Berli Jucker Public Co., Ltd.

Responsible Artificial Intelligence Policy	Reference number : SRMD 01/2026
	Review Date : -
	Approval Date : 30 July 2026
	(Executive Board Meeting No.4/2026)
	Effective Date : 30 July 2026
	Supersede Date : -

Berli Jucker Public Company Limited and its group companies (hereinafter collectively referred to as the "BJC Group") recognize the strategic importance of Artificial Intelligence (AI) and are committed to its responsible development, adoption, deployment, and use to foster innovation, enhance operational excellence, create sustainable business value, and uphold the interests of all stakeholders.

The BJC Group recognizes the potential risks and impacts associated with the use of Artificial Intelligence (AI). Accordingly, this Policy has been established to provide an enterprise-wide governance framework and operational guidelines for the responsible development, adoption, procurement, integration, deployment, and use of AI. The Policy aims to ensure that AI is implemented in a manner that is responsible, secure, transparent, fair, and accountable; respects privacy; and complies with applicable laws, business ethics, information security standards, and the BJC Group's sustainability commitments.

Policy Scope

This policy applies to the business operations under Berli Jucker Public Company Limited and its subsidiaries.

Guidelines

1. AI Governance and Risk Management

AI systems that are developed, adopted, procured, integrated, or deployed shall have a clearly defined business purpose and be subject to appropriate governance and risk management throughout their lifecycle. Governance and risk management measures shall take into consideration the nature of the data involved, the criticality of the business process, the potential impact on stakeholders, and the organization's risk appetite. AI systems classified as high-risk or those with significant business, legal, or ethical impacts shall be subject to appropriate review, approval, and governance prior to deployment.

2. Data Privacy and Protection

The use and development of AI shall respect privacy and protect personal data throughout the AI system lifecycle in compliance with applicable data protection laws and regulatory requirements. Data shall be collected, accessed, and used only to the extent necessary and for authorized purposes, and be subject to appropriate governance and control measures. Personal data, customer information, employee information, confidential business information, and other sensitive data shall not be used in AI systems in any

inappropriate manner that could adversely affect the rights, trust, or legitimate interests of the Company and its stakeholders.

3. Cybersecurity of AI Systems

AI systems, applications, models, platforms, and services used or developed by the organization shall be protected through cybersecurity and information security controls commensurate with their risk levels. Such controls shall safeguard AI assets, data, and supporting infrastructure against cyber threats, unauthorized access, data leakage, data manipulation, system compromise, and other AI-related security risks. Appropriate measures shall also be implemented to secure the development, deployment, integration, and use of AI, including controls over connectivity, access, third-party AI services, and unapproved AI tools, to prevent cybersecurity incidents and mitigate risks arising from harmful, inaccurate, or inappropriate AI-generated outputs.

4. Fairness and Bias Management

The design, use, and development of AI shall promote fairness, mitigate the potential risk of bias, and avoid discrimination or inappropriate adverse impacts on individuals or groups. The use of AI to generate, reinforce, or amplify unfair or discriminatory outcomes, or to adversely affect the legitimate rights and opportunities of individuals, shall not be permitted.

5. Human Oversight and Intervention

The use of AI in critical decisions or decisions that may have a significant impact on individuals, businesses, or the Company shall be subject to appropriate human oversight. AI-generated outputs shall not be used as the final basis for high-risk decisions without appropriate human review, assessment, approval, and the ability to intervene or override by an authorized and accountable individual.

6. Transparency and Explainability

The use of AI shall be conducted with a level of transparency commensurate with its risk level and context of use. Users, service recipients, and other relevant stakeholders shall be informed, in an appropriate manner, when they are interacting with an AI system or when AI-generated outputs are used to support decision-making. AI systems shall be designed to provide explanations for their outputs, including the underlying rationale, limitations, and key influencing factors, at a level appropriate for the intended stakeholders.

7. Accountability for AI Outcomes

Clear roles, responsibilities, and accountability shall be established for the governance, approval, development, deployment, use, monitoring, and

oversight of AI. The use of AI shall not diminish, transfer, or exempt the accountability of individuals, organizational units, or decision-makers responsible for AI-enabled activities, outcomes, or decisions. Human accountability shall be maintained for decisions informed by AI-generated outputs, including the assessment of their appropriateness, accuracy, and impacts.

8. AI Usage Boundaries

The use of AI shall be subject to clearly defined purposes, scope, and usage conditions to establish clear boundaries on what AI systems are permitted and not permitted to do. This is intended to prevent misuse, mission creep, and inappropriate or unlawful use in violation of laws, organizational policies, or business ethics. Unapproved AI tools or services shall not be used for sensitive data, confidential information, personal data, or high-risk processes.

9. Sustainable AI and Low Ecological Footprint

The use of AI shall be appropriately aligned with business needs, taking into account efficient resource utilization, including energy use, water consumption, and greenhouse gas emissions. Consideration shall also be given to the selection of AI models, AI data centers, cloud services, and AI service providers with a low ecological footprint, as appropriate to the business context, risk level, and availability of alternatives in the market.

10. Prohibited AI Practices

The development, procurement, or use of AI shall not be permitted where it violates applicable laws, human rights, business ethics, fairness, security, or the Company's values. This includes, but is not limited to, the following prohibited practices:

- The use of AI employing manipulative, deceptive, or subliminal techniques to improperly influence or materially distort an individual's behavior.
- The use of AI to exploit the vulnerabilities of individuals or groups.
- The use of AI for social scoring or the classification or ranking of individuals in a manner that results in unfair or disproportionate adverse treatment.
- The use of biometric data, biometric identification, or surveillance of individuals without authorization or in violation of applicable laws.
- The use of AI that may pose significant risks to human rights, fundamental freedoms, safety, or human dignity without appropriate safeguards, governance, and oversight.

The use of AI with sensitive capabilities or high-impact applications, including facial recognition, biometric identification, surveillance, profiling, or automated decision-making in critical contexts, shall be subject to appropriate governance, approval, and controls commensurate with the associated level of risk.

11. Third-Party AI Management

The use of third-party AI, including cloud AI, SaaS AI, APIs, external AI platforms, and vendor AI tools, shall be subject to appropriate assessment and governance covering information security, cybersecurity, privacy, data protection, legal, contractual, and other relevant risks. The use of third-party AI shall be aligned with approved business purposes and shall not expose the Company to risks exceeding its defined risk appetite.

12. Employee Training on the Ethical and Secure Use of Artificial Intelligence (AI)

Employees, users, and other relevant stakeholders shall be encouraged and supported to receive appropriate education and training to enhance their AI knowledge, understanding, and skills. Such education and training shall also promote awareness of the risks, limitations, ethical considerations, and responsibilities associated with the use of AI.

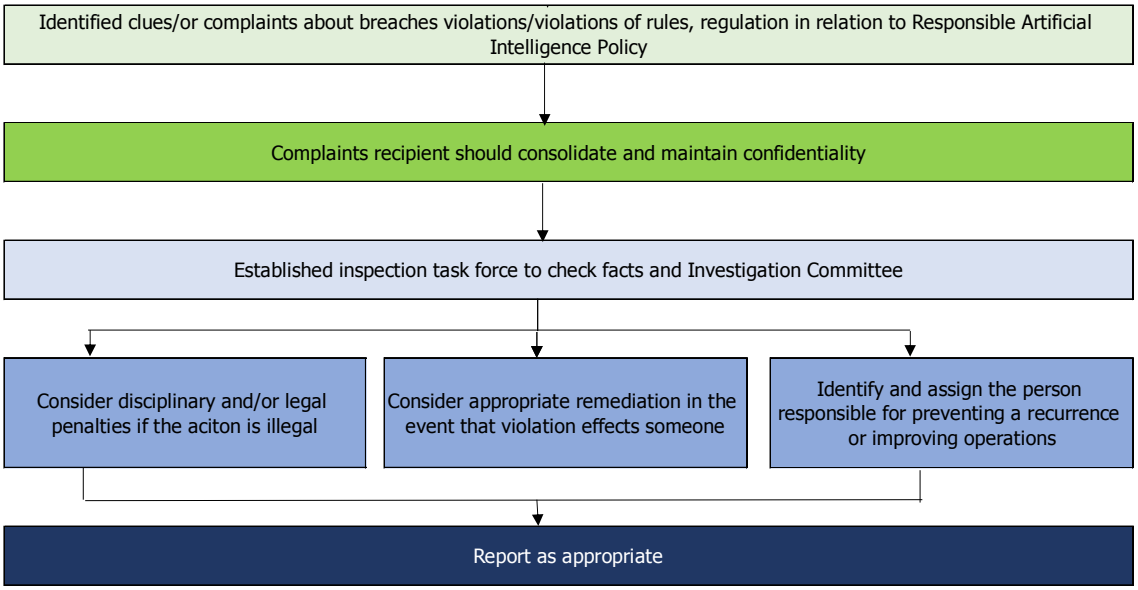
13. AI Monitoring, Review and Improvement

AI systems with significant or high-risk impacts shall be subject to ongoing monitoring and periodic review commensurate with their level of risk to ensure that they remain safe, fair, free from undue bias, transparent, fit for their intended purpose, and do not result in unintended adverse impacts. The Company shall also promote the continual improvement of AI governance to ensure alignment with evolving technologies, applicable laws and regulations, emerging risks, and relevant standards and best practices.

In the event of an actual or suspected violation of applicable laws, regulations, the Company's Code of Conduct, or Company policies, including circumstances in which directors, executives, or employees authorize, condone, or fail to take appropriate action in response to violations committed by their subordinates, directors, executives, employees, and all stakeholder groups are encouraged to report the matter to the Human Resources Department or through the Company's designated whistleblowing and complaint reporting channels.

The Company has established clear reporting procedures and whistleblower protection measures to ensure that all reports are handled confidentially. Upon receipt of a report, the designated recipient will collect the relevant information and refer the matter to the fact-finding team and/or the Investigation Committee for review and investigation in accordance with the Company's established procedures.

Following the investigation, the Company will take appropriate actions based on the findings of each case. Such actions may include disciplinary and/or legal measures, appropriate remediation for affected parties, and corrective and preventive actions to prevent recurrence and strengthen internal processes. The investigation findings and resulting actions will be reported to the designated authority, as appropriate.



The Responsible Artificial Intelligence Policy will be effective from 30 July 2026 onwards.