波司登
BOSIDENG

Bosideng International Holdings Limited
波司登國際控股有限公司
(incorporated in the Cayman Islands with limited liability)
(Stock code: 3998)

INFORMATION SECURITY POLICY

1. APPLICABLE SCOPE

1.1 This Information Security Management Policy (the "Policy") is applicable to Bosideng International Holdings Limited (the "Company") and its subsidiaries (collectively, the "Group"). This policy extends to all suppliers, contractors and third-party partners who have access to the Group's information systems or data under equivalent security agreements.

2. SUMMARY

2.1 The Group commits to complying with applicable national laws and regulations, including the Cybersecurity Law of the People's Republic of China, Data Security Law of the People's Republic of China, Personal Information Protection Law of the People's Republic of China, Cryptography Law of the People's Republic of China, as well as relevant industry standards (including but not limited to cybersecurity tiered protection and critical information infrastructure security requirements). Additionally, we adhere to other applicable laws and regulations in the countries/regions where our operations are conducted, such as the EU "General Data Protection Regulation" (GDPR) and relevant U.S. state privacy legislation, where applicable.

2.2 The Group has established an information security management system (ISMS) that covers all business processes, in compliance with GB/T 22080-2016 standard and ISO/IEC 27001 international requirements. It has implemented a privacy protection framework applicable across all operational domains (including supplier management), enforced a zero-tolerance compliance mechanism with a four-tier disciplinary hierarchy, and undergone annual internal audits as well as third-party audits to verify compliance.

2.3 The Group is committed to establishing a clear organizational structure for information security, defining job responsibilities and control processes to effectively initiate and coordinate information security activities across the entire organization. Through continuous system operation and dynamic improvements, we aim to build and implement a systematic, dynamic, institutionalized, and company-wide information security management approach that prioritizes prevention. This ensures the confidentiality, integrity, and availability of information for both the company and all stakeholders.

3. INFORMATION SECURITY MANAGEMENT

3.1 Information security management policy

3.1.1 To improve information security awareness: The key element of information security management lies in people, and the primary task of group information security is to

improve the information security awareness of all staff. Through training, publicity, education and clear responsibilities, the work of information security will be implemented to everyone;

3.1.2 Implement information security control: The method of information security management lies in control. The group's information security work is to implement various security control measures, clarify the division of labor, implement technical control measures, and achieve processes, norms, tools, inspection and improvement;

3.1.3 Reduce information security risks: The goal of information security is to reduce risks. The guiding ideology of group information security is to control the loss of information security incidents to an acceptable degree and establish information security control capabilities corresponding to the development of group business informatization;

3.1.4 Ensure business continuity and stability: The core of information security is business. The group's information security takes technical support measures around the requirements of business to ensure the continuous and stable operation of business in emergency situations.

3.1.5 Protect the rights of data subjects: establish a privacy impact assessment (PIA) mechanism to ensure that data collection and processing comply with the Data Minimization Principle, and grant users the right to access/deletion of personal data (response time ≤72 hours).

3.2 Information security goals

3.2.1 Protect the confidentiality, integrity and availability of information assets: prevent unauthorized disclosure (internal or external), tampering and loss of sensitive information (including customer data, trade secrets, employee information); ensure that authorized users can access the required information in a timely and reliable manner.

3.2.2 Improve threat resistance and event response capabilities: Build a strong defense system to resist external attacks and intrusions; establish efficient event detection, response and recovery mechanisms to minimize the impact and loss of security incidents.

3.2.3 Ensure business compliance and privacy protection: strictly comply with all applicable information security and privacy laws, regulations and contractual commitments; establish effective controls to prevent operations that violate laws, regulations and regulatory requirements.

3.2.4 Control privilege and user behavior risk: implement strict permission management and the principle of least privilege; establish effective monitoring and audit

mechanism to timely detect and deal with privilege abuse and other high-risk user behaviors.

3.3 Information security organizations

3.3.1 Organization structure: the information security organization structure of the group is composed of decision-making layer, management layer and executive layer.

3.3.2 Division of responsibilities

Decision level:

- To review and approve the company's information security policy, strategic plan and major policies;
- Supervise the handling process of major information security incidents, review disposal reports and improvement measures;
- Approval for the key resource input (budget, manpower, etc.) for the construction and maintenance of the information security management system.

Management layer ：

- To implement the resolutions of the decision-making level and coordinate the information security management of the whole group;
- Organize the establishment, implementation, operation, monitoring, review and continuous improvement of information security management system (ISMS);
- Lead information security risk assessment, implementation of control measures, event response coordination and audit;
- Report information security performance, risk situation and system operation to decision makers on a regular basis;
- Oversee the implementation of the group's privacy protection policy, review privacy impact assessment (PIA) reports, and implement disciplinary decisions.

Implementation layer:

- Information security interface person of each department: monitor the flow of privacy data in the department, and cooperate with the management layer to complete the construction and daily operation of information security system.
- Information Security & IT Team: Responsible for executing information security-related tasks within the department, including but not limited to serving as the Group's privacy protection responsibility unit. Key responsibilities encompass coordinating privacy policy implementation, completing internal and external annual privacy audits; conducting emergency response and forensic investigations for security incidents; establishing and verifying baseline configurations for security technology system standards; and providing professional security technical support and customized solutions to various departments.
- Supervision department: information security and compliance risk supervision, etc.
- Other departments perform their respective duties and work together to ensure the efficient operation of the information security system.

3.3.3 The company establishes cooperative relations with external units such as law enforcement departments, management departments, information service providers and related suppliers and conducts effective communication to ensure that it can take action and obtain help quickly in case of security incidents or privacy leakage incidents. The company shall implement effective security management for the third parties (including suppliers, partners, service providers, etc.) who have access to the company's sensitive information or information system, clarify their security responsibilities and obligations, and bind them through contracts or agreements.

4. INFORMATION SECURITY SYSTEM

4.1 Management system construction: Drawing on the framework of GB/T 22080-2016 and ISO/IEC 27001 Information Security Management System standards, our group has established a comprehensive information security management system covering all business processes. By refining document control procedures and record-keeping protocols, we ensure standardized and traceable management workflows. We conduct annual tiered security training for all employees, progressing from basic awareness education to technical skill enhancement and position-specific certification programs, thereby comprehensively improving personnel security literacy. Meanwhile, we allocate sufficient resources in human, material, and financial aspects to guarantee the efficient and stable operation of the information security management system, forming the core framework of our security architecture.

4.2 Risk assessment and disposal: The Group strictly adheres to the following standards: GB/T 20984-2022 "Information Security Technology-Information Security Risk Assessment Methodology", ISO 31000:2018 "Risk Management Guidelines", and ISO/IEC 29134:2023 "Guidelines for privacy impact assessment". We also rigorously align with the "Cybersecurity Level Protection System" (Level Protection 2.0) requirements, prioritizing risk assessment as the cornerstone of security system development through establishing a routine evaluation mechanism. The assessment covers three key dimensions: management process vulnerabilities, technical architecture flaws, and privacy compliance gaps, with particular focus on core business scenarios and high-sensitivity data processing activities (including customer privacy collection and cross-border data transmission). Upon completion, we develop customized response plans specifying mitigation strategies, responsible departments, and timelines based on risk levels. Continuous monitoring ensures risks remain within acceptable thresholds, thereby laying a solid foundation for building an effective information security framework.

4.3 Performance evaluation and optimization: The Group has established a quantitative evaluation system covering critical metrics including incident response timeliness, processing efficiency for user data rights requests (within 72 hours), and completion rate of privacy impact assessments. Through regular management review meetings combined with a dual verification mechanism of "internal audit + third-party independent audit", we conduct in-depth data analysis to evaluate system performance and accurately identify weak points. Based on review conclusions, we dynamically adjust security policies and control measures. Meanwhile, in response to new business development needs and emerging technological trends, we drive synchronized iteration and upgrade of the security system to align with corporate operational requirements. This ensures the information security framework remains effective and advanced through continuous optimization, adapting to evolving internal and external environments.

5. CONTACT INFORMATION

5.1 For information security & privacy protection policy related matters, please contact the Information Security Department of the Group at email: IS@bosideng.com.

6. FOLLOWING-UP WITH CONCERNS AND INFORMATION DISCLOSURE

7.1 The Group will continue to improve, update and enhance its information security policies and implemented measures based on real situation to ensure the rights and interests of all stakeholders.

7. CIRCULATION AND REVISION

8.1 The Group reserves the right to revise, alter or abolish this Policy from time to time. The Group will regularly review this Policy and make revisions when necessary. The latest version of this Policy is available on the Company's official website at http://company.bosideng.com.