天工国际有限公司

信息安全管理声明

Tiangong International Company Limited

Statement on Information Security Management

第一章 总则

Chapter One. General Provisions

第一条 我们高度重视信息安全及隐私保护管理工作，严格遵循《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规要求，以高标准体系管理信息安全风险，确保天工国际有限公司（以下简称“公司”）信息安全管理体系稳定运行。

Article 1 We attach great importance to information security and privacy protection management, and strictly comply with the requirements of laws and regulations such as the *Data Security Law of the People's Republic of China* and the *Personal Information Protection Law of the People's Republic of China*. We manage information security risks with a high-standard system to ensure the stable operation of the information security management system of Tiangong International Company Limited (hereinafter referred to as "the Company").

第二章 适用范围

Chapter Two. Scope of Application

第二条 本制度适用于天工国际有限公司及其合并报表范围内的所有实体（以下统称“本集团”）。同时，本集团积极倡导供应商、经销商、承包商等合作伙伴共同遵守本规范。

Article 2 This policy applies to Tiangong International Company Limited and all entities within its consolidated financial statements (hereinafter collectively

referred to as "the Group"). Meanwhile, the Group actively advocates for suppliers, distributors, contractors, and other partners to jointly comply with this policy.

第三章 政策及原则
Chapter Three. Policies and Principles

第三条 本集团持续完善信息安全管理架构，识别各类信息安全风险，不断健全信息安全管理体系。

Article 3 The Group continuously improves its information security management structure, identifies various types of information security risks, and keeps improving its information security management system.

第四条 本集团致力于以合法合规且正当的方式收集数据。通过规范数据采集流程和方法，运用受控网络及传输介质，实施分级存储与加密存储措施，并明确数据使用权限，有效降低数据管理各环节的泄露风险。

Article 4 The Group is committed to collecting data in a legal, compliant and legitimate manner. By standardizing data collection processes and methods, using controlled networks and transmission media, implementing hierarchical storage and encrypted storage measures, and clarifying data usage rights, the Group effectively reduces the risk of leakage in all aspects of data management.

第五条 本集团严格控制信息接触和知悉范围，确保仅有授权人员才可访问敏感信息，满足权限最小化策略。

Article 5 The Group strictly controls the scope of information access and awareness, ensuring that only authorized personnel can access sensitive information, in line with the principle of least privilege.

第六条 本集团依据数据安全防护级别，实施相应的监测预警和保密措施，实时监测数据泄露、毁损、丢失、篡改等异常情况。

Article 6 The Group implements corresponding monitoring, early warning and confidentiality measures according to the data security protection level, and monitors abnormal situations such as data leakage, damage, loss and tampering in real time.

第七条 本集团建立完善的信息安全事件应急响应机制，涵盖职责分工、发现与报告、应急保护、追踪与处置等环节，一旦发生安全事件，将迅速启动应急预案。

Article 7 The Group has established a sound emergency response mechanism for information security incidents, covering division of responsibilities, detection and reporting, emergency protection, tracking and disposal. In the event of a security incident, the emergency plan will be activated promptly.

第八条 本集团全体员工使用网络时应当遵守法律法规及公司规章制度，在采集和管理信息数据时不得窃取个人信息，禁止私自下载和转移重要的个人信息和企业数据至个人移动数据传输设备。

Article 8 All employees of the Group shall abide by laws, regulations and company rules and regulations when using the network. They shall not steal personal information when collecting and managing information and data, and shall not download or transfer important personal information and enterprise data to personal mobile data transmission devices without permission.

第九条 本集团通过将信息安全培训纳入员工培训体系，制定并推进培训计划，强化全员信息安全意识。

Article 9 The Group strengthens the information security awareness of all employees by incorporating information security training into the employee training system, formulating and promoting training plans.

第十条 所有可接触本集团敏感数据的第三方供应商，包括云服务商、外包服务商、合作开发机构等，合作前必须完成严格的信息安全资质评估，未通过评估不得开展合作，合作协议中必须明确信息安全责任条款。同时，本集团要求第三方严格遵守本集团信息安全标准、落实对应数据保护措施，并定期对核心供应商开展信息安全审核，不符合要求的要求供应商限期整改，整改仍不达标则终止合作。

Article 10 All third-party suppliers that could access the Group's sensitive data, including cloud service providers, outsourcing service providers, cooperative development institutions, etc., must complete a strict information security qualification assessment before cooperation. Cooperation shall not be carried out without passing the assessment, and information security responsibility clauses must be clearly specified in the cooperation agreement. At the same time, the

Group requires third parties to strictly abide by the Group's information security standards, implement corresponding data protection measures, and conduct regular information security audits on core suppliers. Suppliers that fail to meet the requirements shall be ordered to rectify within a time limit, and the cooperation shall be terminated if they still fail to meet the standards after rectification.

第四章 附则

Chapter Four. Supplementary Provisions

第十一条 本声明由数据中心负责解释、修订。

Article 11 This Statement shall be interpreted and revised by the Company's Data Center.

第十二条 本声明自发布之日起生效。

Article 12 The Statement shall come into effect from the date of its release.