



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

Responsible AI Guidelines

■ Purpose

While Artificial Intelligence (AI) brings convenience to people's lives and enhances workplace productivity, it may also pose risks such as bias and discrimination, disclosure of confidential information, cybersecurity threats, infringement of privacy and personal data, violation of intellectual property rights, and the generation of inappropriate content. Employees shall use AI responsibly, taking into account sustainable development and maintaining meaningful human oversight and autonomy.

■ Applicability and Scope

This Policy applies to all departments and employees of the Company involved in the development or use of Artificial Intelligence (AI) applications. For procurement activities conducted by the Company, the responsible business units shall require the awarded suppliers, organizations, or individuals to comply with this Policy and its associated Guidelines and Standards.

■ AI System Management Policy

✓ Privacy and Security by Design

Security – Protect AI systems and information assets.

Privacy & Personal Data Protection – Respect privacy and safeguard personal data.

✓ Fairness and Bias Mitigation

Fairness & Non-Discrimination – Minimize bias and promote fair, inclusive outcomes.

✓ Transparency and Human-in-the-Loop

Transparency & Explainability – Ensure AI operations and outputs are understandable.

Human Oversight – Maintain human review for critical decisions and allow human intervention when needed.



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

✓ **Accountability and Clear Boundaries**

Accountability – Define clear ownership and responsibilities for AI systems.

Clear Boundaries – Clearly define what AI is permitted and prohibited to do.

✓ **Environmental Sustainability and Ecological Responsibility**

Low Ecological Footprint – Promote Green AI and require Company-owned or third-party AI models and data centers to minimize environmental impact.

✓ **Prohibited AI Applications**

Ethical Red Lines – Prohibit the use or deployment of AI systems involving manipulation, exploitation of vulnerable groups, social scoring, or unauthorized biometric surveillance, consistent with the prohibited practices defined under the EU AI Act.

■ **Responsible AI Governance and Oversight Mechanism**

To ensure the effective implementation of the Responsible AI Policy, the Company has established a cross-functional Artificial Intelligence Management Office (AIMO) responsible for the governance, oversight, development, and continuous improvement of AI-related management mechanisms. The AIMO is led by the Information Security Management Office and integrates existing governance frameworks, policies, and management processes. Relevant departments participate in the AIMO to support cross-functional decision-making and oversight. The specific roles, responsibilities, authorities, and accountabilities of participating departments shall be defined and maintained through the Company's internal management procedures.

■ **AI Applications and Associated Risks**

Practical Applications of Artificial Intelligence

Business units may leverage Artificial Intelligence (AI) and related Information and Communication Technologies (ICT) across a wide range of use cases, including but not limited to the following application scenarios:

Education and Training



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

AI may be utilized to enhance educational quality and professional training, including but not limited to:

- Improving training administration efficiency;
- Developing diverse learning resources;
- Analyzing employees' learning progress and recommending personalized learning content;
- Identifying workforce skill requirements to strengthen professional training programs; and
- Supporting the development of education and training policies.

Intelligent Customer Service

AI-powered chatbots may be used to improve employee services, including but not limited to:

- Responding to frequently asked questions;
- Identifying employee needs and directing inquiries to the appropriate departments;
- Assisting employees in accessing company-related information; and
- Supporting the handling of routine and standardized administrative tasks.

Policy Communication and Engagement

AI may be used to strengthen policy communication and stakeholder engagement, including but not limited to:

- Analyzing public or employee sentiment;
- Identifying employee needs and pain points;
- Supporting the delivery of service information tailored to employee needs; and
- Assisting in the preparation of communication materials and policy awareness content.

Healthcare

AI may be utilized to improve healthcare quality and public health, including but not limited to:

- Enhancing healthcare administration efficiency;
- Monitoring and analyzing outbreaks of epidemics and infectious diseases;
- Analyzing medical records and diagnostic images;
- Supporting drug discovery and efficacy prediction;
- Improving the quality of long-term care services; and
- Assisting in the development of healthcare-related policies.



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

Data Analytics

AI may be used for data cleansing, format conversion, feature extraction, data mining, analysis, and visualization. These capabilities help organizations identify issues, perform deeper analysis, and support informed decision-making.

AI Assistants

Across the application scenarios described above and other emerging use cases, software applications, online services, or devices developed using AI technologies—such as machine learning, natural language processing, and related techniques—that function as virtual assistants to support business activities may be broadly categorized as AI Assistants.

Examples include:

- Email processing;
- Schedule and calendar management;
- Automated document generation; and
- Other productivity-enhancing support functions.

The application scenarios described above are provided for illustrative purposes only. As AI technologies continue to evolve and become more widely adopted, the range of AI applications is expected to extend beyond the examples listed in this document.

■ **AI Usage Risks and Limitations**

Practical Applications of Artificial Intelligence

While the use of Artificial Intelligence (AI) can improve efficiency and enhance the quality of decision-making, it may also introduce risks arising from inappropriate use or even legal non-compliance. AI usage scenarios are therefore categorized into Prohibited Uses, High-Risk Uses, Medium-Risk Uses, and Low-Risk Uses. The following section describes Prohibited Uses.

Prohibited Uses

The use of AI involving sensitive information, personal privacy data, confidential business information, or information that has not been authorized for public disclosure by the Company is generally prohibited. Likewise, the processing of special categories of personal data without legal basis and prior



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

consent, or the use of AI to make decisions affecting the rights and interests of employees or external parties without human review and validation, shall be strictly prohibited.

Examples of prohibited uses include, but are not limited to, the following:

A. Use of Sensitive or Confidential Information

When AI systems process sensitive information, confidential business information, or data that has not been approved for public disclosure by the Company, such use is strictly prohibited unless the AI system is deployed within a Company-controlled environment, such as an internally managed data center, an isolated on-premises infrastructure without external network connectivity, or an equivalent environment providing the same level of information security protection. Any approved use must also comply with the applicable data classification requirements.

B. Unauthorized Biometric Identification

The use of AI for facial recognition, fingerprint recognition, or other forms of biometric identification without a legal basis and the prior consent of the data subject is strictly prohibited.

C. Unauthorized Processing of Special Categories of Personal Data

The use of AI systems to process or analyze special categories of personal data—including medical records, healthcare information, genetic data, information concerning an individual's sex life, health examination records, or criminal records—without a legal basis and the prior consent of the data subject is strictly prohibited.

D. Automated Decisions Affecting Rights and Obligations

The use of AI to directly make administrative, employment-related, legal, or other decisions that affect an individual's rights, obligations, or interests without prior human review and confirmation is strictly prohibited.

E. Automated Scoring or Evaluation of Individuals

The use of AI to directly score, rank, evaluate, or assess individuals without prior human review and validation is strictly prohibited.

These prohibitions are intended to protect privacy, ensure legal and regulatory compliance, safeguard individual rights, and promote the responsible and trustworthy use of AI within the Company.



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

■ Responsible AI Development and Application Management

The risk owner of an AI development project shall define the objectives, intended use, and operational boundaries of the AI system. Based on these objectives, cross-functional collaboration involving Information Technology, Legal, Ethics, and other relevant stakeholders shall be established to: Identify risks throughout the AI lifecycle, including Initiation, Design & Development, Verification & Validation, Deployment, Operation & Monitoring, Reassessment, and Retirement. Conduct risk and impact assessments, considering confidentiality, integrity, and availability, as well as potential impacts on individuals, groups, society, and sustainability. Conduct risk and impact assessments, considering confidentiality, integrity, and availability, as well as potential impacts on individuals, groups, society, and sustainability.

The following management responsibilities shall apply to all AI applications:

(1) Accountability

Users of AI systems are responsible for the content generated by such systems, including ensuring its accuracy and compliance with applicable legal and ethical requirements. As AI-generated outputs may still contain hallucinations or other unacceptable errors, any AI-generated text, images, videos, or other content must be reviewed and verified before use. Compal's AI Management Office, operating in accordance with ISO/IEC 27001 and with reference to ISO/IEC 42001, is responsible for AI governance, risk management, and regulatory compliance. Through mechanisms for investigating and addressing AI-related errors or harm, as well as maintaining auditable data and models, the Company ensures clear accountability among developers, users, and management.

(2) Cybersecurity

In accordance with the Company's information security classification and protection requirements, appropriate cybersecurity controls and safeguards shall be established, maintained, and updated based on factors such as the type, volume, and sensitivity of information processed, as well as the scale and nature of the information systems involved. These measures are intended to protect data, systems, devices, networks, and personnel, and to reduce the risks of theft, misuse, disclosure,



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

alteration, or destruction of information assets resulting from human error, malicious actions, or natural disasters. When using AI systems, employees shall carefully select AI platforms and tools, review the applicable terms of use, and ensure compliance with the Company's information classification requirements to prevent the disclosure of Company or customer confidential information. When using external or public AI services, users must assume that all inputs and outputs may be recorded or retained by third parties. Unless using Company-approved AI systems that are self-hosted or isolated from public networks, employees shall not use AI systems to process, generate, or submit sensitive or confidential information.

(3) Transparency and Explainability

Transparency – AI systems shall provide an appropriate level of transparency regarding their purpose, capabilities, limitations, data sources, and associated risks.

At a minimum, users should be:

1. Informed when they are interacting with an AI system.
2. Provided with information on how their data will be processed by the AI system.
3. Informed of any choices available to them during their interaction with the AI system.
4. Made aware of their right to question or appeal AI-generated outcomes.

AI systems shall incorporate traceability measures throughout their lifecycle and maintain ongoing processes for evaluating the quality and sources of input data. Records of datasets, data collection methods, data labeling activities, and algorithms used in AI decision-making should be maintained to support transparency and auditability.

Explainability – AI systems should employ methods and processes that enable users to understand the basis, reasoning, and decision-making logic behind AI-generated outputs. To the greatest extent practicable, Company-developed AI systems shall be designed, implemented, and used in a manner that allows decisions and results to be explained and that clearly demonstrates the relationship between user inputs and generated outputs.



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

(4) Fairness and Non-Discrimination

Avoiding potential bias in the use and/or development of AI. When using AI systems to generate text, images, videos, or other content, users shall ensure that the outputs are fair, inclusive, and free from discrimination based on race, ethnicity, gender, socioeconomic status, or any other protected characteristic.

AI models may produce biased outcomes due to unrepresentative training data, sampling bias, or bias introduced during data labeling and model development. Therefore, all AI-generated content shall be subject to human review and, where necessary, revised and validated to mitigate potential bias and ensure fairness.

(5) Data Privacy and Personal Data Protection

The development and use of AI systems shall comply with the Company's [Compal Group Personal Data and Data Privacy Protection Policy and Guidelines](#). Personal and privacy (sensitive) data used by AI systems shall follow the principles of data minimization and, where applicable, be anonymized or de-identified. Users shall ensure that data entered into AI systems, as well as AI-generated outputs, do not contain personal or privacy-sensitive information. Where employee personal data is involved, appropriate de-identification measures shall be applied prior to use.

(6) Keeping humans “in the loop” for critical decisions and allowing human intervention

Appropriate human “in the loop” and intervention mechanisms shall be established throughout the AI system lifecycle to ensure effective control and supervision. AI-generated outputs shall be subject to human review and, where necessary, intervention to ensure their validity, reasonableness, and accuracy. Mechanisms shall be in place to identify and correct potential biases, errors, or unintended outcomes. For material, high-risk, or irreversible decisions, appropriate human review and approval processes shall be maintained. AI outputs may serve as decision-support tools, but final decisions shall remain subject to human judgment and shall not be made solely by AI without human “in the loop”

(7) Environmental and Ethical Impact



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

Environmental Responsibility

The environmental impact of AI systems shall be considered throughout their design, development, and deployment. Relevant factors including sustainability, resource conservation, and ecological stability should be assessed. Where reasonably practicable, Requiring Company-owned or outsourced AI-related computing resources (such as data centers and AI models) to have a low ecological footprint.

Ethical Responsibility

Ethical principles, including integrity, human rights, and the rule of law, shall be incorporated throughout the AI system lifecycle. The Company shall not develop, deploy, or use AI systems that involve manipulative practices, exploitation of vulnerable individuals, social scoring, or unauthorized biometric surveillance. Prohibited AI applications include, but are not limited to:

- (a) AI systems that employ subliminal influence or manipulative techniques;
- (b) AI systems that exploit an individual's vulnerabilities, including those related to age, physical or mental conditions, or other circumstances;
- (c) AI systems that classify or profile individuals in a discriminatory manner based on social behavior, socioeconomic status, race, ethnicity, or other sensitive personal attributes;
- (d) AI systems trained on or using biometric data indiscriminately collected from social media or publicly available sources;
- (e) AI systems that collect sensitive personal data for profiling or the creation of individual behavioral profiles.

By adopting responsible AI practices, the Company strives to reduce environmental and societal risks while fostering sustainable innovation.

(8) Training and Responsible Use

Users of AI systems shall understand the risks and limitations associated with AI and learn how to effectively leverage its capabilities to enhance work quality and productivity. This includes developing effective prompting skills to improve the performance and usefulness of AI systems. Compal shall provide regular privacy protection training to all personnel and periodically assess the effectiveness of such training programs.



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

■ Zero-Tolerance Policy

Compal adopts a zero-tolerance approach to violations of AI governance requirements. Any employee found to be in violation of this Policy may be subject to disciplinary action in accordance with the Company's personnel management policies and employee disciplinary regulations. Serious violations may also be referred to the relevant authorities in accordance with applicable laws and regulations.

■ Complaints and Reporting

Any employee, external organization, or individual who becomes aware of an incident that may affect individual rights and interests—including issues relating to AI privacy protection, fairness, or bias—or who suspects a violation of this Policy, may submit a complaint or report through the Privacy Protection Hotline: +886-2-8797-8588 ext. 14385 and Email: Compal_PIR@compal.com. Compal will maintain the confidentiality of reporters' information and take appropriate measures to protect their rights and interests.

- This Policy may be revised from time to time to support the effective governance of Responsible AI. Any updates will be published on the Compal website upon approval. Users are encouraged to review the Responsible AI Policy and Guidelines periodically to stay informed of the latest requirements and relevant information.

■ Supplementary Provisions

Article 1 The Principles take effect after approval of the board of directors and also could be revised as the same approval.

Article 2 The Guidelines were adopted of BOD Meeting on Aug 13, 2026.