合勤投資控股股份有限公司

資訊安全政策

目的：

為強化資訊安全管理， 建立安全及可信賴之電子化作業平台，確保資料、系統、設備及網路永續運作，並在兼顧資訊安全與工作效率下 ,建立資料處理、傳送及儲存之安全控管機制，擬定本公司之資訊安全管理政策。

1. 資訊安全政策

本公司為達成資訊安全目標訂定之資訊安全管理作業規定、措施、標準、規範及行為準則等，由資訊安全委員會負責辦理 ，每年評估一次，以反映資訊技術及公司業務等最新發展狀況，確保資訊安全實務作業之有效性。 為落實資訊安全管理，本公司相關的資訊安全管理，以書面或電子方式告知公司員工、連線作業之子公司及提供資訊服務之廠商共同遵行。

資訊安全管理之範圍

本公司資訊安全管理涵蓋 13 項資訊安全管理事項，以避免如因人為疏失、蓄意或天然災害等因素，遭致不當使用、洩漏、竄改、破壞等情事，而對本公司帶來可能之風險及危害程度。其安全管理事項如下：

●資訊安全政策訂定與評估。
●資訊安全組織。
●資訊資產分類與管制。
●人員安全管理與教育訓練。
●實體與環境安全。
●通訊與作業安全管理。
●存取控制安全。
●系統開發與維護之安全。
●資訊安全事件之反應及處理。
●營運持續管理。
●相關法規與施行單位政策之符合性。
●專案管理之資訊安全
●供應商管理

2. 資訊安全組織與資訊分類

A. 本公司之資訊安全相關政策由資訊安全委員會負責制定

a. 資訊安全委員會之組成 ：設有專職資安長、稽核、法務及各 BU 代

表共同組成，

統籌資安策略規畫，於 2014 年依 ISO27001 所訂定資訊安全組織架構，成立專職資

訊安全團隊，由資安長領導，負責擬定資訊安全策略與目標、監控資安事件與活動、

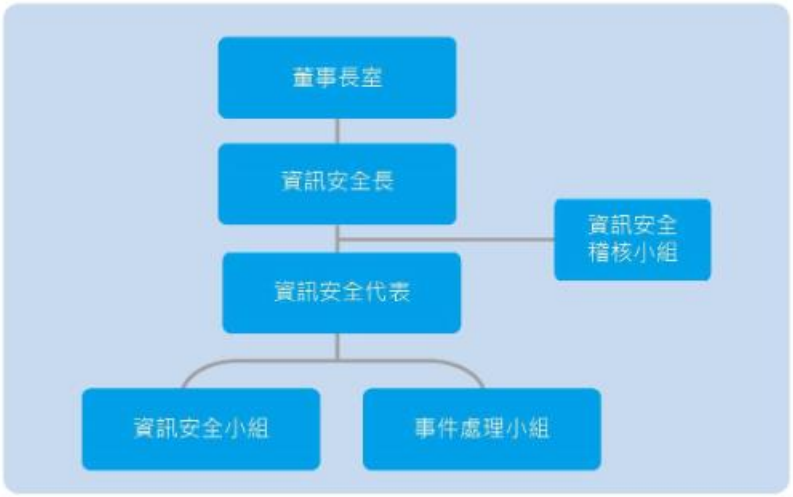
執行各項資訊安全工作與專案、辦理資訊安全宣導教育訓練。

由資安長擔任召集人。

b. 資訊安全委員會之職責：

- 制定資訊安全管理相關規範。
- 推動資訊安全相關活動。
- 辦理資訊安全相關教育訓練。
- 建立風險管理制度，執行風險管理。
- 建立資訊安全事件緊急應變暨復原措施。
- 執行稽核改善建議事項。
- 執行預防措施之改善。
- 研討新資訊安全產品或技術。
- 執行資訊安全委員會決議事項。
- 鑑別資訊安全相關之法規。

資訊安全委員會



c. 資訊安全之執行單位

- 總公司：

  各單位資訊安全符合性稽查，由稽核室會同相關單位負責辦理。

  資訊系統安全控管措施由資訊部配合各 BU 代表負責執行

  門禁管制按照門禁管理辦法執行

- 子公司

  子公司必須指派資訊或適當單位負責，並依總公司規定辦理。

- 委外與第三方[協力廠商]
  依據合約內容配合，本公司資訊安全運作。

B. 資訊分類與控管

- 資訊分級依機密文件分類管理辦法 (機密,限閱及一般)為資訊安全等級之分類標準。
- 配合資訊分級及風險評估，依照資訊資產暨風險評鑑管理程序書管控。
- 對於安全等級要求高的各類資訊文件，不論電子或紙面必須標示清楚。
- 資訊的控管分類應以下列原則來進行：可接受風險的決定、選擇控制措施以及風險改善裝況的後續追蹤。

3. 人員安全與管理

A. 工作說明及資源分配安全

a. 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工有妥適分工，分散權責，儘可能建立人力備援制度 ，並定期演練。

b. 訂定資訊安全員工須知手冊並以書面或電子方式傳送相關員工

B. 使用者訓練

a. 員工必須瞭解單位之資訊安全政策。

b. 隨時公告資訊安全相關訊息。

c. 不定期派員參與外界舉辦相關訓練、研討會、產品發表會。

d. 不同層級之人員進行資訊安全教育宣導或訓練，包含資通安全專職人員(每人每年至少接受 12 小時)、資通安全專職人員以外之資訊人員(每人每年至少接受 6 小時）、一般使用者及主管（每人每年需 3 小時）之資安訓練時數要求，促使人員了解資訊安全的重要性及各種可能的安全風險，提升資安意識，並遵守相關資安規定。

C. 安全及失效事件反映及處理

a. 發生疑似資訊安全事件 ,應以電話、簡訊、e-Mail 或書面向本組織或是親自至本組織進行通報資訊安全委員會，並副本通知直屬主管,。

b. 資訊安全事件發生時的回報及處理依照安全事件管理程序書規範進行處理。。

4. 實體及環境安全管理

A. 安全區域

a. 電腦機房、DCC、資料室、研發區域及其它重要地區，對於進出人員必須由管理人員作必要之限制及監督其活動。
b. 為確保相關設施之安全性，非權責單位指定之人員不得擅自進入安全區域或使用相關資訊設備。
c. 人員進出應設置門禁管制，及適當之身份驗證機制或管控措施，以確保人員須經核准授權後，方可進入。
d. 進入二樓資訊服務機房，需有二種驗證方式，除第一種識別證刷卡驗證，仍需要第二種驗證輸入密碼方能進入機房，而密碼需每半年變更一次。
e. 人員如需申請/異動機房進出權限，應填寫「門禁申請單」提出門禁進出權限異動申請。機房管理員應至少每月 1 次檢視門禁系統進出許可名單及異常存取紀錄。
f. 若外部人員或本組織未具備機房進出權限人員，因執行業務需求進入機房時,必須由資訊資產權責單位或保管單位指派人員隨行並填寫「人員進出機房登記表」後，方可進出機房，並遵守相關設備管理之規定。機房管理員應至少每月 1 次檢視「人員進出機房登記表」登記情況並呈由其主管審查。
g. 安全區域應設置必要之監視設備，對於可進出之通道及重要資訊處理設施進行安全偵測，作為警戒或記錄資訊安全事件之機制。
h. 安全區域之監視設備影像紀錄及門禁進出紀錄至少保存 3 個月。
i. 離開機房時，應確認門窗已確實關閉並上鎖。

B. 一般控制措施
a. 為防止未經授權之存取,同仁應於離開本組織時,遵守桌面淨空政策，並將限閱等級以上之文件與可攜式資訊設備皆存放於櫥櫃並上鎖，避免資訊外洩之機會。
b. 同仁於本組織安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並且儘速通知相關單位進行處理。
c. 同仁需隨時清理個人電腦的資源回收筒，以確保已經刪除的重要資料不會因為遺留在資源回收筒未清理，而遭未經授權之使用。
d. 未經授權不得將設備攜出入安全區域並私自在機房上架使用。如有需要，則須填寫「設備進出紀錄表」，並經主管人員核准後，始得進行。
e. 維護或服務廠商如需攜帶筆記型或平板電腦進入安全區域進行維運時，應於「人員進出機房登記表」註明，並請廠商提供相關安全防護佐證（如：已安裝防毒軟體、防毒軟體病毒碼更新至最新及作業系統弱點更新等畫面），並由本組織專人全程陪同，且不得使用任何可攜式媒體（如：USB、Flash Card 等），以防止資料遭受外洩或不當存取。

5. 網路安全與操作管理

A、網路安全規劃作業：

a. 應建立資訊系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。
b. 資訊系統管理職務與責任應加以區隔，足以影響業務經營管理的資訊，不可只由單獨一人知悉。如因人力資源限制，無法區隔責任，則應加強監督與稽核等措施。
c. 伺服主機及網路設備應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理。主機或網路設備負責人無法進行管理時應由代理人負責，未指定負責人之主機及網路設備由機房管理負責人員負責。
d. 網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。
e. 應規劃系統與設備的開發與測試環境，並避免於已上線運作設備及環境進行開發或測試工作。
f. 系統及設備建置前，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。如需委外開發或採購，則依「委外管理程序書」辦理。
g. 系統設備與軟體之建置，均應依照「系統開發與維護程序書」之程序進行測試及驗收。

B、主機安全防護：

a. 系統負責人應定時檢查作業系統及硬體設備之效能，並注意作業系統版本更新及問題資訊，做最適建議及導入。
b. 主機負責人應進行伺服器主機監控，檢查系統、安全及應用程式日誌紀錄、或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知廠商處理。
c. 為提升伺服器主機連線作業之安全性，得考量使用加密通道等各種安全控管技術。
d. 應關閉不需要之服務。
e. 系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。
f. 應視需要保留日誌紀錄，以利異常事件處理。
g. 軟體由系統負責人安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。
h. 系統軟體測試由系統負責人辦理，測試時應事先公告並通知及協調相

關人員支援，且視狀況需要通知相關人員及使用者以避免因資訊服務中斷而影響業務。

i. 常狀況排除

i.1 遇異常狀況時系統負責人應先行回報單位主管，再依下列步驟處理：

i.1.1 中斷程式或服務

i.1.2 重新開機

i.1.3 其他方式

i.2 通知相關人員協助，並說明詳細原因、先行處理步驟及相關資料。如無法自行排除則向維護廠商報修維護，並將故障情形公告及通知使用者及相關人員。

i.3 將處理過程及結果記錄於「資訊安全事件報告單」中。

j. 系統入侵之處理

j.1 立即拒絕入侵者任何存取動作（例如關閉可疑帳號），以防止災害繼續擴大。

j.2 關閉受侵害的主機，並立即與網路離線。

j.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

j.4 通知主機供應商提供必要的回復協助。

j.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復止，最後再將該主機重新上線。

j.6 將處理過程及結果記錄於「資訊安全事件報告單」中。

C、電子郵件之安全管理

a. 電子信箱帳號之註冊、離職、異動申請，應遵循下列相關管理規範之規定，並填寫「網路帳號申請單」之正式申請程序，經單位部門主管核准後，再交由系統管理者或經授權之管理者建置相關資料。

b. 勿在上下班時間利用電子郵件傳送與工作無關之檔案、圖片、桌面、遊戲程式、盜版軟體等。

c. 除了個人的電子郵件外，公司內所有電子郵件清單皆屬於集團所有，除非經過公司同意外，禁止拿來用於私人用途上，包含註冊各種網路服務。

d. 寄至公司外的電子郵件，禁止傳遞與公司工作上相關的機密文件及資訊，經查獲者將依公司規定嚴處。

e. 請勿隨便發 To All 的電子郵件，To All 的使用條件為「該訊息需與工作上有關且有必要讓全公司都知道。」例如，行政部的公告、福委會訊息、社團活動等。

f. 與工作上沒有任何關係的事情，絕對禁止發 To All 的電子郵件，例如八卦新聞（包含政治、生活趣聞、笑話、生活經驗等），及未經證實

的任何事情。

g. 應禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致其他使用者之不安與不便。

h. 機密等級和限閱等級資料或文件，如需寄送應事前檢視內容有無錯誤後方可傳送，並以壓縮軟體壓縮加密後再行寄出，密碼與檔案應分開寄送。

i. 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

j. 對來路不明之電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

D.公開資訊及外部應用服務安全管理

a. 於對外提供服務之網站上公告、發佈或變更本集團公開資訊，須建立核准程序，並經權責主管審查後執行。

b. 對外部人員提供資訊或應用服務，應採取必要之資料保護或控管措施，以防範詐欺活動、契約爭議及未經授權之揭露與修改，確保資料的完整性與安全性。

c. 對外提供服務之網站應停用任何不需要或不使用之服務與網路通訊協定，降低遭受攻擊之風險與減少開放給攻擊者之途徑。

E. 無線網路使用之管理

a. 無線網路基地台之使用應經適當控管。

b. 無線網路設備之安裝設定應經核准。

c. 無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。

d. 無線網路設備之使用應有適當管理機制，例如：帳號身份之確認、授權使用之 IP 數量、連接埠、網卡位址（Mac address）過濾等。

6. 存取控制

A. 存取控制之營運要求

a. 資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

b. 應正確地使用資訊資產，以維護資訊資產之可用性、完整性與機密性。

c. 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。

d. 被賦予系統管理最高權限之人員、掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

e. 因處理系統當機與異常狀況需視狀況授與適當存取權限，並避免共用

帳號。

f. 可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、光碟、磁帶等，應採取適當之控管措施，以防止未經授權之資料、系統、網路存取或病毒傳播。

g. 資料、資訊之存取，必須符合「個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資料保護及資料存取使用控管之規定。

h. 針對無人看管的資訊資產設備，應有適當控管程序，以防未經授權之存取或濫用。

i. 個人桌上型電腦、可攜式電腦不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未經授權之存取。

B. 使用者存取管理

a. 須符合各項系統資源使用權限之申請、註冊及註銷作業管理程序，並留存維護相關之申請、註冊、註銷資料與紀錄，以備查核。

b. 使用者職務異動或離職時，部門主管應即時通知相關單位調整或終止使用者之存取權限。

c. 特殊權限之使用者必須與一般權限之使用者區分管理；針對特殊權限帳號，應妥善管理。

d. 特殊權限之授權管理，必須依執行業務系統別之需求，例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。

e. 系統相關作業人員需經正式授權存取業務相關之資訊資產，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。

f. 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）應有書面紀錄並妥善保管該項文件。

g. 使用者帳號與存取權限應於每半年定期審查一次，以妥善管理久未登錄系統之帳戶，並將閒置帳號予以停用或刪除，且記錄清查結果於「帳號清查紀錄表」；第二級防火牆/網路設備則為每年至少執行一次。

h. 應強制要求使用者變更初始密碼並定期變更密碼。

7. 系統開發與維護

A. 系統維護

a. 系統負責人需定期檢視更新系統之安全修補、防毒軟體及病毒碼，以維持系統正常運作。

b. 系統更新須經過評估及核准後始能進行，並先於測試環境進行安裝，並檢視是否造成系統異常，如無異常再視需要予以更新。

c. 在採購套裝軟體時，應視其安全需求，進行分析。除事前需經權責單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。

d. 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，可能帶來之風險與損害程度。

e. 程式原始碼須有版本控管機制,若需變更,須由經授權人員執行變更,並保留存取行為紀錄與至少 3 代的程式原始碼。

B. 系統開發的安全

a. 委外開發合約中須對著作權之歸屬訂有規範內容。

b. 應用系統服務上線前，須進行相關風險評估與技術檢測(弱點掃描、滲透測試），以處理所面臨之風險，而資安檢測項目定義於「系統資安項目查檢表」???中。

c. 系統開發及正式作業必須在不同的系統環境處理，並且使用不同的登入程序。

C. 系統資料之安全

a. 各項系統設定檔、網頁資料、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」。

b. 應視回復測試之可行性，每年於測試主機上測試備份復原是否正確。

b. 儲存媒體依保存規格要求存放在安全的環境。

8. 永續經營管理

A. 對於可能影響營運之狀況應訂有明確的緊急應變計畫及備援措施

B. 對於關鍵性系統信擬訂其風險評估、衝擊影響並檢討系統停頓的企業損失。

C. 指定適當層級主管負責永續經營政策之執行與協調。

D. 定期作風險評估並調整永續經營政策。

E. 緊急應變計畫復原程序須測試無誤。

9. 內部稽查，法規及其他

A. 安全政策與技術符合性之考量

a. 相關措施必須留下相關記錄檔案供內部稽核。

b. 每年應至少執行 1 次資訊安全內部稽核作業。亦可視需要不定期執行

專案稽核。

c. 須有專人負責管理與資訊安全相關的記錄檔案。

B. 內部稽核考量

a. 訂定本公司內部稽核管理規定

b. 定期稽查資訊安全事項辦理情形。

c. 稽查人員須經過訓練並作事前工作分配。

d. 須訂有資訊安全作業稽查計畫(含稽查內容、範圍、程序、人員)，並公布。

C. 符合法規要求

a. 組織執行業務時，應遵守相關法令、法規之要求。

b. 資訊安全稽核小組亦應於每次進行資訊安全稽核時，檢視其符合性。