Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)

Please refer to SinoPac Holdings supervises Bank SinoPac and SinoPac Securities in accordance with the “Guidelines for the Management of Emerging Technology Applications” and the “Detailed Rules for the Application of Artificial Intelligence in Emerging Technologies” to establish an AI governance framework and an Emerging Technology Application Management Committee. In addition, in line with the “Operating Regulations for Financial Institutions Applying Artificial Intelligence Technology” and the “Guidelines on the Use of Artificial Intelligence (AI) in the Financial Industry,” all AI applications have undergone risk self-assessment and cross-functional reviews (including information security, compliance, and risk management). Among these applications, only one has been classified as high risk. Applications involving customer data or external service scenarios are categorized as medium risk and are subject to enhanced controls. Furthermore, in accordance with the “Information Security Management Regulations – Cloud Service Security Management Procedures,” the principles of least privilege and access control are enforced to ensure that access to sensitive AI capabilities are restricted to authorized use only, with comprehensive logging and auditing mechanisms in place. This approach ensures the implementation of risk-based management and responsible AI governance.
Taking Bank SinoPac as an example, its current AI-related applications do not involve specific sensitive technologies (such as facial recognition or surveillance systems). Therefore, these applications are managed under the “Information Security Management Regulations – Cloud Service Security Management Procedures,” which enforce least privilege and access control to ensure that sensitive technologies are used only with proper authorization. For non-cloud systems (including those involving AI applications), the “Application System Authorization Management Rules” clearly define system permissions and access controls, along with complete logging and audit mechanisms, thereby ensuring risk-based management and responsible AI governance.

Distinct labeling of AI-generated content and outcomes of AI-driven decisions
Please refer to SinoPac Holdings supervises Bank SinoPac and SinoPac Securities in adhering to the competent authority’s regulations and guidelines on AI technology operations, and actively enhances information transparency. All current generative AI applications implement distinct labelling of AI-generated content and outcomes of AI-driven decisions (or equivalent wording) at appropriate locations and contexts within user interfaces, generated outputs, and AI-driven decision-making processes. This mechanism has been institutionalized as part of internal control management policies. This approach not only complies with regulatory requirements but also, while balancing information security and commercial confidentiality, implements the principle of accountability within sustainable governance through standardized procedures, thereby strengthening user trust in the application of technology.

Mechanisms to detect and correct drift or degradation of AI models over time
Please refer to SinoPac Holdings, Bank SinoPac, and SinoPac Securities, with reference to the “AI Guidelines for the Financial Industry” and in accordance with the “Regulations on Emerging Technology AI Applications,” have established a comprehensive model monitoring and validation framework to detect and correct drift or degradation of AI models over time. Current application systems not only implement regular compliance monitoring and maintain detailed logs, but also apply full lifecycle management mechanisms—covering pre-deployment validation, in-process monitoring, and post-deployment adjustment—for critical models such as cloud-based conversational systems and risk analytics. Where necessary, manual review is incorporated to ensure system robustness, detect and prevent model drift, and further enhance operational stability and service quality.

Regular assessments of deployed AI models for fairness/bias

Please refer to SinoPac Holdings supervises Bank SinoPac and SinoPac Securities in formally stipulating fairness and ethical principles within the “Regulations on Emerging Technology AI Applications.” Bias assessment and mitigation are conducted during both model development and validation stages. In addition, in accordance with the FSC’s AI guidelines, financial institutions are required to periodically review model outputs to prevent discrimination and ensure the reasonableness of decisions. The current framework already covers pre-

deployment reviews and reassessment upon any model changes. Going forward, a regular fairness testing and audit mechanism (e.g., annual testing and reporting) will be further established and incorporated into internal control processes to strengthen ongoing oversight.

Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models

Please refer to SinoPac Holdings supervises Bank SinoPac and SinoPac Securities in stipulating, under Article 8 of the “Regulations on Emerging Technology AI Applications,” that AI applications must incorporate sustainability principles and be managed with reference to international sustainability goals. At present, energy efficiency has been improved through hardware optimization and resource management. Based on the latest inventory, generative AI applications are largely low-risk and concentrated on a limited number of platforms, enabling scalable energy-saving benefits. In addition, efforts have been made to optimize hardware, enhance computational efficiency, and improve resource allocation. Energy and carbon emission indicators are also being progressively established to strengthen the quantitative management of AI’s environmental impact, thereby advancing green technology practices and sustainable operations.

Appeals process for users/affected third parties to contest an AI decision or outcome

Please refer to Currently, SinoPac Holdings and its subsidiaries provide an appeals process for users and affected third parties to contest AI decisions or outcomes through existing customer service and complaint mechanisms. In addition, the “Detailed Rules for the Application of Artificial Intelligence in Emerging Technologies” stipulate that all AI applications must assess consumer rights and implement risk control measures. In accordance with the FSC’s AI guidelines, financial institutions are encouraged to provide appropriate remediation options to enhance accountability. Going forward, dedicated complaint and handling processes for AI-driven decisions will be established based on specific application scenarios, with clearly defined complaint scopes and response mechanisms, in order to further strengthen transparency and customer trust.

Taking Bank SinoPac as an example, it has already established the “Customer Service Center – Customer Service Operations Manual,” which ensures fair and neutral handling of customer inquiries (including questions and feedback related to AI applications). Additionally, the bank has implemented “Emergency Response Guidelines” to address relevant incidents based on their nature, thereby maintaining customer confidence in the technologies and services provided.

Quantification of the impact of AI initiatives/tools on sustainability outcomes

Please refer to SinoPac Holdings and its subsidiaries leverage AI applications to enhance operational efficiency and optimize resource allocation. Current assessments indicate that multiple AI applications (including generative AI and predictive models) have been integrated into business processes, most of which are classified as low risk and incorporate benefit feedback mechanisms. Through automation, data analysis, and customer service optimization, these applications effectively reduce manual workload and minimize resource waste. Furthermore, a framework for tracking and measuring the the impact of AI initiatives on sustainability outcomes has been progressively established, covering aspects such as improvements in operational efficiency, system processing capacity, and optimization of resource utilization. These efforts are aligned with sustainable development goals, strengthening data-driven ESG management capabilities. This includes quantified indicators for AI applications related to fraud prevention and fair customer treatment, thereby enhancing AI’s contribution to the organization’s long-term value.

Training of employees on the ethical use and/or security of AI

Please refer to SinoPac Holdings supervises Bank SinoPac and SinoPac Securities in establishing AI governance and talent development mechanisms in accordance with the “Guidelines for the Management of Emerging Technology Applications” and the “Detailed Rules for the Application of Artificial Intelligence in Emerging Technologies.” The Emerging

Technology Application Management Committee is responsible for coordinating AI-related training programs, covering topics such as information security, personal data protection, AI ethics, and model risk management. For units implementing AI applications, relevant professional expertise is required during project review and risk self-assessment processes. Employees' awareness of risks associated with generative AI (such as data leakage and prompt injection) and fairness-related issues is enhanced through targeted training.

In addition, in accordance with AI governance requirements, such training has been incorporated into internal control frameworks and institutionalized management processes. Awareness initiatives are conducted based on practical cases and application scenarios (including generative AI and predictive AI) to ensure that employees comply with regulatory and information security requirements throughout the entire AI lifecycle. Through continuous education and capability enhancement, the organization is progressively building a culture of responsible AI, improving employees' ability to use AI appropriately, reducing the risk of misuse, and strengthening sustainable governance and organizational resilience. In 2025, four information security training sessions were conducted, covering employees across the group and key AI-related units. The courses integrated AI security risks and compliance topics, strengthening fundamental awareness while focusing on application risks, evaluation processes, and secure development. More than 600 participants attended, enhancing cross-department communication and information security governance capabilities.