

WNC Artificial Intelligence Security Management Policy

1. Corporate Governance Commitment and AI Development Guidelines

WNC Corporation and its affiliated entities (hereinafter referred to as “the Company”) are committed to leveraging Artificial Intelligence (AI) technologies to enhance operational efficiency and innovation, while establishing a comprehensive governance framework that ensures AI usage adheres to the highest standards of information security, legal compliance, data privacy protection, and environmental sustainability. This policy sets out the Company's AI governance principles, approved tools inventory, data protection measures, and accountability mechanisms to all stakeholders.

1.1 Governance Structure

The Company plans to establish an AI Governance Committee, convened by the Chief Information Officer (CIO), responsible for reviewing AI development strategies and resource allocation, granting final approval for high-risk applications, and approving non-standard tool onboarding. The Committee shall hold governance review meetings annually, and initiate dynamic risk-driven reviews of major security incidents, regulatory changes, or significant architectural changes.

1.2 Responsible AI Usage

The Company supports the responsible use of AI to improve work efficiency and empower employees. For Agentic AI with autonomous execution capabilities — such as accessing local resources, executing system commands, and integrating third-party extensions — the Company applies more stringent governance principles to ensure all automated operations remain secure and controlled.

2. Scope of Application

This Policy applies to the AI systems, models, data, APIs, applications, knowledge bases, development tools, and related infrastructure owned, managed, developed, procured, deployed, or used by the Company and its affiliated entities, including but not limited to various official, production, development, testing, or sandbox environments (collectively, the "AI Tools and Platforms"). The parties subject to this Policy include all employees of the Company, dispatched and contract personnel, and suppliers and customers who use the Company's AI Tools and Platforms for business purposes (collectively, the "Stakeholders of this Policy").

3. Approved AI Tools & Platforms

When conducting business activities, stakeholders covered by this Policy shall prioritize the use of AI systems or platforms introduced or developed for the enterprise by the Digital and Management Information Services Department (DMIS), as well as tools approved by the AI Governance Committee.

3.1 Company-Internal AI Platforms

Stakeholders subject to this Policy shall prioritize the use of the following AI tools and platforms that have been introduced or established by the Company.

a. Orion AI

Orion AI is the Company's enterprise-grade AI integration platform, providing model integration capabilities and support for application development. Stakeholders subject to this Policy should prioritize using this platform for all generative AI tasks.

b. Microsoft Copilot (Enterprise)

Microsoft Copilot (Enterprise) is an AI assistant integrated into the Microsoft 365 (M365) ecosystem. Its use must strictly comply with M365's enterprise data protection requirements to ensure that business data is not used to train public models. Stakeholders subject to this Policy should also prioritize using this tool.

c. Other Approved Tools

Stakeholders subject to this Policy may also use AI systems introduced or established for the enterprise by the Digital and Management Information Services Department (DMIS), as well as tools approved by the AI Governance Committee.

3.2 Tool Application and Approval Process

When stakeholders subject to this Policy need to use approved standard tools, such as Orion AI or Microsoft Copilot, they shall submit an application through the Company's ITSR process.

4. Restricted AI Systems

To ensure data security and the protection of intellectual property rights, the following categories of AI systems and tools are subject to usage restrictions. Before using any restricted tools, stakeholders subject to this Policy shall complete an AI risk self-assessment or obtain review and approval from the AI Governance Committee, and it is strictly prohibited to input the Company's sensitive data into any restricted AI systems or tools.

a. Embedded AI Tools & Frameworks

Open-source or proprietary packages, vector databases, and similar components used in R&D projects must comply with corporate security and compliance requirements. Agentic AI/AI Agents — systems capable of autonomous retrieval, code execution, local file access, browser and SaaS operations, or installation and execution of third-party extensions — are classified as high-risk due to their high-privilege operational characteristics, and may only be used after completing a project review by DMIS and the AI Governance Committee.

b. Third-Party Browser Extensions

For AI extensions with web-reading, data-scraping, or automatic translation capabilities, stakeholders subject to this Policy shall, prior to installation, have their respective business unit conduct and document a self-assessment of security risks, and may consult the Cybersecurity Department when necessary.

c. Specific Open-Source and High-Risk Collaboration Tools

Agentic AI tools with autonomous execution capabilities, such as OpenClaw (including predecessors or derivative names Clawdbot and Moltbot), Claude Cowork, and other Agentic AI platforms that have not passed the Company's security review, are prohibited from Company network access; unauthorized installation or integration is strictly prohibited. Use is permitted only after DMIS security assessment and AI Governance Committee approval for special business requirements.

d. Others

For other categories of AI tools — particularly those involving the integration of the Company's sensitive data with cloud-based AI platforms or the adoption of third-party AI services — the relevant department head shall review and approve the request based on an assessment of its business value. The Cybersecurity Department shall collaborate in evaluating the technical feasibility and compliance approach.

5. Prohibited AI Systems

Based on the European Union Artificial Intelligence Act (EU AI Act) and the Company's information security and compliance requirements, the Company strictly prohibits the development, deployment, use, or sale of the following types of AI systems, including but not limited to:

a. Unauthorized Public AI Tools

The input of the Company's confidential information, customer confidential information, research and development and technical data, personal data, or project code into unreviewed public AI platforms—including various free personal-use versions and services without a signed enterprise confidentiality agreement—is strictly prohibited.

b. Manipulative Behavior AI

AI systems that use subliminal, deliberately manipulative, or deceptive techniques to materially distort a person's behavior.

c. Vulnerability Exploitation AI

AI systems that exploit vulnerabilities arising from age, disability, or specific socioeconomic situations, thereby materially distorting behavior.

d. Social Scoring Systems

AI systems that evaluate or classify individuals based on their social behavior or personal characteristics over a period of time, resulting in unfavorable treatment in unrelated contexts.

e. Unauthorized Biometric Surveillance

Real-Time Remote Biometric Surveillance AI systems that perform real-time remote biometric identification of unspecified persons, without their active involvement, in public spaces or spaces accessible to the general public (e.g., real-time facial recognition and tracking). One-to-one biometric verification whose sole purpose is to confirm that a specific person is who they claim to be (e.g., access control, device unlock, account authentication) is not prohibited under this item and shall be managed as High-Risk under Section 6.2.

f. Human Surveillance via Biometrics

Intrusive Biometric Applications AI systems that (1) continuously track or monitor specific individuals or groups through facial recognition or other biometric features without notice or a lawful basis; (2) use biometric data to infer a person's race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; or (3) create or expand facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage.

6. AI System Risk Classification Framework

The Company establishes a four-tier risk classification framework for AI systems based on their application scenarios, data sensitivity, impact level of automated decision-making, autonomous execution privileges, and potential impact on stakeholder rights, serving as the foundation for differentiated governance and resource allocation.

6.1 Prohibited

"Prohibited" refers to AI systems whose development, deployment, use, or sale is absolutely prohibited by the Company. All types defined under the aforementioned "Prohibited AI Systems" fall within this tier, and no unit may submit a request for exemption.

6.2 High-Risk

"High-Risk" refers to AI systems that may have significant adverse impacts on human rights, safety, health, or property, including but not limited to: agentic AI capable of autonomously executing system instructions; customer-facing AI that processes sensitive data; facial recognition and biometric identification systems; AI systems that may affect employee rights and interests; and automated decision-making systems that may affect the rights and interests of customers or suppliers. High-risk AI systems must undergo a dedicated review by the AI Governance Committee before deployment, undergo a human rights impact assessment, establish a human-in-the-loop (HITL) mechanism, and maintain complete technical documentation and review records. AI systems involving facial recognition or biometric identification shall additionally complete a personal data protection impact assessment, provide prior notice and a non-biometric alternative where applicable, and ensure that biometric data is stored in encrypted form with a defined retention period.

6.3 Limited-Risk

"Limited-Risk" refers to AI systems that interact with individuals and require users to be informed, such as generative AI content intended for external use, customer service assistance tools, and AI-enabled features made available on public websites. Such systems must clearly disclose that they are AI-generated or AI-driven before the interaction or within the content itself, and must provide users with the ability to make choices or access a complaint channel.

6.4 Minimal-Risk

"Minimal-Risk" refers to AI tools intended solely for internal use that do not process sensitive data or produce external impacts, such as document drafting and editing

assistants, code auto-completion tools, and internal data analysis tools. Such tools shall comply with the Company's general information security and compliance requirements. No additional dedicated project review is required; however, they shall be included in the AI system inventory for centralized management.

6.5 Dynamic Risk Classification Management

Initial risk classifications are proposed by business units and finalized following review and approval by the Cybersecurity Department and the AI Governance Committee. When an AI system's application scenario, data category, or technical architecture undergoes significant changes, its risk tier must be reassessed.

7. Data Protection and Privacy Safeguards

The Company places data security and the protection of personal privacy at the core of its AI governance. Throughout the entire lifecycle of the design, development, and operation of all AI Tools and Platforms, applicable data protection laws and regulations shall be complied with.

7.1 Data Classification and Control

It is strictly prohibited to input sensitive data — including company confidential information, product designs, core source code, keys and certificates, undisclosed financial data, employee personal data, supplier quotations, and controlled technologies — into any public AI platform or uncontrolled third-party service.

7.2 De-identification Processing

Business units shall ensure that personal identifiers are removed or appropriately transformed before data is submitted to an AI system. Re-identification risks arising from combinations of data attributes shall be assessed and mitigated in accordance with applicable privacy and information security requirements.

7.3 Secret Key Governance

All AI service API encryption keys and certificates must be stored in managed secrets management systems; plaintext storage is strictly prohibited. Key issuance shall be restricted to service accounts, and local storage on personal devices is strictly forbidden.

8. Transparency, Explainability and Accountability

The Company is committed to ensuring that AI Tools and Platforms are transparent and explainable, by clearly disclosing their intended purposes, capabilities, limitations, data sources, and associated risks, thereby enabling stakeholders to fully understand how the AI

Tools and Platforms operate. All content produced by AI Tools and Platforms shall undergo substantive review by appropriately qualified personnel before being formally released or acted upon, to ensure that humans retain final decision-making authority and that legal and administrative accountability is properly assigned.

8.1 Final Review Responsibility (Human-in-the-Loop)

All AI-generated content shall be treated as a “draft” or “reference baseline.” Users are ultimately responsible for proofreading and shall apply professional judgment to identify and filter out model hallucinations, thereby ensuring the accuracy and professional quality of the output. The person performing the relevant task shall be responsible for any business consequences arising from the output. When the output of agentic AI involves code changes, system configuration changes, data processing, or the automated execution of external communications, it shall not be used directly as the basis for final decision-making or automatic execution. Appropriate human review must be completed before any such action is taken.

8.2 Stakeholder Requirements

AI-assisted research and development deliverables or official documents shall be reviewed in advance to ensure compliance with the contractual requirements of customers or other stakeholders.

9. Ethics, Fairness and Bias Management

The Company is committed to ensuring that AI Tools and Platforms do not perpetuate existing inequalities or give rise to new forms of discrimination.

9.1 Training Data Diversity and Representativeness

Datasets used for AI model training or fine-tuning shall be diverse and representative, covering relevant characteristics across demographic groups to avoid discriminatory or unfair model outputs due to data bias.

9.2 Sensitive AI Capability Access Control

Strict access controls are implemented for sensitive AI applications that may raise ethical or privacy concerns (e.g., facial recognition, biometric surveillance, emotion analysis).

9.3 AI Ethics Officer

The Company plans to establish a dedicated AI Ethics contact point to serve as the primary point of contact for all AI ethics-related inquiries. Its responsibilities include providing ethical consultation and guidance, coordinating the review of high-risk AI use cases, and coordinating regular AI model fairness assessments and bias audits.

10. Environmental Sustainability and Ecological Footprint Management

The Company is committed to honoring its environmental management commitments throughout the development, deployment, and use of AI Tools and Platforms, taking carbon reduction and efficiency performance into consideration across the entire lifecycle of AI solutions. The Company requires that both proprietary and third-party AI data centers and models maintain a low ecological footprint, and shall continuously monitor and improve their environmental impact, with considerations including but not limited to: green design, infrastructure optimization, supply chain requirements, hardware lifecycle, and monitoring and improvement.

10.1 Ecological Footprint Monitoring Metrics

The AI Governance Committee periodically reviews quantitative indicators and improvement progress for AI data centers and models—including energy consumption, water usage, and carbon emission intensity.

11. Risk Management and Security Guardrails

The Company has established multi-layered security protection measures and risk management mechanisms throughout the development and operation and maintenance of AI Tools and Platforms.

12.1 Security Guardrail Mechanism

AI development teams shall deploy dynamic filtering mechanisms at AI interfaces to intercept malicious instructions in real time and proactively defend against system vulnerabilities. Agentic AI tools with external tool-calling capabilities shall implement the Principle of Least Privilege and enforce execution controls. Agentic AI tools that do not possess the aforementioned control capabilities shall not be used on the Company's network or devices.

12.2 Prompt Engineering Security

Developers implement defensive prompt engineering: prompts must not contain hard-coded credentials, keys, or highly identifiable system architecture details; the risks of prompt leakage and prompt injection attacks must be mitigated. For tasks

requiring high accuracy, parameters should be tuned (e.g., setting the temperature parameter close to 0) to maximize output determinism.

12.3 Emergency Response

When a Company AI Tool or Platform is identified as having experienced a major information security vulnerability, a sensitive data breach, or the generation of content posing a legal compliance risk, the Cybersecurity Department shall have the ultimate authority to activate the "Emergency Forced Shutdown Mechanism," requiring the responsible unit to perform an immediate shutdown or service isolation to contain the damage and ensure compliance. Should the RAG knowledge base suffer data poisoning or malicious contamination, the affected indices shall be cleared immediately, and after the contamination source has been eliminated, data cleansing and re-ingestion processes shall be re-executed.

12. AI Decision Appeals Mechanism

The Company plans to establish an AI Decision Appeals Mechanism, applicable when users or third parties affected by AI-driven decisions object to decisions or outputs made by AI systems.

13.1 Appeals Handling Process

Appeals shall be received and coordinated by the AI Ethics Officer. The handling process includes: acknowledging receipt and providing case tracking; assessing the validity, severity, and scope of the appeal, with suspension of the relevant AI system when warranted; investigating the decision basis, data inputs, and model behavior in coordination with business units and the Cybersecurity Department; and issuing a written response to the appellant with findings and corrective measures. Dissatisfied appellants may request a review by the AI Governance Committee. Specific acceptance criteria, handling timelines, and operational procedures shall be established by the AI Governance Committee separately.

13.2 Records and Reporting

All appeal cases — from receipt, investigation, and resolution to corrective measures—shall be documented in detail, compiled periodically, and submitted to the AI Governance Committee for review. Appeal statistics shall serve as reference indicators for AI governance reviews.

13.3 Official Reporting Email

Official reporting email: security.issues@wnc.com.tw

13. Employee Training and Security Awareness

The Company builds a culture of responsible AI usage through systematic training and continuous awareness programs. New employees shall complete AI security training during onboarding to understand the Company's AI usage policies and security operational standards, ensuring they possess an appropriate understanding of tool usage and risk prevention capabilities before commencing business activities. Additionally, the Cybersecurity Department annually issues security bulletins on emerging AI threats and incorporates them into regular educational resources to continuously enhance the organization's defensive resilience against AI-related risks.

14. Regulatory Compliance & Governance Standards

The Company's AI governance framework aligns with international and domestic regulations and standards to ensure the legality, compliance, and alignment with international practices of AI applications.

15. Policy Review and Revision

This policy has been reviewed and approved by the Chief Information Officer (CIO), and shall be periodically reviewed and revised to ensure that the Company's AI governance direction aligns with stakeholder expectations and applicable standards. The AI Governance Committee conducts annual regular governance reviews to monitor regulatory changes, emerging risk topics, and implementation effectiveness.