勤益投資控股股份有限公司
制度規範說明書

編　　號	主題	資通安全管理辦法	生效日期	頁次	1/10
GTM-MIS-0002			107.02.23	版本	1

一、目的

本文件提供本公司資通安全系統管理實施原則建議,以增進資訊作業之安全性，確保公司資料之機密性、完整性與可用性。

二、適用範圍

本公司內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

三、實施規定

1 **網路安全**

1.1 網路控制措施

1.1.1 與外界連線,應僅限於經由網路管理單位之管控,以符合一致性與單一性之安全要求。

1.1.2 應禁止以私人架設網路（如：電話線、2G 或 3G 網路等）連結機房內之主機電腦或網路設備。

1.1.3 宜依業務性質之不同，區分不同內部網路網段，例如：行政、宿網等，以降低未經授權存取之風險。

1.1.4 對於開放提供外部使用者或廠商存取之服務,必須限制使用者之來源 IP 及網路連線埠(Port)，以確保安全。

1.2 無線網路存取

1.2.1 應禁止使用者私自將無線網路存取設備介接至本公司網路;若有介接之必要應經權責管理人員同意並設定帳號密碼或加密金鑰以防未經許可之盜用。

1.2.2 本公司內應提供無線網路存取服務,並採取適當安全管控措施：

- 提供之無線網路熱點建議設定加密金鑰防護,並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。
- 於辦公室區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制,並經由本公司無線路漫遊服務系統提供外來之來賓使用。

2 系統安全

2.1 設備區隔

伺服器主機可依個別應用系統之需要，設置專屬主機，以避免未經授權之存取，例如網路服務主機(電子郵件、網站主機)、系統主機(例如隨選視訊主機)等。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

2.2.1 個人電腦應：

- 裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。
- 作業系統及軟體應定期更新，以防範系統漏洞。

2.2.2 個人電腦所使用的軟體應有授權。

2.2.3 新伺服器系統啟用前，應執行相關程序(如：確認適合該作業系統之掃毒工具、預設密碼更新、系統更新等，並記錄於「啟用與報廢紀錄單」)，以防範可能隱藏的病毒或後門程式。

2.3 桌面淨空與螢幕淨空政策

2.3.1 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密或敏感特性的資料（如公文、資料等）妥善存放。

2.3.2 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全個人電腦應設定螢幕保護機制。

2.4 資料備份

2.4.1 系統管理人員需針對公司重要電腦系統及資料（如:系統檔案、網站、資料庫等）應定期(日、月、季)至少進行一次備份工作；建議使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。

2.4.2 每年應定期檢查備份資料之可用性與完整性。

2.5 資訊工作日誌

2.5.1 系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作

時，應針對這些活動填寫紀錄於「資訊工作日誌」，作為未來需要時之查核。

2.5.2　系統管理人員應至少每季執行一次校時。

2.6　資訊存取限制

共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（如：限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。

2.7　使用者註冊

人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容：

- 使用唯一的使用者帳號。
- 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
- 保存一份包含所有帳號註冊的記錄。
- 使用者調職或離職後，應移除其帳號的存取權限。
- 定期應檢查使用者帳號，以確保帳號的有效性。

2.8　密碼（Password）之使用

2.8.1　管制使用者第一次登入系統時，必須立即更改預設密碼，預設密碼應設定有效期限。

2.8.2　資訊系統與服務應避免使用共用帳號及密碼。

2.8.3　公司應發佈『密碼設定與使用規則』(詳附件一)給使用者，內容應包含以下各項：

- 使用者應該對其個人所持有密碼盡保密責任。
- 要求使用者的密碼設定，建議應該包含英文字及數字，長度為 4 碼（含）以上。

2.9　通報安全事件與處理

2.9.1 資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩等。

2.9.2 資訊安全事件等級，由輕微至嚴重區分等級如下：

- 符合下列任一情形者，屬 0 級事件：

(1) 未確定事件或待確認工單:來自不同計畫所使用新型技術(A-SOC，miniSOC,…)所產生之工單，但其正確性有待確認。

(2) 設置檢舉信箱通告之資安事件。

- 符合下列任一情形者，屬 1 級事件：

(1) 非核心業務資料遭洩漏。

(2) 非核心業務系統或資料遭竄改。

(3) 非核心業務運作遭影響或短暫停頓。

- 符合下列任一情形者，屬 2 級事件：

(1) 非屬密級或敏感之核心業務資料遭洩漏。

(2) 核心業務系統或資料遭輕微竄改。

(3) 核心業務運作遭影響或系統效率降低,於可容忍中斷時間內回復正常運作。

- 符合下列任一情形者，屬 3 級事件：

(1) 密級或敏感公務資料遭洩漏。

(2) 核心業務系統或資料遭嚴重竄改。

(3) 核心業務運作遭影響或系統停頓,無法於可容忍中斷時間內回復正常運作。

- 符合下列任一情形者，屬 4 級事件：

(1) 公司機密資料遭洩漏。

(2) 公司重要資訊基礎建設系統或資料遭竄改。

(3) 公司重要資訊基礎建設運作遭影響或系統停頓,無法於可容忍中斷時間內回復正常運作。

2.9.3 任何人發現異常情況或疑似資安事件,應立即向資安業務承辦人通報，資安業務承辦人應儘速進行處理並研判事件等級。

2.9.4 資安業務承辦人當發生研判事件等級 3（含）以上之事件，應立即通報資訊主管及總經理，並以電話聯絡資訊安全管理單位，由

總經理儘快召集會議研商處理的方式。

2.9.5 當發生無法處理之資通安全事件,應通報資訊安全管理單位協助處理。

2.9.6 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事件發生後 72 小時內處理完成並結案(包括通報與應變)，3、4 級事件於事件發生後 36 小時內完成並結案。

2.10 災害復原計劃

2.10.1 對於災害發生時，應依『系統復原計劃及測試程序規則』(詳附件二)，採取事先訂定之步驟及因應措施，並按既定之復原程序作完整而有秩序之復原，以減少因災害而造成之損失至最低程度。

2.10.2 擬訂災害復原計畫並定期執行測試，並將測試結果作成記錄呈報權責主管。

3 實體安全

3.1 設備安置及保護

3.1.1 主機機房宜設置偵煙、偵熱或滅火設備（氣體式滅火器)，並禁止擺放易燃物或飲食。

3.1.2 主機機房及電腦教室的電源線插頭應有接地的連結或有避雷針等裝置，避免如雷擊事件所造成損害情況。

3.2 溫濕度控制

重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在 20℃~25℃，濕度建議控制在相對濕度 50%R.H.~70%R.H.)，以防止資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。

3.3 電源供應

重要的資訊設備（如：主機機房等）應有適當的電力保護設施，例如設置 UPS、電源保護措施(如：穩壓器、接地等)，以免斷電或過負載而造成損失，並設置緊急照明設備以作為停電照明之用。

3.4 纜線安全

主機機房及電腦教室內線路應考量設置保護設施(如:高架地板、線槽、

套管等)。

3.5 設備與儲存媒體之安全報廢或再使用

所有包括儲存媒體的設備項目,在報廢前應填寫「啟用與報廢紀錄單」,確認已將任何敏感資料和授權軟體刪除或覆寫。

3.6 財產攜出

3.6.1 禁止資訊設備在未經授權之情況下攜離所屬區域,若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。

3.6.2 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。

4 可攜式電腦設備與媒體

4.1 公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定密碼、圖形辨識、臉孔辨識或指紋辨識等。

4.2 公務用可攜式電腦設備應執行安全相關程序（如：掃毒、預設密碼更新、系統更新等），以防範可能隱藏的病毒或後門程式。

4.3 公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。

5 人員安全

5.1 人員安全責任

為維護公務機密、個人權益及公司機敏資料，新進人員須簽署「維護公務機密暨競業禁止契約」。

5.2 資訊安全教育與訓練

5.2.1 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。

5.2.2 鼓勵所有員工參與資訊安全教育訓練或宣導活動,以提昇資訊安全認知。

6 資訊業務委外管理

6.1 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規

定。

6.2 委外廠商服務異動或終止時，應填寫「電腦系統使用/取消申請單」中止或刪除其系統上的帳號與權限。

7 應對以下各項相關法令有基礎之認知，並隨時教育宣導。

7.1 智慧財產權

著作權法

7.2 個人資訊的資料保護及隱私

個人資料保護法及施行細則

7.3 刑法電腦犯罪專章

編　　號	主題	資通安全管理辦法	生效日期	頁次	8/10
GTM-MIS-0002			107.02.23	版本	1

附件一

密碼設定與使用規則

一、密碼設定原則

1. 混合大寫與小寫字母、數字，特殊符號。
2. 密碼越長越好，最短也應該在 4 個字以上。
3. 依不同使用者設定密碼變更時間，系統使用頻率較高之使用者至少每三個月更改一次密碼。
4. 使用技巧記住密碼
   - 使用字首字尾記憶法：
     a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
     b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc
   - 中文輸入按鍵記憶法：
     a. 例如「密碼」的注音輸入為「wj/ vu/6a83」

二、應該避免的作法

1. 嚴禁不設密碼
2. 密碼嚴禁與帳號相同
3. 密碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如公司或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的密碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11. 不分享密碼內容給任何人，包括男女朋友、職務代理人、上司等。

附件二

系統復原計劃及測試程序規則

一、目的

為確保電腦系統在受損時,能有秩序且及時的運作,並且確保公司電腦資料在恢復時的完整性,以降低因作業中斷所造成的損失。

二、範圍

適用於 DB 主機。

三、目標

系統復原計劃應達到以下目標

1.儘速隔離損害來源

2.儘速恢復設備運作

3.利用備份設施及媒體進行災變復原

4.協調使用單位補齊作業中斷期間資料

四、系統復原計劃

1.系統復原相關範圍定義

(1)公司及所屬各部門應定義及評估重要電腦作業,電腦資源及各類災變威脅並根據此做成影響評估及人工作業替代程序。

(2)災變所指範圍包含一切天然或人為災害,凡對於重要電腦作業造成終止狀況即符合系統復原計劃所指範圍。

2.相關聯絡人

重要電腦作業的相關單位,其主管及主要操作人員均為相關聯絡人，應建立緊急聯絡管道保持聯繫。

3.災變宣告

各單位作業人員發現災變發生後,盡可能先行搶救以隔離災變源,並即時通知相關聯絡人。

4.災變管理

(1)災變處理應注意人員的安全。

(2)災變處理以專業防災人員指揮為主,否則由現場最高主管指揮調度,應以減少災變範圍擴大為優先考量。

(3)災變處理時需保持冷靜,注意周圍環境情況,並排除閒雜人等駐足圍觀。

5.資料檔案回復程序

(1)系統回復可根據 SYBASE 系統使用說明。

(2)資料檔案回復前請檢視所有備份媒體(文)種類及資料期間。

(3)聯繫設備廠商提供相關設備租借或緊急採購。

(4)通知使用單位收集時差性資料做補建準備工作。

(5)電腦設備除現有設置地點外,另選定適當可供災害回復處理場所供備用。