Artificial Intelligence Management Program

1. Purpose

This Artificial Intelligence Management Program (hereinafter referred to as the " Program") is established to implement the governance principles set forth in the *Artificial Intelligence Governance Policy* of Avary Holding (Shenzhen) Co., Ltd. and its subsidiaries (hereinafter referred to as the "Group"), and to establish mechanisms for the risk assessment, review, control, and ongoing monitoring of artificial intelligence (AI), serving as the basis for the Group's execution of AI governance.

2. Scope

This Program applies to all employees of the Group and its joint ventures, including full-time employees and contract personnel, as well as business partners such as suppliers, outsourcing providers, and contractors. It covers AI systems and related applications that are developed in-house, externally procured, developed under commission, or built using open-source technology.

3. Governance Structure and Responsibilities

The Group shall establish an AI governance structure spanning from senior management to executing units, with clearly defined roles, responsibilities, and decision-making authority at each level.

Senior management is responsible for overseeing and deciding on the direction of AI governance and on material risk matters; the dedicated AI management unit is responsible for driving and implementing the AI governance framework; and each AI system shall have a designated business owner responsible for its use, management, and ongoing oversight. Corresponding assessment, review, approval, monitoring, and accountability measures shall be applied according to the risk level of the AI system.

Avary Holding (Shenzhen) Co., Ltd. ©All Rights Reserved

4. AI System Inventory and Registry Management

The Group shall establish an AI system inventory that records information such as the purpose, using unit, owner, data types, system or model source, risk level, and management status of each AI system, and shall update it periodically in order to maintain visibility over the use and risk status of AI systems.

5. Risk Classification and Assessment

The Group shall establish an AI risk assessment mechanism that assesses and classifies AI systems based on factors such as their purpose of use, sensitivity of data, intended users, scope of impact, and potential impact on the rights and interests of stakeholders.

Each risk level shall be subject to corresponding review, testing, human oversight, and ongoing monitoring requirements.

Where there is a material change in the purpose, data, model, or usage context of an AI system, a risk assessment shall be conducted again.

6. Application and Onboarding Review for AI Use

Requesting units shall submit an application for AI use in accordance with the applicable procedures, describing the purpose of use, usage context, data sources, expected benefits, and associated risks, and shall complete the required review in accordance with the process.

AI applications that involve a high-risk level, material decisions, or a possible impact on the rights and interests of stakeholders shall, prior to onboarding, be reviewed by the dedicated AI management unit and approved by senior management before use. Any use that is unapproved or exceeds the approved scope is strictly prohibited.

7. Data and Model Management

The data used by AI systems shall have its source, lawfulness, scope of authorization, quality, and purpose of use verified, and corresponding management and protection measures shall be adopted according to the sensitivity of the data.

Avary Holding (Shenzhen) Co., Ltd. ©All Rights Reserved

The selection, development, tuning, version change, and decommissioning of models shall be subject to corresponding review, testing, and record-keeping according to their risk level.

Where there is a material change to the model, data source, key parameters, or functionality, a reassessment and any necessary testing shall be conducted according to the level of risk, and the relevant version and change records shall be retained.

8. Testing and Validation

Before an AI system goes live, the necessary testing of functionality, performance, reliability, security, output quality, fairness, and bias shall be conducted according to the level of risk, and the test results shall be recorded.

After an AI system goes live, its fairness and bias shall be assessed periodically according to the level of risk, and improvement measures shall be taken in response to any unfair outcomes or bias identified.

9. Human Oversight and Decision Control

The Group shall set human oversight requirements according to the risk level of the AI system. For critical or high-risk decisions affecting the rights and interests of stakeholders, personnel with the corresponding authority and competence shall be designated to conduct review, and the authority to intervene in, review, override, or suspend the operation of the AI shall be reserved.

AI outputs shall be subject to the necessary human judgment and review, and decisions shall not be made solely on the basis of AI outputs.

10.Transparency and Explainability Management

When an AI system interacts with users, the necessary disclosure of its AI identity and instructions for use shall be provided; AI-generated content and AI-driven decisions or outcomes shall be clearly labeled as being AI-generated or AI-assisted in nature.

For AI outputs that affect the rights and interests of stakeholders, sufficient information shall be provided according to the level of risk to help stakeholders

understand and use them correctly.

11.Privacy and Information Security Management

The collection, processing, storage, transmission, and use of data by AI systems shall comply with applicable privacy and personal data protection laws, and protection measures such as data minimization, de-identification, encryption, and access control shall be adopted according to the level of risk.

Systems involving facial recognition, surveillance, or other sensitive AI capabilities shall have their use and access rights restricted according to their risk level, and measures such as identity authentication, tiered authorization, and access control shall be adopted.

AI systems shall be incorporated into the Group's existing information security management mechanisms, and the necessary detection, defense, and response measures shall be taken against AI-related risks such as prompt injection, data poisoning, model theft, and unauthorized access.

12.Boundaries of Application and Prohibited Uses

The Group shall establish the permitted and prohibited uses of AI applications, and AI systems may be used only within the approved purpose and scope.

The permitted and prohibited scope of AI applications shall be reviewed and updated periodically by the information security, legal, and other relevant units. AI applications that infringe human rights, such as those involving manipulation, social scoring, or unauthorized biometric surveillance, shall not be developed, onboarded, or used.

Where an AI system is found to be used in an unapproved manner, beyond its authorized scope, or for a prohibited use, this shall be reported immediately to the dedicated AI management unit and other relevant units.

13.Third-Party AI Service Management

When adopting third-party AI models, platforms, and related products or services, the necessary assessment shall be conducted according to their risk level to verify matters such as data use, privacy protection, information security,

Avary Holding (Shenzhen) Co., Ltd. ©All Rights Reserved

model reliability, and legal compliance.

For high-risk AI products or services, management requirements such as data use, information security, confidentiality, incident notification, service changes, and allocation of responsibility shall be clearly stipulated in the contract.

14.Ongoing Monitoring and Reassessment

After an AI system goes live, an ongoing monitoring mechanism shall be established according to the level of risk to periodically review system performance, output quality, anomalies, fairness, bias, and other applicable risk indicators, and a mechanism for detecting model drift and performance degradation shall be established.

Where a decline in model performance, model drift, output anomalies, or other material risks are identified, improvement measures such as model tuning, retraining, revalidation, restricted use, or suspension of operation shall be taken as appropriate.

Where there is a material change in the purpose, data, model, functionality, or usage context of an AI system, a risk assessment and any necessary review shall be conducted again.

15.Grievances and Response

The Group provides users and stakeholders affected by AI decisions or outcomes with safe and accessible channels for objections and grievances, and handles all objections and grievances with care and diligence.

Grievance cases shall be received by the dedicated AI management unit, which shall respond with the outcome within a reasonable investigation period. Grievance and investigation records shall be properly retained, and the confidentiality of the complainant's identity and freedom from retaliation of any kind shall be safeguarded.

16.Training and Use Management

The Group shall provide training on AI governance, ethical use, information security, privacy protection, risk identification, and responsible AI use according

to personnel responsibilities and AI usage contexts, and shall do so at least once a year.

Users of AI systems shall operate them in accordance with the approved purposes and usage rules, shall not input unauthorized confidential, personal, or other protected information, and shall not use AI systems to engage in conduct that violates laws or the Group's rules.

17.Low-Carbon Energy and Ecological Footprint

In the selection, design, and application of AI systems, the Group shall consider energy efficiency and resource-use efficiency, and shall, to the extent feasible, adopt measures to reduce energy consumption, carbon emissions, and water consumption.

The Group shall establish indicators for the energy and resource use of AI applications, quantify energy consumption, carbon emissions, and water consumption, and track the effectiveness of related improvements, as a basis for sustainability management and subsequent improvement.

18.Disciplinary Provisions

Employees of the Group who violate this Program and related rules shall be dealt with in accordance with the internal reward and disciplinary regulations. Business partners such as suppliers, outsourcing providers, and contractors who violate this Program and related rules shall be subject to claims or litigation according to the severity of the violation and in accordance with the contract or relevant terms.

19.Record Retention, Audit, and Continuous Improvement

The Group shall retain records relating to AI applications, risk assessments, review and approval, testing and validation, models and versions, monitoring, incident handling, grievances, and improvements according to the risk level of the AI system, in order to support the management, traceability, and audit of AI systems. This Program shall be revised as appropriate in accordance with the *Artificial Intelligence Governance Policy*, international standards, laws and regulations, developments in AI technology, and the Group's business needs.

Avary Holding (Shenzhen) Co., Ltd. ©All Rights Reserved

20.Implementation and Amendment

This Program shall take effect after being signed by the head of the dedicated AI management unit on September 8, 2026, and the same procedure shall apply to any amendment.

Avary Holding (Shenzhen) Co., Ltd. ©All Rights Reserved