

采江互動科技股份有限公司

資訊安全政策

機密等級：一般

文件編號： IS-001

版 次： 2.0

發行日期： 114 年 7 月 10 日

目錄

1. 目的.....	3
2. 範圍.....	3
3. 權責.....	4
4. 定義.....	4
5. 作業內容.....	4
6. 附件.....	6

1. 目的

確保本公司所屬之資訊資產及客戶所提供資料的機密性、完整性及可用性，並符合相關法規及合約之要求，使其免於遭受內、外部的蓄意或意外之威脅。

2. 範圍

- 2.1 考量公司之客戶服務中心及利害關係者之需求及期望，基於保護資訊資產機密性、完整性、可用性、個人資料保護為目標，將相關資訊系統使用、客戶服務中心設施及環境優先納入資訊安全管理及個人資料保護管理範圍，展現本公司永續發展經營管理理念。
- 2.2 個人資料保護管理事項依照「個人資料保護管理政策」執行。
- 2.3 為避免因人為疏失、蓄意或天然災害等因素，導致資訊資產不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來可能之風險及危害，應採用組織、人員、技術或實體等面向控制措施適切應對風險。資訊安全管理系統之管理事項如下：
 - 2.3.1 資訊安全管理
 - 2.3.2 資訊安全政策管理。
 - 2.3.3 資訊安全組織管理。
 - 2.3.4 人力資源安全管理。
 - 2.3.5 資訊資產管理。
 - 2.3.6 存取控制管理。
 - 2.3.7 密碼管理。
 - 2.3.8 實體與環境安全管理
 - 2.3.9 作業安全管理。
 - 2.3.10 通訊安全管理。
 - 2.3.11 資訊系統獲取、開發及維護管理。
 - 2.3.12 供應商關係管理。
 - 2.3.13 資訊安全事件管理。
 - 2.3.14 業務持續管理。
 - 2.3.15 遵循性（適法性）管理。
 - 2.3.16 資料安全管理。
 - 2.3.17 變更與組態管理。

2.3.18 雲端服務管理。

3. 權責

3.1 個人資料保護及資訊安全委員會

3.1.1 本公司個人資料保護及資訊發展暨安全管理階層決策組織。

3.1.2 本公司個人資料保護及資訊安全管理制度規劃、建立、實施、維護、審查與持續改善。

3.2 公司同仁、資訊系統服務使用者、委外人員

3.2.1 配合個人資料保護及資訊安全管理制度作業。

3.2.2 遵守相關個人資料保護及資訊安全管理制度規範。

4. 定義

4.1 資訊安全

保護資訊的機密性、完整性及可用性；亦能涉及如鑑別性、可歸責性、不可否認性及可靠性等性質。

4.2 個人資料保護

依照法令法規及合約要求保護所蒐集、處理及利用之個人資料。

5. 作業內容

5.1 原則

5.1.1 應考量相關法律規範、合約及營運要求，進行資訊資產之資訊風險評估，確定個人資料保護及資訊作業安全需求，建立「資訊安全管理程序」作業標準，採取適當資訊安全措施，確保資訊資產安全及個人資料保護事項。

5.1.2 依人員角色及職能為基礎，建立評估或考核制度，並視實際需要辦理個人資料保護及資訊安全教育訓練及宣導活動。

5.1.3 個人資料及資訊資產存取權限之賦予，應依業務需求並考量最小權限、權責區隔及獨立性審查。

5.1.4 建立個人資料事件管理程序及資訊安全事件管理程序，以確保事故妥善回應、控制與處理，訂定業務持續計畫並定期演練，以確保資訊系統或服務持續運作。

5.1.5 依據個人資料保護法與智慧財產法之相關規定，審慎處理及

保護個人資訊與智慧財產權。

5.1.6 定期執行個人資料保護及資訊安全稽核作業，檢視個人資料保護及資訊安全管理制度之落實。

5.1.7 違反本政策與個人資料保護及資訊安全相關規範，依相關法規或人事規定辦理。

5.1.8 為確保所有同仁知悉本身在個人資料保護及資訊安全上應盡職責，應透過個人資料保護及資訊安全持續訓練，強化同仁對個人資料保護及資訊安全要求之認知。

5.2 瞭解組織及其全景

5.2.1 依營運目的，鑑別其會影響個人資料保護及資訊安全管理系統之結果的內部、外部議題，包含相關法律要求或主管機關政策需求及關注方需求，並依鑑別結果建立「組織全景鑑別表」及「業務流程營運衝擊分析表」及「個人資料業務流程分析表」以作為鑑別及執行之依據，並據以確認 ISMS 及 PIMS 之範圍符合性。

5.2.2 「組織全景鑑別表」得於每年重大議題變更時進行確認及必要之修訂。

5.3 目標

5.3.1 維護資訊之機密性、完整性與可用性，並保障個人資料隱私。

5.3.2 保護客戶服務業務資訊，避免未經授權的存取、修改，確保其正確完整。

5.3.3 建立資訊營運持續計畫，以確保客戶服務業務之持續運作。

5.3.4 客戶服務業務執行須符合相關法令或法規及客戶合約之要求。

5.3.5 確保本公司所蒐集、處理及利用之個人資料符合法令及合約要求。

5.3.6 每年依上述目標訂定量化量測項目，填寫於「目標管控及量測表」，依實際執行情形管控。

5.4 審查

5.4.1 本政策應於每年檢討乙次，以適時呈現法令規範、客戶合約

技術、組織及業務等最新發展現況，以確保個人資料保護及資訊安全實務作業之有效性。

5.4.2 本政策必須以書面、電子或其他方式告知所有同仁及提供資訊服務之相關廠商或利害關係者適時取用。

5.5 實施

本政策經個人資料保護及資訊安全委員會核定後實施，修訂時亦同。

6. 附件：

6.1 IS-001-01 目標管控及量測表。