大 江 生 醫 股 份 有 限 公 司

TCI Co., Ltd.

文件名稱： Title:	資訊安全政策 Information Security Policy
制訂單位： Formulated by:	戰略數據中心 Strategic Data Center
編　　號： Document No.:	TCI-M-IT-001
版　　本： Version:	01
總 頁 數： Total Pages:	03
制訂日期： Formulated on:	2025 年 1 月 1 日 January1, 2025
首發日期： First Issued on:	2022 年 10 月 28 日 October 28, 2022

制 訂 / 修 訂 記 錄
Formulation / Revision Records

版本 Version	制訂/修訂日期 Formulation / Revision Date	修 訂 內 容 摘 要 Description of Changes
00	2022 年 10 月 28 日 October 28, 2022	因應 ISO27001 資安管理制度，首次發行 Issued for the first time in response to the ISO27001 information security management system.
01	2025 年 1 月 1 日 January1, 2025	因應 ISO27001 2022 改版修正資安管理制度

大江生醫關係企業集團
TCI GROUP

大江生醫股份有限公司
TCI Co., Ltd.

文件名稱 Title	資訊安全政策 Information Security Policy			文件編號 Document No.	TCI-M-IT-001		
制訂單位 Formulated by	戰略數據中心 Strategic Data Center	生效日期 Effective Date	2025.1.1	文件版本 Version	01	頁次 Page	1

1. 目的
Purpose

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之業務持續運作環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

To strengthen information security management, ensure the confidentiality, integrity, and availability of the company's information assets, provide a continuous operational environment for the company, comply with relevant regulations, and protect against intentional or accidental internal and external threats, this policy is established.

2. 範圍
Scope

2.1. 適用於本公司資訊資產、系統及服務之安全管理作業，涵蓋機密性、完整性和可用性。
This policy applies to the security management operations of the company's information assets, systems, and services, covering confidentiality, integrity, and availability.
2.2. 適用於本公司全體員工、提供資訊服務廠商及第三方人員。
It applies to all company employees, information service providers, and third-party personnel.
2.3. 本公司會維持資訊安全管理系統有效性並秉持持續改善的精神加以維護管理
The company will maintain the effectiveness of the information security management system and uphold the spirit of continuous improvement in its management.

3. 定義
Definition

所謂資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

Information security refers to the application of management procedures and

security protection technologies to various information operations, including software and hardware equipment used during operations and media storing various information and data, to ensure the security of information collection, processing, transmission, storage, and circulation.

4. 本公司資訊安全政策

Company Information Security Policy

「資訊安全是大江生醫對客戶必要的保障與承諾」

「Information security is TCI’s necessary guarantee and commitment to customers」

強化本公司的資訊安全管理，建立「資訊安全是大江生對客戶必要的保障與承諾」之觀念，確保客戶及同仁資料處理之機密性、完整性及可用性，務使本公司資料之處理全程均獲安全保障，提供安全穩定及高效率之資訊服務。

Strengthen the company’s information security management, establish the concept that "information security is TCI’s necessary guarantee and commitment to customers," ensure the confidentiality, integrity, and availability of customer and employee data processing, and guarantee security throughout the entire data processing process, providing safe, stable, and efficient information services.

5. 主題特定政策

Specific Policies

5.1. 存取控制：

Access Control

5.1.1. 限制對資訊及資訊處理設施之存取。

Restrict access to information and information processing facilities.

5.1.2. 確保授權使用者得以存取，並避免系統及服務的未授權存取。

Ensure authorized users can access, and prevent unauthorized access to systems and services.

5.1.3. 令使用者對保全其鑑別資訊負責。

Require users to be responsible for safeguarding their authentication information.

5.1.4. 防止系統及應用遭未經授權存取。

Prevent unauthorized access to systems and applications.

5.2. 實體及環境安全：

Physical and Environmental Security

5.2.1. 防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。

Prevent unauthorized physical access, damage, and interference to organizational information and information processing facilities.

5.2.2. 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。

Prevent loss, damage, theft, or compromise of assets, and prevent disruption of organizational operations.

5.3. 資產管理：

Asset Management

5.3.1. 識別組織之資產並定義適切之保護責任。

Identify organizational assets and define appropriate protection responsibilities.

5.3.2. 確保所有資產依其對組織之重要性，受到適切等級的保護。

Ensure all assets are protected according to their importance to the organization.

5.3.3. 防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。

Prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

5.4. 資料傳送

Data Transmission

5.4.1. 確保資料傳送可追溯性及不可否認性 。

Ensure traceability and non-repudiation of data transmission.

5.4.2. 維持傳送作業之可靠性及可用性。

Maintain reliability and availability of transmission operations.

5.4.3. 實體傳送使用破壞存跡或抗破壞之控制措施。

Use destruction-proof or tamper-resistant controls for physical transmission.

5.4.4. 使用規定之電子傳輸媒體傳遞資料，不可因貪圖方便而任意使用非法與不當之傳輸

媒體。

Use designated electronic transmission media for data delivery; do not use illegal or improper media for convenience.

5.4.5. 不得利用任何傳輸媒介透過資料傳遞、訊息傳送、發言或視訊等方式透露機密或敏感性資訊給其他組織或人員。

Do not disclose confidential or sensitive information to other organizations or personnel via any transmission medium.

5.4.6. 內部資訊網站須依權責及工作需求核發適當權限，以管制相關文件之存取。

Internal information websites must grant appropriate permissions based on authority and work needs to control document access.

5.5. 端點裝置之安全組態及處置

Endpoint Device Security Configuration and Handling

5.5.1. 對使用者端點裝置分發及回收 。

Distribute and recover user endpoint devices.

5.5.2. 對使用者端點裝置軟體安裝進行控制。

Control software installation on user endpoint devices.

5.5.3. 對使用者端點裝置進行安全性更新。

Update security on user endpoint devices.

5.5.4. 使用者端點裝置經登入程序使用。

Use login procedures for endpoint devices.

5.5.5. 防範惡意軟體對使用者端點裝置危害。

Prevent malware threats to endpoint devices.

5.5.6. 管制私人裝置使用。

Control use of personal devices.

5.6. 網路安全

Network Security

5.6.1. 網路使用者經授權後，只能在授權範圍內存取網路資源。

Network users may only access network resources within their authorized scope.

5.6.2. 對使用網路系統的電腦連接線路，應適當加以控制，以減少未經授權之系統存取或

電腦設施的風險。

Control computer connection lines for network systems to reduce risks of unauthorized system access or facility compromise.

5.6.3. 設定網路區隔之規劃，應遵循內外網路實體區隔規定，並應禁止個人無線網路裝置破壞內外網路實體區隔之安全機制。

Plan network segmentation according to internal and external network physical separation requirements; prohibit personal wireless devices from compromising network separation security mechanisms

5.6.4. 非經授權嚴禁使用無線網路及私有有線設備與網路介接。

Unauthorized use of wireless networks and private wired equipment/network interfaces is strictly prohibited.

5.7. 資訊安全事故管理：

Information Security Incident Management

5.7.1. 確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。

Ensure consistent and effective management of information security incidents, including communication of security events and vulnerabilities.

5.7.2. 建全資訊安全事故通報體系。

Establish a robust information security incident reporting system.

5.8. 資訊備份：

Information Backup

5.8.1. 依照資訊之可用性及完整性需求，制定個資訊備份週期、方式及保存期限，並測試其有效性。

Define backup cycles, methods, and retention periods according to information availability and integrity needs, and test their effectiveness.

5.8.2. 依照備份資料之機密性需求加以防護，避免衍生之其他資安事件。

Protect backup data according to confidentiality requirements to avoid other security incidents.

5.9. 密碼學：

Cryptography

5.9.1. 依照法規、客戶要求及資訊資產風險設置加密機制。
Set up encryption mechanisms according to regulations, customer requirements, and information asset risks.

5.9.2. 管制金鑰產生、分派啟用、儲存、更新、廢止到封存和銷毀等作業。
Manage key generation, distribution, activation, storage, updating, revocation, archiving, and destruction.

5.10. 資訊分類分級及處理。
Information Classification, Grading, and Handling

5.10.1. 資訊標示涵蓋所有格式的資訊及其他相關聯資產
Information labeling covers all formats and related assets.

5.10.2. 使人員及其他關注方認知標示要求。
Ensure personnel and stakeholders are aware of labeling requirements.

5.10.3. 提供所有人員必要之認知方法，以確保正確標示資訊並進行相對應的處理 。
Provide necessary awareness methods to ensure correct labeling and corresponding handling of information.

5.11. 技術脆弱性管理
Technical Vulnerability Management

5.11.1. 定義並建立與技術脆弱性管理相關聯之角色及責任 。
Define and establish roles and responsibilities related to technical vulnerability management.

5.11.2. 偵測其資訊資產是否存在脆弱性。
Detect vulnerabilities in information assets.

5.11.3. 軟體更新管理過程，以確保對所有獲授權軟體，安裝最新經核可之修補程式及應用程式之更新套件。
Manage software updates to ensure all authorized software has the latest approved patches and updates.

5.11.4. 使用適合所使用技術之弱點掃描工具，以識別脆弱性並查證脆弱性修補是否成功 。
Use appropriate vulnerability scanning tools to identify vulnerabilities and verify successful remediation.

5.12. 保全開發政策：
Secure Development Policy

5.12.1. 確保資訊安全係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。

Ensure information security is part of the entire lifecycle of information systems, including requirements for systems providing services via public networks.

5.12.2. 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

Incorporate security requirements during system planning and analysis when developing new systems or enhancing existing functions.

5.12.3. 在採購軟體時，視其安全需求，進行評估。

Evaluate security requirements when procuring software.

5.12.4. 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

System security requirements and controls should match the value of information assets and consider the potential harm from insufficient security measures.

5.12.5. 資訊系統應保護資料，防止洩漏或被竄改。

Information systems should protect data from leakage or tampering.

6. 適用性聲明書

Statement of Applicability

依據「ISO 27001 資訊安全管理系統-要求」要求產出「適用性聲明書」，以書面方式列舉資訊資產是否適用其標準所列之控制措施，及其不適用之原因。當組織架構、人員、設備、實體環境等變動時，資訊安全管理委員應重新定義控制措施之適用性。

Produce a Statement of Applicability according to the requirements of the ISO 27001 Information Security Management System, listing in writing whether information assets are subject to the standard's control measures and reasons for non-applicability. When organizational structure, personnel, equipment, or physical environment changes, the Information Security Management Committee should redefine the applicability of control measures.

7. 實施

Implementation

大江生醫股份有限公司
TCI Co., Ltd.

文件名稱 Title	資訊安全政策 Information Security Policy			文件編號 Document No.	TCI-M-IT-001		
制訂單位 Formulated by	戰略數據中心 Strategic Data Center	生效日期 Effective Date	2025.1.1	文件版本 Version	01	頁次 Page	8

本政策經主任委員核定後實施，修訂時亦同。

This policy is implemented upon approval by the Chief Supervisor; revisions follow the same process.