資訊安全政策

Information Security Policy

第一條 目的

Article 1 Purpose

佳世達科技股份有限公司(以下簡稱本公司) 因本公司業務之推展，提供內部員工（使用者）及外部客戶（客戶、供應商、顧問及合作夥伴等）重要產品及服務之資訊，為就相關資訊建立系統安全管理標準、策略、系統架構和資訊持續運作環境確保資訊資產(與資訊處理相關之硬體、軟體、資料、文件及人員等)之機密性、完整性、可用性及適法性，並避免遭受內、外部蓄意或意外之威脅，並衡酌本公司之業務需求，故訂定資訊安全政策（以下簡稱本政策），作為資訊安全工作之指導方針。

Due to the development of its business, Qisda Technology Co., Ltd. (hereinafter referred to as "the Company") provides important information about products and services to internal employees (users) and external clients (customers, suppliers, consultants, and partners). To establish system security management standards, strategies, system architecture, and an information continuity operating environment for relevant information, the Company aims to ensure the confidentiality, integrity, availability, and legality of information assets (including hardware, software, data, documents, and personnel related to information processing) while avoiding intentional or accidental threats from internal and external sources. Considering the Company's business needs, this Information Security Policy (hereinafter referred to as "this Policy") is established as a guiding principle for information security work.

第二條 適用範圍

Article 2 Scope of Application

本公司員工、臨時雇員、訪客與本公司有業務往來之廠商(含員工、臨時雇員等)於維護、保管、使用、管理本公司資訊資產時，皆應遵守本政策。

All employees, temporary workers, visitors, and vendors (including employees and temporary workers) who have business dealings with the Company shall comply with this Policy when maintaining, safeguarding, using, and managing the Company's information assets.

第三條 說明

Article 3 Explanation

一、 資訊安全目標

Information Security Objectives

本公司之資訊安全目標如下：

The information security objectives of the Company are as follows:

(一) 確保本公司資訊資產之機密性，落實資料存取控制，資訊需經授權人員方可存取。

Ensure the confidentiality of the Company's information assets by implementing access control, allowing information access only to authorized personnel.

(二) 確保本公司資訊作業管理之完整性，避免未經授權之修改或作業錯誤。

Ensure the integrity of the Company's information operations management, avoiding unauthorized modifications or operational errors.

(三) 確保本公司資訊作業持續運作，符合營運服務水準。

Ensure the continuous operation of the Company's information operations in line with operational service levels.

(四) 確保本公司資訊作業均符合相關法令規定要求。

Ensure that the Company's information operations comply with relevant legal requirements.

二、 資訊安全控制措施

Information Security Control Measures

本公司之資訊安全控制措施如下：

The information security control measures of the Company are as follows:

(一) 成立資訊安全管理委員會，督導資訊安全管理制度之運作，鑑別資訊安全管理制度之內、外部議題及利害相關團體對本公司之資訊安全要求與期望。

Establish an Information Security Management Committee to supervise the operation of the information security management system and identify internal and external issues related to the information security management system, as well as the requirements and expectations of stakeholders regarding the Company's information security.

(二) 管理階層應承諾維護資訊安全，持續改善資訊安全系統，從軟體、硬體、資料到人員、全面提升資訊安全品質，減少資訊安全事故之發生，以保障客戶之權益。

Management shall commit to maintaining information security, continuously improving the information security system, and comprehensively enhancing information security quality from software, hardware, data to personnel, in order to reduce the occurrence of information security incidents and protect customers' rights and interests.

(三) 資訊安全管理制度文件應適時更新，紀錄之保護應有明確管理機制。

Information security management system documents should be updated in a timely manner, and the protection of records should have a clear management mechanism.

(四) 定期進行資訊資產分類與風險評鑑。

Regularly conduct classification and risk assessment of information assets.

(五) 本公司全體人員皆有責任及義務保護其擁有、保管或使用之資訊資產。依職務分工設定差異化資安責任，包括但不限於：IT 部門負責系統維護防護，財務部門管控敏感資料存取，一般員工至少需識別可疑活動並通報。

All personnel of the company have the responsibility and obligation to protect the information assets they own, custody, or use. Differentiated information security responsibilities are assigned based on job functions, including but not limited to: IT departments are responsible for system maintenance and protection, finance departments control access to sensitive data, and general employees are required at minimum to identify suspicious activities and report them.

(六) 工作分派應考量職能分工，職務責任範圍應予區分，以避免資訊或服務遭未經授權修改或誤用。

Job assignments should consider functional divisions, and the scope of job responsibilities should be differentiated to avoid unauthorized modifications or misuse of information or services.

(七) 對於與本公司有業務往來之廠商及其員工、臨時雇員有使用或存取本公司資訊資產之需求時，應進行必要之審核及建立資訊安全要求，並遵循本公司相關規範。該等人員並負有保護其所擁有、保管或使用本公司資訊資產之責任。建立第三方資訊安全要求制度，依供應商接觸資料機密程度與業務影響風險進行分級管理。高風險供應商需評估營運持續、系統開發等資安面向，中風險需包含資料防護、網路安全等，低風險級需評估基礎安全要求。

When vendors and their employees or temporary employees who have business dealings with the company require access to or use of the company's information assets, necessary audits should be conducted, and information security requirements should be established in accordance with the company's relevant regulations. Such personnel are responsible for protecting the information assets of the company that they possess, safeguard, or use. A third-party information security requirement system should be established, with graded management based on the level of confidentiality of the data accessed by suppliers and the risk of business impact. High-risk suppliers must assess information security aspects such as business continuity and system development, medium-risk suppliers must include data protection and network security, and low-risk suppliers

must assess basic security requirements.

(八) 依業務需求訂定資訊作業持續運作計畫，並定期測試演練。

Establish information operation continuity plans based on business needs and conduct regular testing and drills.

(九) 定期檢測資訊安全指標，以維持資訊安全管理制度及管控程序實施之有效性。

Regularly test information security indicators to maintain the effectiveness of the implementation of information security management systems and control procedures.

(十) 確保工作區域場所之安全，以防範資訊資產遭竊取或毀損。

Ensure the security of work areas to prevent theft or damage of information assets.

(十一)落實通訊安全管理。

Implement communication security management.

(十二)資訊作業或程序之開發、修改及建置，皆須符合並遵循資訊安全目標之規定。

The development, modification, and construction of information operations or procedures must comply with and follow the provisions of information security objectives.

(十三)本公司全體人員應隨時注意是否有發生資訊安全事件、安全弱點及違反安全政策與規範之虞等情事，並依程序進行通報。公司須持續監控網路安全威脅，及時應變資安事件，並實施風險減輕策略。建立通報機制，於應變各階段都能及時告知內外部利害關係人，說明應變措施與預防改善計畫。

All personnel of the company should remain vigilant at all times for information security incidents, security vulnerabilities, and potential violations of security policies and regulations, and report them according to established procedures. The company must continuously monitor cybersecurity threats, respond promptly to security incidents, and implement risk mitigation strategies. Establish notification mechanisms to timely inform internal and external stakeholders at all stages of incident response, explaining response measures and preventive improvement plans.

(十四)遵循內、外部相關法令規定，並定期更新法令法規清單，建立應有之管控程序，定期執行資訊安全查核作業。

Comply with relevant internal and external legal regulations, regularly update the list of legal regulations, establish necessary control procedures, and conduct regular information security audits.

(十五)應採用行動裝置安全措施，以管理使用行動裝置所導致之風險。

Implement mobile device security measures to manage risks associated with the use of mobile devices.

(十六)應於資訊作業專案管理中納入資訊安全相關議題。

Incorporate information security-related issues into information operation project management.

(十七)應全面安裝防毒軟體避免公司電腦設備遭受惡意軟體侵害。

Ensure comprehensive installation of antivirus software to prevent company computer equipment from being compromised by malware.

(十八)應定期舉辦資訊安全相關教育訓練並透過測驗方式加強員工資訊安全意識。

Regularly conduct information security-related training and strengthen employees' information security awareness through testing.

(十九)確保與相關利害關係者之間的有效溝通，以促進資訊共享、增進信任，並確保資訊安全管理的透明度。

Ensure effective communication with relevant stakeholders to promote information sharing, enhance trust, and ensure transparency in information security management.

(二十)提升全體員工對資訊安全的認識和責任感，建立強健的資安文化，以減少資訊安全事件的發生，保障公司資訊資產的安全。

Enhance the awareness and sense of responsibility of all employees regarding information security, establishing a robust security culture to reduce the occurrence of information security incidents and protect the Company's information assets.

(二十一) 確保本公司資訊資產之完整性，持續提升保護能力，從資料建立、儲存、傳輸、使用到銷毀，實施加密、存取控制、備份和稽核等防護措施，確保資料保持準確、一致，並防範未經授權的存取、篡改或破壞。

Ensure the integrity of our company's information assets, continuously enhance protection capabilities, and implement protective measures such as encryption, access control, backup, and auditing throughout the data lifecycle from creation, storage, transmission, and usage to destruction, ensuring data remains accurate and consistent while preventing unauthorized access, tampering, or destruction.

三、 年度檢討

Annual Review

本政策每年至少檢討一次，以符合相關法令規定及資訊業務最新發展現況，並於必要時修正之。

This Policy shall be reviewed at least once a year to comply with relevant legal regulations and the latest developments in information business, and shall be amended as necessary.

第四條 罰則

Article 4 Penalties

一、 本公司員工違反本政策者，其主管應要求限期改善，如限期未見改善或案件情節重大者，由當事人所屬單位部門主管、人力資源部及其他相關單位研議獎懲內容後，依本公司獎懲辦法之規定，報請權責主管核定後予以議處。

If an employee of the Company violates this Policy, their supervisor shall require them to make improvements within a specified period. If no improvements are seen within the specified period or if the case is serious, the supervisor of the department to which the person belongs, along with the Human Resources Department and other relevant units, shall discuss the disciplinary content and, in accordance with the Company's reward and punishment regulations, submit it for approval by the responsible supervisor for action.

二、 與本公司有業務往來之廠商違反本規定者，應依雙方訂定之合約或約定辦理。

If a vendor with business dealings with the Company violates these regulations, it shall be handled according to the contract or agreement established by both parties.