花仙子企業股份有限公司
資通安全管理辦法

一． 目的:

為達資訊系統之完整性，資料之通透性、安全性，並完成公司全面資訊化，特訂定此管理規則以為各項業務資訊化之規範。

二．範圍:

(一)本法所指各項專有名詞及名稱解釋如下：

1．資訊設備：為資訊之輸出、入時所使用硬體設備，如個人電腦、平板、印表機、數據機、掃瞄器、螢幕、磁碟機、網路設備、不斷電系統．．等相關設備。

2．資訊文件：使用資訊設備所產生之電子文件。

3．固定資產取得作業：詳不動產廠房及設備取得作業(CA-600)。

4．固定資產維護作業：詳不動產廠房及設備取得作業(CA-600)。

5．固定資產異動作業：詳不動產廠房及設備取得作業(CA-600)。

6．固定資產處置作業：詳不動產廠房及設處置作業(CA-601)。

7．儲存設備(儲存媒體)：用於儲存電子文件資料之各種讀寫設備之總稱。如磁碟片、磁碟機、光碟片、磁帶機、可保存式記憶體等等謂之。

(二)本法由資訊部訂定之，且本法之廢止、修改、增減條文皆須由執行長核可後實施。

(三)資訊部之權責：

1．負責資訊安全管理辦法之訂定。

2．負責資料輸出、入之查核。

3．負責資訊設備需求之初核。

4．負責人員使用設備之密碼管制。

5．提報資訊系統軟、硬體使用建議說明。

6．提報資訊安全查核狀況與建議。

7．統籌處理公司各部門資訊系統之建立並協助執行。

8．各部門業務電腦化之規劃、協調及推動。

9．電腦軟硬體設備之維護及技術支援。

10．各部門資訊安全使用狀況查核。

11．電腦室主機房設備之安全維護與設置管制。

12．各項資訊設備需求之審核與建議。

13．提供各部門軟、硬體問題諮詢。

14．建立各項技術文件，並提供線上查詢。

15．提供並排定各項資訊使用教育訓練。

(四)資訊使用人員權責

1．對所使用之資訊設備有保管及維護其外觀清潔之責。

2．對所使用之各項資訊文件有保密及確保其正確性之責。

3．對所使用之密碼及使用權限有保密及善用之責。

三、流程圖：依電子計算機循環

四、作業程序：

(一)資訊設備之使用

1．資訊設備之新購、添購與啟用：

(1)依不動產廠房及設備取得作業(CA-600)流程進行購置。

(2)其設備之點交及驗收，須由資訊部負責設備人員隨同點交及驗收方可生效。

(3)設備完成購置後，如為個人設備須由申請人員填寫資訊系統密碼申請表(F-G-10)，如需使用ERP或其他應用系統，則須填寫系統權限申請單(F-G-117)。

(4)資訊部提供適當之操作手冊教育使用者依正確方式使用，並由設備使用者簽收行動裝置及軟體配備單(F-G-163)後開始啟用。

2．資訊設備之維護與維修：

(1)資訊設備之維護由設備保管人為之，負責外觀之清潔，環境之維護及設備之保管。

(2)資訊部應定期維護，以保持資訊設備維持最佳工作狀態，防範設備損害維修之事件發。並於維護時填寫定期維修表備查。

(3)資訊設備發生保管使用者無法處理之狀況時，得填寫資訊服務申請單(F-G-42)經部門主管核定後，報請資訊部派員維修。

(4)如因設備損害無法使用，使用者應先填具資訊服務申請單(F-G-42)，交由資訊部進行維修。維修期間，由資訊部調換堪用設備給使用者暫用，待設備回復後再由資訊部派員裝設完成，點交後啟用。

(5)緊急或特殊狀況發生時，由資訊部立即派員修護，唯完成後，由使用者補填資訊服務申請單(F-G-42)，完成程序後，交資訊部備查。

(6)維護或維修時，設備維修人員須將處理過程詳實記錄於資訊服務申請單(F-G-42)備查。

(7)資訊部應定期將修復內容於EIP系統文件庫中建立技術資料庫，以利技術之傳承及統計數值，並考慮排定適當之教育訓練課程以加強使用者錯誤排除之能力，進而減少錯誤之產生。

3．軟體之設計、購置、修改、起用：

(1)由需求部門填寫資訊服務申請單(F-G-42)，經部門主管核准後，由資訊部評估可行性後，如需外包設計，資訊部門先提簽呈(F-G-06)做為評估報告，批准後由申請單位寫總務請採購單(F-G-14)，依金額核決權限核可後，才進行開發或委託廠商設計。

(2)委託廠商設計時，由資訊部依不動產廠房及設備取得作業(CA-600)流程進行購置，並與廠商訂立設計、維護合約，以維系統、程式之正常運作，並保障現有系統、程式之安全。

(3)如自行開發，則以下程序進行，並填具書面資料以備查：

系統分析→程式設計→文件製作→系統導入→測試修正→正式起用。

(4)程式或程序之起用，須擬定測試計劃經資訊人員與相關使用者測試無誤並填具測試記錄單(UAT 文件) (F-G-164)備查後，始可啟用。

(5)系統、程式正式起用後，如需修正，則依本條第 1、2、3 條文程序辦理。

(6)系統程式開發設計之前二階段，應由需求部門使用者參與討論，必要時召開會議，使程式設計者(廠商)實際瞭解使用者之真正需求，以求程式之完全符合需求 。

(7)系統程式之設計應加入各項權限之設定與限制，達到階段控管、層次控管、流程控管之效，以確保資訊之安全與完善應用 。

(8)系統程式之設計應考慮軌跡追查之必要性，資料格式之正確性，自動報表之可行性，自動編號之標準性 。

(9)系統程式之設計應有自動產生錯誤訊息之功能，以利程式錯誤之處理。

(10)系統程式之設計應考慮使用狀況之追查，並設置可能之插斷點 。

(11)如為新舊系統程式之替換時，新系統應可將舊系統之資料整合至新系統，否則應採雙軌制，並將舊系統保留，直至舊系統資料已無保存價值時，始可廢止舊系統 。

(12)為防止軟體之濫用、盜用、非法使用，員工應於入職時簽訂資訊系統使用切結書(F-G-122)外，並由資訊部定期排定檢測時間表，稽查、檢測軟體使用狀況發現異狀時應立即制止並排除錯誤 。

(13)系統開發完成後，將完成之各項資料依序存放於電腦、檔案中，於完成系統測試程式後，將其相關文件資料（如系統說明書、操作手冊等）交由資訊單位保管。

(14)系統文件應由專人負責保管。

(15)系統文件之借閱，應限制相關人員方得借閱。

(16)系統修改時，文件應隨之修改，並註明修改時間。

4．公共設備資源之使用，借用者應填寫資訊服務申請單(F-G-42)，經核可後，

由資訊部設定起用。

5．各部門間之設備借用或共用，應報請資訊部協助辦理，不應私自變動設備。

6．如為資訊設備之調撥，則依不動產廠房及設備取得作業(CA-600)固定資產異動作業辦理。

7．資訊設備之購置、使用、調撥，應考慮設備內容，經濟效益，未來發展，當時資訊設備發展狀況，使用者程度，使用之功能等等為考量點，確切達到物盡其用之效。

8．其他資訊設備之處置作業可依不動產廠房及設處置作業(CA-601)辦理。

9．相關軟體，應每半年配合公司盤點進行版權重新計算，盤點後應重新登載軟體盤點清冊(F-G-121)，如有版權不足數，應在每年第三季完成版權補。

(二)資料之分類使用

1．依資料大件之重要性分：保密資料、保護資料、共用資料、一般資料，分述如下：

(1)保密資料：

1. 只有資料之使用者及相關人員可讀取、修改或搜尋到之檔案。
2. 此類檔案資料依使用之軟體不同作適當之保護作業，如設定開啟檔案密碼及編輯密碼。
3. 嚴禁使用網路分享。
4. 只能儲存於受保護管制之儲存設備。
5. 列印時須經一定程序之權限核可後始可輸出。
6. 設定版本版次稽查追蹤資料輸出入。

(2)保護資料：

1. 可設定網路分享，唯須區分唯讀密碼及完全控制密碼。
2. 此類檔案資料依使用之軟體不同作適當之保護作業，如設定開啟檔案密碼及編輯密碼。
3. 必要時可設定使用者權限。

(3)共用資料：

1. 儲存於共用資料區。
2. 依資料之用途做密碼分類保護，限定使用人員。
3. 依資料之不同，分別設立群組，訂定使用原則。
4. 各個共同資料群組分別設立一人以上之資料維護人員以確保資料之正確性及可用性。

(4)一般資料：

1. 可儲存於共用資料區。
2. 必要時可作密碼保護。
3. 由使用者自行管制與應用，唯不得隨意複製，成為資訊垃圾。

2．應依資料之重要性，分別設立保管人，並定期製作資料備份，以確保資料之安全

與正確性。

3．備份之製作分每日備份、定期備份、重大備份，分述如下：

(1)每日備份：應用程式資料庫應進行每日資料備份。可使用覆蓋式備份，但以間隔式覆蓋為原則，以確保資料安全。

(2)定期備份：雲端系統之映象檔採定期備份計劃，依計劃執行之時程備份。

(3)重大備份：遇重大改版，或重大資料轉換時，所作之備份，此種備份常需作妥善之保管，並作較常期之保存。

4．依資料庫之可用性分：線上資料庫、暫存資料庫、短期資料庫、永久資料庫，分述如下：

(1)線上資料庫：即時上線使用之資料庫，依資料之時效性不同設定時間，將線上使用之資料轉存至短期資料庫，本資料庫提供現階段經常性輸入、修改、輸出之資料。

(2)暫存資料庫：由程式自動產生之資料庫，提供查詢、列印短期性發生之各項作業資料、作為程式運算之運用資料庫。

(3)短期資料庫：存放非線上使用之短期存檔資料庫，以利各項非經常性查詢、修正、統計、列印作業之迅速確實完成。如年度資料週期行資料、固定長期性報表、統計資料等等。

(4)永久資料庫：本資料庫存放須永久保存、備查之重要資料，以為各項稽查、統計、列印處理作業之根據。

5．資料之輸出、入，除依本項第 1 條重要性分類保密保護外，各部門主管應詳加查核及管制資料輸出、入之正確性。

6．一般性、例行性公事所需之報表，依相關之作業流程控管，經相關核准權限完成列印，唯若屬機密性資料，除依核定權限核可後方能列印外，其列印時應於列印機旁注視，以防機密之外漏。

7．必要時需於列印之報表內加印輸出者姓名及列印時間以備查。

8．各資料之儲存應有記錄，如須使用儲存媒體，需在外標籤，詳實記載檔案資料之用途、登錄時間，必要時設置目錄表單。

9．各部門資料必要時應設置檔案櫃，以保護儲存設備及資料，並設置查詢目錄，指定專人保護管制，以利資料之取用與管理。

10．必要時依資料使用之應用程式功能設置讀取與修改密碼，以確保資料之保密與安全。

11．各部門應要求加強各同仁之設備、程式操作能力，以提升各項資料處理之可信度與時效性，必要時申請內部教育訓練。

12．為加強同仁操作能力，必要時資訊部得舉辦能力測驗，以確保各項應用程式之可用性與活用程度。並以測驗結果為各項軟、硬體調配、設置、購買之考慮因素。

13．資料之對外連線對傳，除申請許可之工作站外不得對外傳輸，且傳輸時須設置線上掃瞄程式以防病毒之破壞。

(三)資料輸入管理：

1．資料輸入人員於收到原始憑證、單據時，應先審核資料內容業經權限主管簽核，但無異常情形者，方得據以登錄。

2．資料輸入處理應留下可供確認記錄。

3．應用程式對資料正確性應有下列核對功能：

(1)資料屬性(文字、數字.....等)檢查。

(2)檢查碼核對。

(3)範圍限度檢查。

(4)代號對照表查對。

(5)資料間關聯性檢查。

4．當發生錯誤時，應先分析是屬於資料本身錯誤，或主檔錯誤，或程式錯誤，並追究其原因，採取不同應變措施。

5．錯誤資料之更正，須經過適當申請程序，並經單位主管核准。

6．錯誤資料更正後，應能確定資料已經正確更正，並留下記錄。

(四)資料輸出管理：

1．輸出不成功需重新處理時，原印製未完之輸出應確實作廢。

2．輸出資料使用後若無保存需要，應經過適當燬棄處理。

3．輸出資料若以磁性媒體保存時應定期檢查，以確定在必要時能以報表方式列印。

(五)安全措施

1．主機設備應設置溫控設備，以提供主機於安全作業溫度下執行系統程式，確保系統安全運作。機房溫度如超過 28 度，須全面停機，避免硬體損壞，造成資料流失。

2．各項主要之資訊設備應設置不斷電系統，確保穩定供電，需設置不斷電系統確保之不斷電系統需按年限更換電池。

3．為確保資料之安全，應擬定備份計劃，確保資料損毀後之回復，必要時將資料依本項第 4 條可用性分類，分別備份於保存年限不同之儲存媒體，如:NAS、硬碟機、外接磁碟等。備份資料須在每個上班日檢查是否備分成功，檢查人員應填具資料備份記錄暨機房日常檢查表(F-G-40)

4．依資料及程式之重要性分別訂定復原計劃如下：

(1)主要伺服器程式資料之復原:

1. 主要伺服器之程序資料由資訊部人員作維護控管，分別依事件之狀況，作

適當確切之維護與處理。

2. 如遇重大之程式錯誤，應立即報告資訊部主管，作安全、妥善、迅速之處理，並由處理作業人員填寫資訊異常事件紀錄表(F-G-140)，由資訊部主管簽核後存檔後備查。

3. 如因伺服器之硬體設備損壞，而造成伺服程式系統當機，則應立即安排備用主機(與原使用主機配備相近)起動相同伺服程序系統正常作業，待主機修護完善後，再行重新上線作業。

4. 如為伺服系統損毀，則依該系統之修護程序作安全適當之修護，若無法修護完整，則起動最近一次之備份系統回復作業

5. 如因故無法起用最近一次之備份系統回復作業，則應會商各程式、資料之使用部門，共同訂定回復程序、回復內容，回復時間及版本，由執行長核准後由資訊部實施之。

(2)主要應用程式資料(如 SAP、EIP、Cognos)之復原：

1. 由資訊部依該程式資料之發生事件狀況，作確切安全之維護與處理。並依各程式之狀況將重要資料作備份性之資料抄錄。

2. 程式損毀或無法正常作業實得由資訊部主管核可後作同一版本之程式回復安裝，並作好各使用工作站之各別設定，並依各程式之各別情況，應立刻修護完全。

3. 回復作業完成後，須作安全性之追蹤使用狀況，如有不同於前之情況，應立刻修護完全。完成後處理人員應填寫資訊異常事件紀錄表(F-G-140)存檔備查。

(3)伺服器操作系統程式資料(OS)之復原：

1. 系統使用者依該系統之使用錯誤報告，提報資訊部人員，作錯誤處理之依據，並由資訊部人員作安全適切之修護。

2. 如錯誤無法更正，則須會商使用者，是否先作原資料之備份後，由資訊部人員作與原操作系統相同版本、相同設定之回復安裝，測試無誤後，回復原資料之備份。完成後處理人員應填寫資訊異常事件紀錄表(F-G-140)存檔備查。

(4)工作站應用程式及操作系統程式資料(OS)之復原：

1. 使用者依該系統之使用錯誤報告，提報資訊部人員，作錯誤處理之依據，並可由使用者作安全適切之修護。

2. 如錯誤無法更正，則須會商資訊部，由使用者決定是否先作原資料之備份後，由資訊部人員作與原應用程式相同版本、相同設定之回復安裝。完成後處理人員應填寫資訊異常事件紀錄表(F-G-140)存檔備查。

5．電腦室之安全措施除依本項第 1 條、第 2 條規定辦理外，其進出應管制非使用、維護人員不得進入，並須填寫電腦機房進出登記表(F-G-43)備查。

6．為資訊使用之安全，應設置各種權限密碼，如開機密碼、上各網路密碼、各種資料取用權限密碼，管理等級密碼，控制密碼等，並由各部門主管控管，並不得將

密碼告知非自身以外之人員使用，以確保資料取存之安全。

7．各部門人員所保管、使用之各項資訊設備及電子文件應明列，必要時應造冊管制，作為業務交接、代理之依據。

8．對已提辭呈之員工，儘量避免允許其於離職前接近敏感或機密性程式或檔案。

9．員工離職時，其所經手之一切文件、磁帶、磁碟、磁片等均需盤點清楚並辦理移交。

10．員工離職後，其曾接觸之密碼應予以適當調整更動，由資訊部於員工離退流程確認表(F-G-114)上檢核資訊設備移交後，將離職人員之各項使用帳號凍結或刪除使用。

11．如有外部媒體需進入須進入區域網路使用，需先交由資訊人員掃描確認無病毒後，再由資訊人員放入區域網路。

(六)遠端存取及 Internet 服務作業

1．本章所定義的遠端存取及 Internet 服務作業共有下列三項：

(1)外勤或駐外人員由公司外部透過 Internet VPN 存取公司內部個人資料，及由 Internet 存取 POP3 電子郵件。

(2)資訊部人員透過 VNC 連接伺服器。

(3)公司內部人員透過 Internet 對外上網或傳送資料。

2．使用人員如有在公司外部透過VPN存取資料需求，須填具資訊系統密碼申請表(F-G-10)，待核准後資訊部方將存取權限開啓，如有使用截止日，應在截止日將存取權限回收。

3．資訊人員如有處理伺服器異常，得透過 VNC 操作伺服器時，待先口頭向資訊部主管報備，同時處理完畢後應填寫資訊異常事件紀錄表(F-G-140)備查。

4．存取權限應依據 最小授權原則 (Least Privilege Principle) 設定，確保員工僅能存取業務所需的最少資源。

5．若 VPN 存取權限未於 30 日內使用，資訊部門應自動停用該帳戶，重新啟用需重新申請。

6．禁止使用未經資訊部門核准的遠端存取工具，如 TeamViewer、AnyDesk 等，以確保存取行為受控。

7．強制實施多重身分驗證 (MFA)。

(1) 所有遠端存取帳戶必須使用多重身分驗證 (MFA)，以確保身分驗證安全性。

(2) 身分驗證方式可包括但不限於：

- OTP（一次性密碼）認證
- 硬體或軟體 Token
- 指紋或生物辨識技術

(3) 對於具有 高權限（如系統管理者）的帳戶，應採用更高安全等級的 MFA，例如 FIDO2 硬體安全金鑰。

8．遠端存取加密與安全要求。

(1) 所有遠端存取流量必須透過安全加密通道（TLS 1.2 以上），並確保憑證有效性。

(2) 禁止使用不安全的協議與加密方式，例如：

- Telnet、FTP（應改用 SFTP）
- SSL 3.0 / TLS 1.0（應升級至 TLS 1.2 或以上）

(3) VPN 伺服器與身份驗證系統須定期更新安全性憑證，避免過期或弱加密漏洞。

(4) 公司內部系統如 ERP、EIP 等，若提供遠端存取功能，應強制使用 HTTPS 加密。

9．使用者行為監控與異常偵測。

(1) 所有遠端存取行為應記錄日誌（Log），並至少保存 6 個月，以供內部稽核與調查。

(2) 監控以下異常存取行為，並設定 自動警示通知資訊部門：

- 非上班時間登入
- 異地登入（如短時間內出現在不同國家/地區）
- 短時間內多次錯誤登入
- 異常大量下載或存取敏感資料

(3) 當偵測到異常行為時，系統應自動觸發警示，資訊部門應立即進行調查與應對。

10．安全性維護與漏洞修補。

(1) VPN 伺服器、身份驗證系統及其他遠端存取相關設備應定期更新安全性漏洞。

(2) 高風險漏洞應於 30 天內完成修補，避免遭駭客攻擊利用。

(3) 公司員工應定期檢查 筆電、個人設備（BYOD）的作業系統、防毒軟體是否為最新版本，並定期安裝更新。

11．居家辦公資安教育與演練。

(1) 遠端存取人員應接受年度資安培訓，內容包括：

- 遠端存取的資安風險
- VPN 與安全存取的正確使用方式
- 防範社交工程與釣魚攻擊
- 密碼管理與 MFA 的應用

(2) 定期進行資安演練，例如模擬釣魚攻擊或異常登入行為，以提高員工資安意識。

12．本辦法未訂事項，悉依照公司相關規定辦理。

五、使用表單及歸檔：

編 號	表單名稱	開出單位	聯數	資訊單位	財務單位
F-G-10	資訊系統密碼申請表	使用單位	1	1	
F-G-117	系統權限申請單	使用單位	1		1
F-G-163	行動裝置及軟體配備單	資訊單位	1	1	
F-G-42	資訊服務申請單	使用單位			
F-G-164	測試記錄單(UAT 文件)	使用單位			
F-G-122	資訊系統使用切結書	使用單位			

F-G-40	資料備份記錄暨機房日常檢查表	資訊單位			
F-G-140	資訊異常事件紀錄表	資訊單位			
F-G-43	電腦機房進出登記表	資訊單位			
F-G-06	簽呈	資訊單位			
F-G-14	總務請/採購單	資訊單位			
F-G-114	離退流程確認表	使用單位			
F-G-121	軟體盤點清冊	資訊單位	1		