training. Provider will maintain a subprocessor list identifying applicable material AI providers.

14. Output Handling

AI-generated Outputs may be displayed to Authorized Users, stored as Customer Data, transmitted to authorized connected systems, used to initiate approved Agent Actions, or subjected to human approval. Provider will apply Customer-configured authorization requirements before executing controlled Agent Actions.

15. Autonomous Communication Controls

Where AI Agents are authorized to send external communications, Customer controls recipient-access permissions, communication channels, approval requirements, template or workflow configuration, and applicable business rules. Customer remains responsible for determining whether communications comply with laws applicable to Customer.

16. Kill Switch and Revocation

Customer administrators may disable an AI Agent, a workflow, an integration, an Authorized User, specific Agent Action capabilities, or applicable authentication credentials. Provider may also disable AI Agent functionality when necessary to protect Customer, Provider, other customers, third parties, or Service security.

17. Emergency Suspension

Provider may immediately suspend an AI Agent or integration where Provider reasonably determines that continued operation poses a material risk of unauthorized access, security compromise, material data loss, unlawful activity, system instability, or harm to Customer or third parties. Provider will notify Customer promptly where commercially reasonable.

18. Agent Error Handling

Where an Agent Action fails, Provider will use commercially reasonable mechanisms to capture applicable errors, avoid uncontrolled repeated actions, report failure status where supported, stop or retry actions according to system configuration, and permit investigation through applicable logs.

19. Rate and Execution Controls

Provider may implement rate limits, execution limits, concurrency limits, transaction safeguards, API limits, and workflow constraints to protect Service reliability and prevent unintended repetitive Agent Actions.

20. Change Management

Provider will maintain change-management procedures applicable to material production AI Agent functionality. Material Service changes are subject to testing and deployment controls appropriate to Provider's software-development lifecycle.

21. Security Testing

AI Agent infrastructure is included within Provider's applicable vulnerability-management program, secure software-development lifecycle, penetration-testing program, access-control reviews, and SOC 2 control environment.

22. Customer Administrative Responsibilities

Customer is responsible for determining Authorized Users, configuring access permissions, reviewing integration scopes, identifying actions requiring human approval, revoking access when no longer required, maintaining security of Customer-controlled systems, ensuring Customer has authority to perform configured Agent Actions, and reviewing Agent Action logs as reasonably appropriate.

23. No Privilege Escalation

Provider will design AI Agents so they cannot intentionally self-authorize additional permissions beyond the access made available by Customer and Provider-controlled Service permissions. AI-generated instructions alone will not create additional system credentials or authorization rights.

24. Cross-Tenant Isolation

Provider will maintain controls intended to prevent AI Agents associated with one Customer tenant from accessing Customer Data belonging to another customer tenant.

25. Prompt and Instruction Security

Provider will maintain reasonable safeguards designed to reduce unauthorized manipulation of Agent behavior, including controls appropriate to system instructions, tool permissions, authorization enforcement, workflow boundaries, input validation, and output handling. Because adversarial AI techniques continue to evolve, no technical control guarantees prevention of every malicious or unexpected AI interaction.

26. Incident Investigation

Provider will use applicable logs and available system information to investigate reported material unauthorized Agent Actions. Where a Security Incident involving Personal Data occurs, the DPA controls.

27. Agent Action Responsibility Matrix

Control	Provider	Customer
Service infrastructure security	X	

Control	Provider	Customer
AI Agent access-control mechanisms	X	
Tenant separation	X	
Credential protection within Provider systems	X	
Customer identity-provider configuration		X
Selection of Authorized Users		X
Selection of connected systems		X
Customer integration authorization		X
Enforcement of configured permissions	X	
Selection of human-approval requirements		X
Enforcement of configured approvals	X	
Business legality of Customer instructions		X
Agent Action logging infrastructure	X	
Customer audit-log review		X
Third-party AI contractual controls	X	
Customer Data submitted to the Services		X
Security Incident response within Provider environment	X	
Security of Customer-controlled systems		X

28. Priority

If this AI Controls Schedule conflicts with the MSA regarding AI Agent authorization, security, logging, or operational controls, this Schedule controls.

SIGNATURES

PROVIDER	CUSTOMER

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