弘憶國際股份有限公司

文件名稱：資通安全管理辦法

文件編號：TW-25

版　　次：6.0

制定日期：2003/12/01

修訂日期：2021/12/20

制定部門：資訊管理處

核　　准	審　　核	制　　定
劉彥輝	林美惠	郭乃智

第 一 條：目的

為維護本公司之永續經營，遵循相關法令規定並保護本公司之資訊資產安全，避免因外在威脅，或內部人員不當之使用與管理，遭致資訊資產不當利用、洩露、竄改、破壞或遺失等風險，以確保資訊資產機密性、完整性及可用性之要求，特訂定資通安全管理辦法（以下簡稱本辦法），作為資通安全管理之遵循依據。本辦法如有未盡事宜，或其他法令另有規定者，從其規定。

第 二 條：範圍

本辦法適用於本公司各單位之全體同仁、委外廠商、第三方人員及所有相關資訊資產安全之管理。

第 三 條：定義

無。

第 四 條：作業流程及說明

一、 資通安全組織及職掌

1.資通安全長：由資訊管理處主管擔任之，負責召開及主持資通安全管理會議，並依會議結果作出裁決交付執行。

2.資通安全小組：由各業務單位主管共同組成，根據資通安全管理事宜提出議案，進行討論和建議，並對決議負責規劃、推動及協調。

3.資通安全執行人員：由資訊部門主管指定之網管人員擔任之，執行資通安全會議中決議事項，進行管制設定。

4.資通安全會議由資通安全長召開及主持，核定各項資訊安全事項、宣達新資訊安全政策、檢討矯正預防措施、資通安全危機事件應變及依本辦法規範相關人員之獎懲事項。

二、 人員管理流程

1.新進人員於報到時，需依照人事部規定填寫到職表單，並簽署保密協定。保密協定涵蓋期間包括從業期間與離職後，均負保密之責任，任何因未遵守本辦法導致之資訊安全意外事件將嚴格懲處，並保留法律追溯權。

2.使用人員應妥善保管個人電腦及資訊檔案，每日下班前應關閉電腦及電源。

3.使用人員應設置使用權限，系統不得任意更改使用權限，以確保系統安全，適時防範操作時之疏失。

4.使用人員對各系統及網路之身分識別及登入密碼應負妥善保護之責任，不得洩漏或借給他人使用，設有特殊權限應用系統，使用人員如需代理人，則需另行申請使用權限及登入密碼。

5.同仁因職務異動而成為非授權使用者時，人事部應主動通知資訊管理部系統

管理人員撤銷該使用者權限應用系統帳號。

6.同仁離職時，須依照「人事管理辦法」之規定執行離職手續，以及依「財產管理辦法」移交保管之資產與電腦設備，最後由資訊管理部撤銷帳號核章，始完成離職程序。

三、 實體及環境安全管理流程

1.電腦設備安全管理

1.1 電腦設備非因故障、更新等維護不得擅自變更、拆裝，亦不得擅自變更電腦作業系統。

1.2 不定期維護保養，確保設備的完整性及可以持續使用。

1.3 相關電腦設備之電源使用應依據製造廠商提供規格設置、並須防止斷電或電力不正常導致的傷害。

1.4 謹慎使用延長線，避免電力無法負荷導致火災等危害安全事情。

1.5 依「財產管理辦法」建立資訊系統有關財產目錄，明列資訊資產的項目、管理人；遇有變更應詳細記載。

1.6 資訊資產實體設備故障應通知資訊管理部人員，並由使用單位依規定填寫「保養修繕申請單」提出請修申請。

1.7 資訊資產實體設備報廢，為避免個資外洩，由資訊單位依如下程序辦理：

(1) 當資訊單位接獲「不動產、廠房及設備異動單」之原因為報廢電腦時，應二周內先行破壞電腦硬碟中之資料，並填寫「資訊設備資安檢核表」，由第二位資訊管理處人員或主管進行確認並於「資訊設備資安檢核表」上簽名負責。

(2) 資訊單位至少應每季彙總「不動產、廠房及設備異動單」，交由財會人員核對每季處分資產無誤後歸檔，始可將該報廢硬碟(或連同主機)進行廢棄物清除。

(3) 報廢資訊資產於等待清除期間，應黏貼報廢標籤，並指定專人專區，妥善保管。

(4) 「資訊設備資安檢核表」正本保存於資訊單位，稽核人員將不定期進行抽查。

2.有關主機機房環境安全與管理，請參閱「系統主機及機房管理辦法」。

四、 軟體使用安全管理流程

1.本公司提供之電腦軟體，未經資訊管理部門主管同意，不得擅自複製或攜出使用。

2.未經資訊管理部門主管同意，不得任意下載軟體或擅自安裝使用，以避免侵犯智慧財產權、誤觸法律或啓動惡意執行檔。

3.本公司嚴禁使用非法軟體。

五、 系統開發及維護安全管理流程

1.自行開發、購入或委外發展之系統，應在開發初始階段或修改系統時，即將資訊安全需求納入考量。

2.系統開發、維護、更新、測試、上線執行及版本異動等作業，應予以安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全，均應保留執行軌跡之記錄，並妥善保存。

六、 通訊安全管理流程

1.網路安全管理

1.1 專人管理網路系統，維持網路系統正常運作，並設置防火牆、資訊安全防護等設備，以防止非法入侵破壞網路。

1.2 防火牆安全設定由資訊管理部提案、設定並執行之：

(1) 所有外部進入管道拒絕

(2) 郵件主機允許外部存取 port:110 (POP3)

(3) 郵件主機允許外部存取 port:25 (SMTP)

(4) 郵件主機允許外部存取 port:80 (WEB/HTTP)

(5) 所有內部對外部存取，不妨礙公司內外網路正常使用狀況下不設限。

1.3 網路系統管理人員應負責製發帳號，提供取得授權人員使用。

1.4 網路系統管理人員應負責監督網路資料使用情形，檢查有無違反資訊安全規定之事件發生。

1.5 內部網路系統管理人員登入主機系統時應保留所有登出入系統紀錄，不得新增、刪除或修改記錄資料檔案，以留有追蹤軌跡。

1.6 內部網路系統、主機系統需保有登出入系統紀錄與異常狀況之紀錄，以利日後追查分析使用。

1.7 非內部網路系統管理人員或未經權責主管人員許可，不得增加、刪除或修改其他網路使用者之檔案。

1.8 人員不得以任何方法竊取他人登入網路的身份識別與網路通行碼。

1.9 人員不得以任何手段蓄意干擾或妨害網路系統的正常運作或以任何儀器設備或軟體工具竊聽網路上的通訊。

1.10 利用網路使用任何電腦資源，均需恪遵被授權的權限，並應主動了解網路安全相關規定，並確實瞭解應負的責任，以免發生違反網路安全情事，遭致懲處。

1.11 不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。

1.12 使用者應安裝病毒偵測軟體，並定期更新病毒資訊；資訊管理處人員亦應以防毒軟體定期掃描檢查伺服器主機，以防止病毒攻擊。

1.13 由資訊管理處同仁定期/不定期發佈資通安全公告或依需要執行教育

訓練。

七、 電子郵件安全管理

1. 郵件主機必須置於實體網路之防火牆內，或郵件主機得於在自備防火牆功能下置於整體防火牆之外，如郵件主機置於防火牆外，則防火牆設定如同網路防火牆之規定，並需安裝郵件防毒功能，每天做病毒定義檔更新動作，以確保病毒定義檔為最新的版本。
2. 非本公司員工不得申請本公司之電子郵件帳號。
3. 郵件信箱密碼需不定期更換，密碼需包含大小寫、符號及數字等。
4. 員工不得利用電子郵件騷擾他人、發送匿名信或偽造他人名義發送電子郵件。
5. 敏感性資料若要以電子郵件傳送，須經加密作業處理。
6. 來路不明的電子郵件，不宜隨意打開，以免啟動惡意執行檔（病毒檔），使網路系統遭到破壞。

八、 資料安全管理流程

1.存取控制

1.1 人員職務須考量適當的權責區隔，各作業系統、應用系統、資料庫系統及網路設備之使用需經過授權，資訊存取權限設定以工作所需最小權限與最少資訊為原則。

1.2 密碼管理原則

(1) ERP、Mail Server、UOF Server 以及 File Server 密碼的安全性及使用須符合至少 8 碼之規定。

(2) 使用者初次登入電腦系統，應立即變更預設密碼。

(3) 密碼須妥善保管，避免他人所知悉。

(4) 各系統應設定連續登入錯誤次數限制，留有錯誤記錄，必要時得停止該帳號之登入或鎖定該帳號。

(5) 每隔三個月須變更密碼。

1.3 系統應啟動記錄存取事件之功能，或視系統之重要性，以書面方式記錄之。

九、 資料存放安全

1. 資訊儲存媒體應依適當之保存規格，存放於安全的環境。
2. 資料之安全、使用管理及保護等事項，由各使用單位負責辦理。
3. 系統安全之管理，請參閱「系統主機及機房管理辦法」。

十、 機密性及敏感性資料管理

1. 機密性及敏感性資料，避免以電子方式傳輸。
2. 機密性及敏感性資料，以電子方式儲存時，應存於安全性及穩定性較高之

主機及週邊設備。

3. 日常經辦機密性或敏感性之資料(含契約、表報、影印資料、磁片、光碟片等)下班後應妥善收存。
4. 廢棄之手寫或影印文件、表報等資料應隨即銷毀處理，不得任意棄置。
5. 儲存機密性及敏感性資料的電腦媒體,當不再繼續使用時,應予以銷毀(鐃毀、碎紙處理、將資料從媒體中完全清除等)。
6. 資料檔案的重要性及保存期限，由各使用單位負責辦理。

十一、委外作業安全管理流程

1.資訊業務委外時，應於事前審慎評估可能的潛在安全風險，與廠商簽定適當的資訊安全協定及規範安全管理責任，納入契約條款中。

2.委外作業承包之工作人員，如需進入相關系統作業，應協同資訊管理處人員進行相關作業，並留下適當的作業軌跡記錄。

3.系統委外開發，承包商應提供系統建置（含規格及軟體程式）之完整、詳細說明文件。

4.資訊支援或維護服務須由資訊管理處人員陪同或授權。

5.資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。

6.對委請資訊安全顧問，或負責資訊安全之人員，各單位及人員應予必要的協助及支援。

十二、營運持續運作管理流程

1.一般資訊安全處理程序

個人電腦當機及個人資訊系統維護或其他更新服務、業務資料處理錯誤作業導致系統資料不正確的修正，需提出「資訊服務需求單」至資訊管理部。

2.重大資訊安全處理程序

1.1 包含系統當機及中斷服務、系統資訊存取異常流失、業務資料呈現不完整或資料不正確、及機密性及敏感性資料外洩狀況。

1.2 應在最短的時間內，確認已回復正常作業的系統及安全控制系統是否完整及正確。

1.3 發生重大資安事件時，資通安全長得臨時召開資訊安全會議，對事件詳加檢討評估，找出原因及檢討改正，並向總經理報告緊急處理情形。

1.4 應限定只有被授權的人員，才可使用已回復正常作業的系統及資料。

1.5 緊急處理的各項行動，應予詳細記載，以備日後查考。

1.6 重大資訊安全處理機制及執行細則，參照「緊急應變計劃」辦理。

3.資訊安全教育訓練

1.1 應對新進同仁辦理資訊安全管理課程訓練，提升同仁危機意識與資訊

安全觀念。課程中必須給予完整智慧財產之軟體著作權與版權觀念，嚴禁非法使用軟體，而自由軟體(freeware)與共享軟體(shareware)之安裝使用亦必須詳細瞭解其版權宣告並遵守。

1.2 資訊管理人員應適當參與外部教育訓練課程、與外部的資訊安全專家或顧問加強協調聯繫，相互合作、分享經驗，以評估本公司可能面臨的資訊安全威脅，據以研擬及推動資訊安全實務措施。

十三、罰則

相關資通安全事項應依本辦法之規定辦理，違反本辦法時，除督促改善外，應視情節輕重依契約內容、本公司「員工績效考核辦法」與員工手冊，採行法律程序或提報考核，進行懲處。

第五條：相關文件

1. TW-05 人事管理辦法。
2. TW-08 員工績效考核辦法。
3. TW-26 緊急應變計畫。
4. TW-74 系統主機及機房管理辦法。

第六條：附件/表單

1.DC-01 資訊服務需求單。

2.DC-04 資訊設備資安檢核表。

3.DF-04 不動產、廠房及設備異動單。

4.DF-05 保養修繕申請單。