

## Walsin Lihwa Corporation

# Artificial Intelligence Application and Information Security Management Policy

### 1. Roles and Responsibilities

#### 1.1. AI System Owner Unit

In accordance with this Policy, the unit shall evaluate the principles for adopting the AI systems under its jurisdiction, submit applications, conduct preliminary risk assessments, and ensure that their intended uses comply with applicable requirements.

#### 1.2. Information Technology Unit

Responsible for the daily management of AI systems, including platforms, architecture, integration, technical operations and maintenance, and identity and access management.

#### 1.3. Information Security Unit

Responsible for the overall security architecture, security assessment of AI tools, access control, and risk monitoring.

#### 1.4. Legal/Compliance Department

Responsible for providing legal and compliance review and consultation, and determining compliance requirements for high-risk uses, to ensure compliance with the Personal Data Protection Act and other applicable laws and regulations.

## 1.5. Business Units

Responsible for final verification of AI-generated outputs (the humans “in the loop” principle), and for ensuring lawful use, authorization for input data, human review, decision-making/publication, and anomaly reporting.

## 2. Operating Procedures and Key Management Points

### 2.1. Definitions:

- A. Generative AI: An AI service that generates text, images, code, or other media content based on prompt instructions entered by users (e.g., ChatGPT, Claude, and Copilot Chat).
- B. Agentic AI (AI Agent): AI that is capable of autonomous planning, tool invocation, data access, or action execution.
- C. Prompt Injection: An attack in which malicious or specially crafted input instructions are used to manipulate or bypass an AI model’s original security restrictions, causing the system to perform unauthorized operations or disclose sensitive information.
- D. AI Impact Assessment (AIA): A systematic assessment, conducted before an AI system is introduced or launched, of the potential impact of the system on the Company’s cybersecurity, privacy,

data sensitivity, and business continuity.

- E. Enterprise AI: Artificial intelligence services, platforms, or systems that have been formally evaluated, approved, procured, or implemented by the Company and that meet the Company's requirements for cybersecurity, regulatory compliance, authentication, access control, data protection, and operational management.
- F. Public or Non-Enterprise AI: Public artificial intelligence services, websites, applications, or models that have not been formally evaluated, approved, procured, or authorized for use by the Company.
- G. Retrieval-Augmented Generation (RAG): A technical architecture in which an AI system retrieves relevant information from internal or external knowledge sources before generating a response, and then combines the retrieved results with a large language model for generation.
- H. AI System Owner: A business or technical manager responsible for the introduction, operation and maintenance, security management, access control, risk management, and regulatory compliance of an AI system.

- I. High-Risk AI: An AI system or use case whose operation may materially affect individual rights and interests, business operations, information security, legal liability, financial condition, product quality, occupational safety, or the public interest.

## 2.2. Core Principles of the Management Policy

This Policy is established in accordance with the core principles of Responsible Artificial Intelligence, including:

### 2.2.1. Establish Governance and Accountability

#### 2.2.1.1. Establish AI policies and guidelines, set up dedicated

oversight mechanisms, clearly define roles and responsibilities, and ensure that critical decisions remain subject to human oversight.

#### 2.2.1.2. Senior management shall actively participate in formulating the AI strategy to ensure that the direction of AI development is aligned with corporate values and business objectives.

#### 2.2.1.3. The Company shall assume the corresponding internal and external responsibilities for the systems it uses. Internally, a senior executive shall be designated to oversee a clear

governance structure and accountability mechanism.

## 2.2.2. Implement Interpretability and Explainability

2.2.2.1. The Company shall be able to clearly explain to stakeholders how an AI system operates, the factors on which its decisions are based, and the potential effects of those decisions.

2.2.2.2. For decisions or outputs produced by a system, appropriate information shall be disclosed to consumers (such as labeling AI-generated content), and reasonable explainability shall be provided where feasible to prevent black-box operation.

2.2.2.3. Transparent and explainable AI is not only essential to building trust, but also necessary for regulatory compliance.

## 2.2.3. Promote Fairness and Eliminate Bias

2.2.3.1. AI systems shall treat everyone fairly, avoid bias and discrimination, and prevent disparate impacts on similar groups.

2.2.3.2. At every stage of AI development, the Company shall proactively identify and mitigate bias risks and implement bias-detection procedures, including reviewing the diversity and representativeness of training data, testing model outputs for

systematic disparities, establishing continuous monitoring, and creating systematic mechanisms for early detection and mitigation of bias.

#### 2.2.4. Ensure Reliability and Cybersecurity

2.2.4.1. The Company shall ensure that AI models maintain stable and reliable performance when facing adversarial attacks, data-quality issues, or environmental changes.

2.2.4.2. Cybersecurity safeguards shall be implemented, including strict data-validation mechanisms, a model-performance monitoring framework, anomaly-handling procedures, and regular security testing and vulnerability assessments, to prevent malicious attacks or major system failures.

#### 2.2.5. Protect Privacy and Customer Rights

2.2.5.1. The Company shall ensure that data collection complies with legal requirements, apply appropriate de-identification, and establish strict access-control mechanisms.

2.2.5.2. Data security and confidentiality shall be maintained throughout the data lifecycle, with strict compliance with privacy-protection requirements.

## 2.2.6. Promote Sustainable Development and Well-Being

2.2.6.1. The management policy shall be aligned with environmental, social, and governance (ESG) objectives to ensure that technological and business development reduces the digital divide and the Company' s ecological footprint while supporting environmental sustainability.

## 2.3. System Acquisition and Supplier Evaluation

### 2.3.1. Baseline Principles for Adopting AI Tools:

2.3.1.1. Use enterprise-licensed AI tools with an enterprise administration console.

2.3.1.2. Obtain an official statement that data will not be returned for training and will not be used to train the supplier' s foundation models.

2.3.1.3. Support integration with the Company' s single sign-on (SSO) and multi-factor authentication (MFA).

2.3.1.4. Provide encryption for data in transit and at rest.

2.3.1.5. Confirm that, upon contract termination, the supplier has a mechanism to completely and irrecoverably destroy the data.

2.3.1.6. Intellectual-property infringement indemnification (whether the supplier provides Copyright Shield protection).

2.3.2. Introduction Application:

2.3.2.1. When a unit introduces, procures, or subscribes to an external AI system (including SaaS services) for business needs, it shall submit an application together with the AI System Use and Introduction Assessment Checklist.

2.3.2.2. When procuring third-party AI software, the unit shall confirm that the supplier has lawful data authorization and that the contract or terms of service comply with the Baseline Principles for Adopting AI Tools.

2.3.3. Information Security Assessment:

2.3.3.1. Review AI tool classification, data-storage and transmission risks, and compliance.

2.3.3.2. Assess whether the supplier has obtained international information-security certification (ISO 27001) or AI management-system certification (ISO 42001), whether its data-storage location complies with statutory localization requirements, and whether it supports internal identity and access controls such as SSO and RBAC.

2.3.3.3. Establish cybersecurity controls and safeguards and include them in risk assessment and monitoring.

2.3.4. Compliance Review:

2.3.4.1. Supplier contract review: When procuring third-party AI software, the unit shall confirm that the supplier has lawful data authorization, and the contract or terms of service shall expressly prohibit the supplier from using the Company' s business data and sensitive information to train its external foundation models.

2.3.4.2. Confirm whether copyright disputes are involved and whether domestic personal-data and privacy laws are satisfied.

2.3.5. Production Approval:

2.3.5.1. Register the approved production deployment in the AI inventory.

2.3.5.2. After approval, submit the item for assessment and inclusion in the AI Tool Allow/Deny List.

## 2.4. AI Tool Classification and Allow/Deny List (Whitelist)

The Company shall establish classifications for AI tool use and update the allow/deny list at least quarterly. The list shall primarily comprise the following three categories:

2.4.1. Category 1: Prohibited Use (e.g., unlawful tools with material security vulnerabilities or data-leakage risks).

2.4.2. Category 2: Restricted Use (e.g., the public version of ChatGPT, limited to routine work that does not involve confidential data).

2.4.3. Category 3: Enterprise Applications (e.g., Azure OpenAI and Copilot for Enterprise; data is protected by enterprise contracts and may be used to process operational data).

## 2.5. Cybersecurity Control Requirements

2.5.1. Data Input Restrictions (Data Leakage Prevention):

2.5.1.1. Company trade secrets, non-public financial data, customer personal data, product source code, and similar information shall never be entered into non-enterprise-authorized AI systems that have not been verified or have not committed to data confidentiality.

2.5.1.2. Priority shall be given to tools that provide enterprise accounts, encrypted transmission (TLS), and a Zero Retention commitment.

2.5.2. Human Oversight and AI Decision Control (Humans “in the loop” ):

2.5.2.1. AI-generated outputs, such as code, analytical reports, copy, or designs, shall be reviewed by personnel with appropriate expertise before publication.

2.5.2.2. Before agentic AI is used in Company operations to execute high-risk workflows, users shall conduct human review to ensure accuracy and confirm that there is no concern of data or system harm.

2.5.2.3. AI-generated results or documents shall never be used directly as the final version of legal documents or contracts.

2.5.3. Prevention of AI Poisoning and Adversarial Attacks:

For internally developed models, safeguards shall address AI poisoning during training and adversarial attacks during inference, and Prompt Injection vulnerability scans shall be conducted regularly.

2.5.4. Adopt ISO/IEC 42001:

Adopt the latest international standard for AI management systems and incorporate it into the Company' s Information Security Management System (ISMS) alongside ISO 27001.

2.5.5. Automated Monitoring:

It is recommended that a Data Loss Prevention (DLP) system be deployed at the Company' s network gateway to automatically identify and block

sensitive keywords uploaded to public AI websites (e.g., CONFIDENTIAL, PASSWORD, and API\_KEY).

#### 2.5.6. Establish an “AI Experimentation Sandbox” :

Provide a secure, internally controlled AI environment (such as a self-hosted LLM or an Azure OpenAI instance) to guide employees in migrating from high-risk tools to controlled tools.

#### 2.5.7. Continuous Education and Training:

2.5.7.1. Role-based training shall be provided for different audiences (such as general users, developers, agent builders, and administrators).

Training shall be conducted every six months, with additional training whenever material risks or policy changes arise.

2.5.7.2. Awareness and training shall cover data classification, AI hallucinations, prompt injection, deepfakes, intellectual property, incident reporting, prevention of AI-enabled fraud, and secure prompt engineering.

### 2.6. AI Application Management

#### 2.6.1. Comprehensibility and Takeover Readiness of AI-Generated Outputs

Code, scripts, system configurations, infrastructure definitions, workflows, rules, technical documents, operating manuals, or other outputs generated or modified by AI that may affect the production environment shall, before deployment, release, or formal adoption, be reviewed by personnel with the appropriate expertise and clearly assigned responsibility. The review shall confirm that the purpose, logic, scope of impact, dependencies, testing method, rollback method, and subsequent maintenance approach are explainable and transparent. If no qualified person can explain, maintain, or take over the output, it shall not be deployed to the production environment.

#### 2.6.2. Separation of AI-Generated Code and Production Deployment

##### Privileges

AI or AI agents may assist in generating or modifying code, configurations, and technical documents, but they shall not simultaneously possess the complete authority chain to generate or modify, merge, and deploy to the production environment without human approval. AI-generated or modified code and configurations shall undergo review by qualified personnel, required testing, security testing, and production approval in accordance with the Company' s

existing SDLC/CI/CD processes. High-risk or irreversible changes shall be subject to segregation of duties or dual approval.

### 2.6.3. Unexpected Autonomous AI Behavior / Unauthorized-Operation

#### Incidents

Any unauthorized access to data; execution of external or production-environment operations without approval; autonomous bypass of established controls or attempted privilege escalation; inability to stop through normal mechanisms; continuous execution of operations that materially deviate from the approved use case; or generation or deployment of code or configurations that no person can understand, maintain, or take over shall be treated as an information-security incident. The relevant agent or automated process shall be stopped immediately, necessary credentials or privileges revoked, the affected scope isolated, operation logs preserved, and incident response initiated.

### 2.6.4. Reservation Clause for AGI / Emerging Highly Autonomous AI

The boundaries of this Policy are not limited to the AI technologies expressly listed herein. If emerging AI with materially greater general reasoning, autonomous planning, tool invocation, self-adjustment, or long-duration autonomous execution capabilities becomes available in the future, including potential artificial

general intelligence (AGI), the Company's evaluation of its introduction or use shall trigger a special AIA and a review of this Policy's applicability. Such technology shall not be directly introduced into the production environment until risk assessment, control design, and required approvals have been completed.

#### 2.6.5. Labeling of AI Output Sources and Human Review

Establish a system for labeling AI output sources and human review, applicable to formal documents, code, system configurations, workflows, analytical results, images/audio/video, and other controlled business outputs.

### 2.7. Legal and Compliance Requirements

#### 2.7.1. Privacy Protection:

Comply with the Personal Data Protection Act. Information that directly or indirectly identifies an individual shall not be uploaded unless it has been de-identified, in order to protect privacy.

#### 2.7.2. Intellectual Property Protection:

Employees shall understand that AI-generated content is not currently eligible for copyright protection under most laws and regulations, and shall take care to avoid generating content that infringes third-party copyrights.

### 2.7.3. Transparency Principle:

If a business output is AI-generated and relates to the interests of external customers, it shall be appropriately labeled: “This content was generated with AI assistance.”

## 2.8. System Production Deployment, Monitoring, and Retirement Mechanisms

### 2.8.1. Pre-Deployment Scanning: Before an AI system is placed into

production, whether cloud-based or on-premises, it shall be integrated with the AI Security control platform and undergo security vulnerability scanning to confirm the absence of high risks such as malware, implanted backdoors, or prompt injection.

### 2.8.2. Activity-Log Monitoring and Anomaly Handling: Access logs for AI

systems shall be retained for reference. If severe deviation (model drift) or anomalous results are identified before, during, or after use, the issue shall be reported immediately for investigation, adjustment, or reset.

### 2.8.3. Secure Retirement: For AI systems or models that are no longer used,

the responsible unit shall retire them in accordance with established procedures and ensure that model-weight files and training data are destroyed in an unrecoverable manner.

## 2.9. Risk Assessment and Incident Response

### 2.9.1. Risk Assessment:

Before introducing a large-scale AI project, an AI Impact Assessment shall be conducted to analyze its impact on organizational security.

### 2.9.2. AI Risk Classification:

| Risk Type                  | Description                                                     |
|----------------------------|-----------------------------------------------------------------|
| Data Leakage               | Entering sensitive data into public AI services (e.g., ChatGPT) |
| Model Hallucination        | AI generates inaccurate information                             |
| Regulatory Noncompliance   | Failure to comply with personal-data or AI regulations          |
| Intellectual Property Risk | Generated content infringes intellectual property rights        |
| Information Security Risk  | Prompt Injection / Data Poisoning                               |
| Decision Risk              | Inaccurate AI-assisted decisions                                |

### 2.9.3. Incident Response and Material Changes:

Risks shall be reassessed when an AI incident occurs or when a material change is made to a model, agent, or supplier.

### 2.9.4. Tiered Management of AI Use

| Risk Level               | AI Use                                                                                                                                   | Control Method                                                                                                   |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Level 1<br>(Low Risk)    | <ul style="list-style-type: none"> <li>Searching public information.</li> <li>Document assistance (excluding sensitive data).</li> </ul> | May be used directly (training required).                                                                        |
| Level 2<br>(Medium Risk) | <ul style="list-style-type: none"> <li>Use of internal, non-sensitive data.</li> <li>AI-assisted analytical reports.</li> </ul>          | <ul style="list-style-type: none"> <li>Approval by the unit manager.</li> <li>Data de-identification.</li> </ul> |
| Level 3<br>(High Risk)   | <ul style="list-style-type: none"> <li>Involves personal, financial, or</li> </ul>                                                       | <ul style="list-style-type: none"> <li>Information-security review and</li> </ul>                                |

|       |                                                                                                                                                  |                                                                                                                           |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Risk) | <p>confidential information.</p> <ul style="list-style-type: none"> <li>Automated AI decisions (e.g., risk control or legal matters).</li> </ul> | <p>compliance review.</p> <ul style="list-style-type: none"> <li>Prepare an AI risk assessment report (AI RA).</li> </ul> |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|

#### 2.9.5. Violation and Exception Handling:

2.9.5.1. All Company personnel who, due to business needs or a specific purpose, are unable to comply with this Policy or related rules shall complete the exception-management approval process in advance and obtain authorization from the department-level manager of the requesting unit and approval from the head of the Information Security Promotion Team before an exception may be granted.

2.9.5.2. If a violation of this Policy results in the leakage of Company confidential information and is substantiated after investigation, the matter may be handled in accordance with the Company's Employee Rewards and Disciplinary Measures and other applicable Company rules.