

資通安全政策

1 目的

理太科技股份有限公司（以下簡稱「本公司」）為確保所屬之資訊資產的機密性、完整性及可用性，以符合資通安全管理法及其子法等相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，特訂定本政策。

2 適用範圍

- 2.1 本政策適用範圍為本公司之全體同仁、委外服務廠商、資料使用者(含保管者)與訪客等。
- 2.2 資通安全管理範疇，包含組織、人員、實體及技術等四大項控制領域，為避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，避免對本公司造成各種資通安全危害之可能風險。

3 目標

本公司資通安全政策為「有效運用資源，確保資訊資產之機密性、完整性與可用性」。期藉本政策之實施，達成下列目標：

- 3.1 建立安全及可信賴之資訊化作業環境，確保本公司資料、系統、設備及網路之安全，以保障本公司業務永續運作。
- 3.2 保護本公司業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
- 3.3 保護本公司業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
- 3.4 建立本公司業務永續運作計畫，以確保本公司資訊業務服務之持續運作。
- 3.5 確保本公司各項業務服務之執行須符合「資通安全管理法」及其子法，以及相關法令規範之要求。
- 3.6 為保護本公司業務及服務相關資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
- 3.7 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料及隱私

保護環境。

4 責任

- 4.1 本公司應成立「資通安全管理委員會」，統籌資通安全事項之推動。
- 4.2 管理階層應支持資通安全管理制度，並提供相關資源，以確保資通安全政策落實執行。
- 4.3 本公司全體同仁、委外服務廠商、資料使用者(含保管者)與訪客等皆應遵守本政策。
- 4.4 本公司全體同仁、委外服務廠商及資料使用者(含保管者)均有責任透過適當通報機制，通報資通安全事件或弱點。
- 4.5 任何危及資通安全之行為，將視情節輕重追究其民事、刑事責任，或依本公司之相關規定進行議處。

5 管理指標

- 5.1 為評量資通安全管理目標達成情形，本公司應訂定相關管理指標，並定期監控、評估及改善。
- 5.2 應定期審查本公司資通安全組織及人員執掌，以確保資通安全工作之推展。
- 5.3 應符合主管機關之要求，依員工職務及責任提供適當之資通安全相關訓練。
- 5.4 應加強本公司資訊資產之環境安全，採取適當之保護及權限控管機制。
- 5.5 應確保資訊不被透漏給未經授權之第三者。
- 5.6 應加強存取控制，防止未經授權之不當存取，以確保本公司資訊資產已受適當之保護。
- 5.7 本公司資訊系統開發應符合安全需求，並定期執行技術檢測及進行修補。
- 5.8 應確保所有資通安全事件或可疑之安全弱點情資，均依循適當之通報機制向上反應，並予以適當調查及處理。

6 管理審查

本政策應每年至少進行 1 次管理審查，以反映政府法令、資通安全標準、技術、主管機關要求及本公司管理制度運作實際需求，確保本公司業務永續運作；另主管機關(或法令、法規要求)、客戶或專家學者等利害關係人如有資通安全相關回饋事項，應列入管理審查會議之討論議題。

7 實施

本政策經本公司「資通安全管理委員會」審查及核定後實施，修訂時亦同。