資訊安全治理

1. 資訊安全目的與範圍:

   對象：包括員工、客戶、第三方合作夥伴，以及營運相關資訊軟硬體設備。

   範圍：為確保本公司資訊安全，制定相關規章制度，應用技術和數據安全標準制定，並納入管理運作體系，以保障員工，供應商和客戶之隱私權保護與資訊安全維護。

2. 資訊安全風險架構:

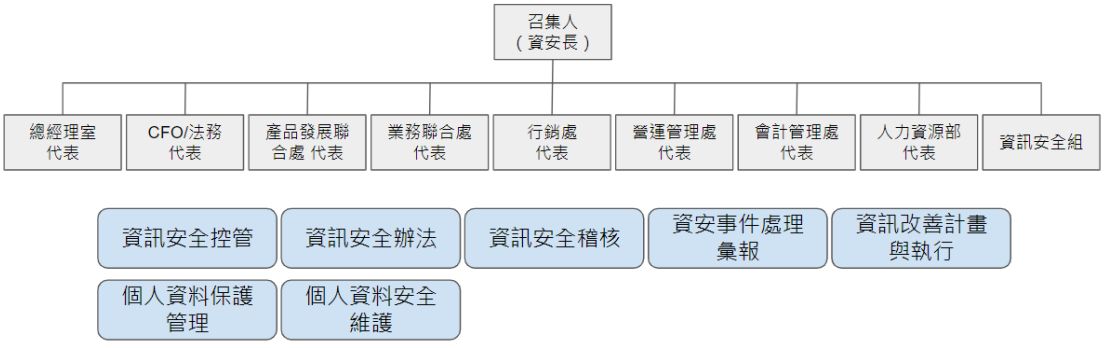
   2.1 企業資訊安全治理組織

   本公司自 2016 年起，依據「91APP 資訊安全政策」，由總經理責成，研發部門主管為召集人，與各部門主管或其指派之代表共同組成「資訊安全委員會」，負責所有資訊安全管控、辦法擬定、內部稽核、資安事件處理彙報及改善計畫與執行。資訊安全委員會亦為本公司個人資料之管理單位，負責訂定個人資料保護管理政策及安全維護計畫等法規規定事項。

   本公司並設有資安專責單位，包含資安專責主管及 2 名資安專責人員，具有 GIAC PenetrationTester(GPEN)、EC Security Analyst(ECSA)、Certified Ethical Hacker(CEH) 、CompTIA Security+ 等專業證照。2022 年，91APP 指派產品發展聯合處資深副總林大維出任 91APP 資安長，統合研發、法務、稽核等單位，統籌資訊安全及保護相關政策制定、執行、風險管理與遵循度查核。此專責單位定期向董事會彙報資安管理成效、資安 相關議題及方向。

   2.2 91APP 資訊安全委員會架構

   本公司目前由資安長任資安委員會召集人，各處處長出任委員，與資訊安全組專責資安人員共同組成資訊安全委員會。



3. 資訊安全政策目標:
    - 確保本公司所提供之系統及服務保有機密性、完整性、可用性，並符合相關法規之要求。
    - 確保本公司所提供之服務，達到善盡保護消費者個人資料安全之責任，並符合相關法規之要求。
    - 確保公司營運業務持續運作，對外提供穩定服務。

4. 資訊安全控制措施:
    - 系統安全
        - ○ 系統架構與設定
            - ■ 所有系統與軟體均必須使用合法版本並適當設定。
            - ■ 所有系統及第三方服務均必須設定系統權限，僅供必要人員使用。
        - ○ 防火牆
            - ■ 網路、資料庫、電腦均必須建置防火牆，並定期更新防火牆軟體與規則。
            - ■ 必需定期執行弱點掃瞄與滲透測試，並彙整報告歸檔。
            - ■ 系統一旦發現有高風險弱點，須列專案處理，並提出明確修復期限。
        - ○ 密碼管理
            - ■ 網路、資料庫、軟體、電腦需使用個人獨立帳號與密碼登入。
            - ■ 應制定密碼相關要求規定，並定期查核所有系統及員工密碼是否符合之。
        - ○ 資料安全
            - ■ 個人可攜式設備(如隨身碟、外接硬碟、筆記型電腦、手機、記憶卡等)應限非公務使用，且不得連接公司網路。
            - ■ 不得使用個人雲端硬碟，儲存本公司系統所保有之任何資料檔案。
            - ■ 信用卡、密碼、交易等敏感性資料應以加密方式儲存，並僅經授權之所屬人員得開啟處理、利用。
            - ■ 以網際網路傳輸上述資料時，亦應以加密方式傳輸。

- 設備安全
  - 所有資訊實體設備需妥善保管、維護，若有遺失、遭人盜用，或發生其他危害設備安全事件，需立即通報並啟動應變措施。
  - 依資訊安全管理辦法之設備安全管理規定，施行設備安全相關作業。
- 系統備援
  - 所有儲存於第三方及內部實體之系統及資料須定期進行備份。
  - 備份資料之所有資料安全保護規格比照原資料安全規格辦理。
  - 定期進行演練並紀錄過程和結果，確保系統在切換至備份時仍可正常提供服務。

- 緊急應變
  - 為快速有效反應資訊安全緊急事件，應定義資安事件應變作業，通報、控管、處理各類資安緊急事件。
- 人員安全管理
  - 對敏感性職務，應於人員晉用前進行安全評估，並於人員晉用、工作及任務指派時，進行必要的考核。
  - 所有員工均應簽署保密協定，並於新進訓練課程施以資安政策宣導。
  - 應每年執行資訊安全教育訓練。
  - 外部訪客亦需遵循本公司資訊安全相關規定。
- 個資保護
  - 本公司系統所保有個人資料檔案應以加密方式儲存，僅經授權之所屬人員得開啟處理、利用。以網際網路傳輸個人資料時，亦應以加密方式為之。
  - 各單位遇有個人資料遭竊取、洩漏、竄改、惡意破壞毀損、作業不慎、駭客攻擊、非法入侵等危害個人資料安全事件，應依資訊安全管理辦法之個人資料侵害緊急應變管理規定，立即通報並啟動應變措施。
  - 所有涉及個人資料處理業務(包含業務終止後)，皆須依照資訊安全管理辦法之個人資料保護安全維護管理規定辦理。

5. 2021 年資訊安全管理項目執行情形:

本公司在 2021 年由資安委員會指導，資訊安全組負責，並由各處協助辦理下，有下列推動執行成果：

- 資安認證
  - 本公司 2021 年持續取得由勤業眾信會計師簽證的 SOC2 無缺失稽核報告，證明 91APP 持續符合美國會計師協會訂立的「服務與組織控制」安全性、可用性、處理完整性、機密性和隱私權等五項確信服務準則
- 資安教育訓練與測驗/社交工程演練
  - 共進行 25 場資安教育訓練，涵蓋所有新進員工
  - 進行法務與資安測驗，補測後通過率 100%
  - 規劃社交工程演練（2021 年規劃，2022 年 1 月執行)
- 資安通報
  - 共發布 6 次資安相關公告，提醒客戶提高資安意識
- 資安情資共享
  - 加入 TWCERT
- 合作夥伴資安評估
  - 共進行 10 次合作夥伴資安評估
- 滲透測試
  - 委託 DevCore 與勤業眾信團隊進行 2 次滲透測試
  - 客戶進行 3 次滲透測試
- 弱點掃描
  - 共進行 4 次 PCI-DSS 規範弱點掃描
  - 自行發動與客戶發動共 10 次弱點掃描