

Information Security Policy Statement

CTCI is committed to become a leading global provider of engineering and technology services. We have established an Information Security Management System (ISMS) in accordance with ISO 27001 Information Security Management Standards, in order to fulfill the following requirements of information security:

- **Ensure information security**

Consolidate the ISMS to protect the company's information assets from internal or external threats of being stolen or disclosed, either maliciously or inadvertently, while ensuring monitoring and responding to information security threats. This includes maintaining transparency with affected stakeholders when breaches or threats occur, outlining actions taken to address vulnerabilities and prevent future risks.

- **Raise information security awareness among staff**

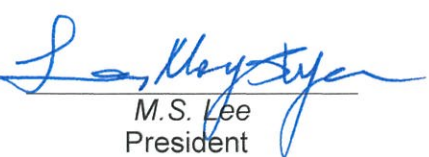
Conduct information security education and training program, keep staff educated to prevent information disclosure that may impact business operations, including establishing individual responsibilities for information security for the entire workforce. All employees shall comply with the company's Information Security Policy Statement and related declarations, follow the Information Security Management Regulations, remain alert to any suspicious activities at all times, understand the Information Security Incident Reporting and Managements Flow Chart, and are responsible for reporting such incidents.

- **Persistent improvement of ISMS**

Persistent supervision, measurement, evaluation, and analysis of information management activities, integrity and protection of data (This involves maintaining security controls that protect data throughout its lifecycle, including measures to prevent breaches and ensure that only authorized users can modify or access sensitive information), along with continuous improving in information security systems, will ensure the robustness and reliability of the ISMS, thereby improving the effectiveness of the system.

- **Compliance with regulatory and contractual requirement**

Operating information of all contracted engineering projects, including planning, design, procurement, construction, etc., is secure and compliant with government regulations, company policies and standards, and contractual requirements (establishing information security requirements for third parties, e.g., suppliers). In addition to complying with our company's information security policy and related regulations, the software used by third parties when fulfilling the contract must not violate copyright laws. If illegal software use causes information security risk or act of infringement, the third parties involved shall assume all liabilities. This approach aims to mitigate risks associated with external relationships and safeguard shared infrastructures and data.

 T.C. Li EMO President	 J.S. Chung HBO President	 Anthony Hsu IEPBO President	 William Pung ATFBO President	 Yu-Hung Su EPCO President
 M.S. Lee President (CISO interim)				

Issue Date: 2026/06/05

資訊安全政策 Information Security Policy

1.0 目的 Purpose

依據「ISO/CNS27001 資訊安全、網宇安全及隱私保護-資訊安全管理系統-要求事項」及相關法令、法規與標準，訂定資訊安全手冊，以提升中鼎同仁的資訊安全意識，強化公司資訊安全防護及應變能力，確保業務持續運作。

In accordance with ISO/CNS27001 requirements (Information security, cybersecurity and privacy protection – Information security management systems – Requirements) and relevant laws, regulations and standards, we draw up the Information Security Manual to help raise information security awareness among CTCI staff, consolidate the company's information security protection and improve the adaptability to change, thus ensuring business continuity.

2.0 適用範圍 Scope

2.1 本公司所有同仁、委外服務廠商及訪客。

This manual applies to all staff members of the company, third-party vendors and guests.

2.2 資訊安全管理之範疇涵括組織、人員、實體及技術四大控管領域，可透過以下控制主題進行安全控管實作，以避免因人為疏失、蓄意或天然災害等因素，降低風險對本公司造成各種可能之危害，各控管主題分述如下：

The information security norm considers 4 control domains, in which potential risk or possible damage to the company may occur in case of human errors, malicious attacks or natural disasters. Those domains are described as follows :

2.2.1 資訊安全政策 Information Security Policies

2.2.2 資訊安全之組織 Organization of Information Security

2.2.3 人力資源安全 Human Resource Security

2.2.4 資產管理 Asset Management

2.2.5 存取控制 Access Control

2.2.6 密碼學 Cryptography

2.2.7 實體及環境安全 Physical and Environmental Security

2.2.8 運作安全 Operations Security

2.2.9 通訊安全 Communications Security

2.2.10 資訊系統獲取、開發及維護 System Acquisition, Development and Maintenance

2.2.11 供應者關係 Supplier Relationships

2.2.12 資訊安全事故管理 Information Security Incident Management

Issue Date: 2026/06/05

2.2.13 營運持續管理之資訊安全層面 Information Security Aspects of Business
Continuity Management

2.2.14 遵循性 Compliance

3.0 作業內容 Activity

3.1 資訊安全政策之研訂與審查 Draw up and review of information security policies

資訊安全政策由「資訊安全推動委員會」進行研訂與審查，以反映本公司資訊安全管理政策、相關法令規範、環境及公司業務之最新狀況，以確保資訊安全實務運作之可行性及有效性。

Information Security Promotion Committee will draw up information security policies and conduct regular review, in order to reflect the company's information security policies, regulatory requirements, environment and current status of business operation, and to ensure the feasibility and effectiveness of practical operation of information security.

3.2 資訊安全之組織 Organization of Information Security

為有效推動與辦理資訊安全各項工作，成立「資訊安全推動委員會」，以擬訂本公司資訊安全之目標、策略及管理程序，促進資訊安全管理制度執行之有效性，期使本公司資訊安全管理制度達成既定之目標。

Information Security Promotion Committee is established to promote and implement information security. The committee develops objectives, strategies and management procedures of information security ensure the implementation effectiveness of ISMS, in order to achieve the established goal of ISMS.

3.3 人力資源安全 Human Resource Security

為規範人力資源之安全管理，並落實資訊安全教育訓練，以提升人員資訊安全認知及警覺意識。訂定人員之安全管控措施，辦理相關安全管理辦法及教育訓練，減少因資訊安全認知不足所引發之資訊安全事件。

Regulate the security management of human resource and implement information security education and training to improve security knowledge and raise awareness. Establish staff security control procedures, conduct relevant security management education and training program, to reduce information security incident resulting from lack of security knowledge.

3.4 資訊資產管理 Information Asset Management

訂定資訊資產分類與分級，據以辦理各項資產風險評鑑、管理及作業方法，保護資訊資產，降低因人為疏失、蓄意或自然災害等風險所造成傷害。

Information assets are categorized and classified, which serve as the basis of risk assessment, management responsibilities and working instructions. Information assets shall be protected to minimize the impact of potential risks of human errors, malicious attacks or natural disaster.

3.5 存取控制 Access Control

訂定資訊資產存取控制細則，將工作需要的存取控制需求，明確告知系統服務提供者，以利執行有效之存取控制機制，保護資訊資產，降低未經授權存取系統之風險，配合稽核制度的建立，達成安全控管。

Establish granular controls of information assets. Specify access controls for work requirements to system service providers, in order to implement effective access control mechanism, protect information assets and reduce the risk of unauthorized system access. With granular controls and the establishment of audit systems, access control will be achieved.

3.6 密碼學 Cryptography

確保本公司有效並適當使用密碼學技術，避免技術誤用。

Ensure that the cryptography is properly and effectively used, in order to prevent misuse.

3.7 實體及環境安全 Physical and environmental security

為保護資訊資產及實體環境安全，以降低威脅所引發之風險。訂定實體與環境之安全管控措施，減少因安全問題所引發的危險，達到保護資訊資產、落實安全控管之目的。

Protect information assets and physical environment to reduce the risk of threats. Establish physical and environmental security controls to reduce security risks and protect information assets.

3.8 運作安全 Operations Security

確保本公司資訊處理設施之正確及安全操作，防範惡意軟體之攻擊與資料漏失、紀錄事件並產生證據、確保運作中系統之完整性、防範對技術脆弱性之利用，及將稽核活動中對運作系統之衝擊降至最低。

Ensure the proper and safe operation of the company's information processing equipment. Guard against malicious attack and data loss. Log events and generate evidence. Ensure the integrity of running systems. Prevent exploits of system vulnerabilities, and minimize the impact of audit activities on running systems.

3.9 通訊安全 Communication Security

為防止本公司資訊系統遭致非預期及非經授權之修改或破壞，以確保資訊系統與資料之機密性、可用性及完整性。

Protect the company's information systems from unexpected and unauthorized modification or sabotage, to preserve the confidentiality, availability and integrity of information systems and data.

3.10 資訊系統獲取、開發及維護 System Acquisition, Development and Maintenance

訂定資訊系統必須考慮之資訊安全面向，於資訊系統建立之規劃及需求分析階

段，即納入資訊安全考量，明訂資訊安全需求，保護資訊資產，降低資訊系統誤用之風險。

When developing information system, consider the information security aspects early in the planning and demand analysis stage of system development. Make information security demand clear, protect information assets, and reduce the risks of misusing information system.

3.11 供應者關係 Supplier Relationships

確保本公司可被委外廠商存取之資產已獲得保護，公司與廠商間維持資訊安全與服務交付之議定等級與合約要求一致。

Ensure that assets accessible to outsourcing vendors are well protected, and information security between company and vendors and the negotiated rate of service delivery is compliant with contract provisions.

3.12 資訊安全事故管理 Information Security Incident Management

資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

In case of information security incident, quickly report the incident to the authority, take necessary actions to address problems, establish the mechanism to learn from information security incident to minimize the incident impact.

3.13 營運持續管理之資訊安全層面 The information security aspect of business continuity management

為確保公司重要營運業務不受重大災難或安全缺失的影響，建置和實施備援計畫，當關鍵營運業務之資訊設備系統中斷或故障時，在可接受的時間內恢復營運，確保公司重要營運業務能及時恢復運作。

Ensure that the company's critical business operation stay unaffected in case of serious disaster or security flaw. Establish and implement recovery plan. When disruption or failure occur on information system supporting critical business operation, recover to normal operation in acceptable period of time, make sure the important business operation resume in a timely manner.

3.14 遵循性 Compliance

避免違反政府法律、行政命令、法規或合約內容對資訊安全的規範。資訊系統的設計、操作、使用和管理應符合法規要求，確保能遵循具管轄權國家之法律要求。

Avoid the breach of government laws, administrative order, regulations or contracts agreement for information security. Design, operation, use and management of ISMS should be compliant with regulatory requirements as well as laws under national jurisdiction.