

奇鈦科技股份有限公司

資通安全辦法

第一條 目的

為確保電子作業相關設備、資訊系統及其資料之安全、加強作業管制、防範災變為害，以維護整體資訊業務正常運作及機密資料的隱密性。

第二條 適用範圍

- 一、電腦設備管理與安全維護。
- 二、作業管制與資訊機密維護。
- 三、備援作業與管理。
- 四、災變處理與作業。

第三條 權責

一、資訊處理單位(IT)：

- (一) 維持電腦正常運作、保護網路安全、確保系統運作、維持網頁更新、Mail Server 管理維護。
- (二) 確保本公司管理相關資訊系統，不得安裝共享軟體及來歷不明之軟體，以防招致毒駭。

二、各部門：

- (一) 正常使用電腦，不使用來歷不明的檔案、軟體。
- (二) 依規定使用電子郵件系統，不任意發送傳播與公司無關之電子郵件、不明檔案。
- (三) 不任意拷貝檔案，不任意下載檔案，不散播有潛在危險之檔案。
- (四) 確實執行資料備份，妥善保存備份資料。

第四條 安全維護

一、機房及相關設備：

- (一) 電腦機房之設置應避免鄰近危險地點（如高壓電箱等），並考

慮結構上之安全性及水患之可能性。

- (二) 機房外圍應有防範外人侵入之隔離設施，機房之出入口必須可以上鎖。
- (三) 電腦機房應有獨立配置之電力設備、專用之空調設備、各項設備並應定期檢視維修。
- (四) 電腦機房由 IT 負責管理，並維護機房作業之安全。
- (五) 連線作業之各項設備及線路、各種電器設備之線路應定期檢視維修。
- (六) 機房嚴禁使用電熱器、不得攜入食品、飲料、收音機、電視機及含有磁性或靜電之物體；並應儘量減少易燃物品之儲存。
- (七) 作業中如遇緊急事故應儘速關機結束作業並切掉電源，以防災害擴大。
- (八) 主機房內不得使用自動噴水滅火器。
- (九) 電源設備換裝，應請電腦公司鑑定容量後再行使用。

二、電腦設備：

- (一) 各項電腦設備應依維護合約，要求電腦公司進行維護作業。
- (二) IT 應主動與管委會或電力公司連繫，要求預先通知停電時間。對已具備接電力設備之主機系統，應加裝穩壓器；對未具備接電力設備者，則加裝不斷電設備，俾防止停電，導致作業失常。
- (三) 主機開、關機應依操作手冊規定程序，由主機操作人員或經核准之人員負責，其他人員不得擅自操作。
- (四) 機器故障時，應立即要求電腦公司人員維修，如屬重大故障，兩天尚無法修護，可能延誤正常作業進度時，應即向部門主管報備，並依維護合約要求電腦公司提供支援作業。
- (五) 當業務需求或人員異動離職應填寫【資產異動單】，所使用之電腦需要異動或整理時，應經 IT 清點及核對整理後，再移交給相關人員使用。
- (六) 電腦之零件如因損壞或升級淘汰後，原零件須送交 IT 確認、資料備份及銷毀，再依其堪用程度報修、庫存或資源回收。

三、信箱、網頁維護：

- (一) 公司專用電子郵件信箱由 IT 負責管理，公司網站則由行銷單位負責管理。
- (二) 網站委外管理，其網頁內容，會在不定期的時間，依行銷單位提出之需求，經總經理認可後指派專人修改其內容，或連絡廠商協助增刪相關內容。

四、系統程式及相關文書：

- (一) 自行或委外開發設計之系統應先填寫【電腦作業需求單】經 IT 部門評估接受，進行開發作業；若為套裝軟體之系統變更，也應提出【電腦作業需求單】經 IT 部門評估接受委外進行變更。
- (二) 規劃系統設計程式時，應將作業安全因素，列入考慮。
- (三) 程式設計管理之標的，包括：程式指令、系統流程圖、程式流程圖、輸出入資料說明、測試報告、變更報告、程式操作文書等，程式設計員撰寫後，均應交 IT 人員保管。
- (四) 各系統執行人員應配合系統管理員，應隨時或定期檢視磁碟內所有應用程式之名稱及建立時間，如發現異常情事，應即列印清單，追查來源後簽報議處。
- (五) 電子作業相關文書，包括各項作業系統說明文書（如系統說明、操作規範、登錄及標符規範等）、電腦設備使用說明、操作系統說明、視訊教材及其他有關參考書籍等，均由相關人員保管並列入交接。
- (六) 開發應用系統時，應加強審核之功能，將各欄位不合邏輯或錯誤之資料，完全剔除，以確保資料之正確性。

五、帳號密碼管理維護：

- (一) 公司網路設備登入之帳號及密碼、員工之 E-mail 帳號及密碼、員工登入 ERP 系統之帳號及密碼之申請必須填寫【電腦網路作業申請/取消單】，經核准後由 IT 建置。並登入【電腦網路資料一覽表】統一管理。
- (二) 當有員工離職，該員工之 E-mail、ERP 帳號、密碼須填寫【電

腦網路作業申請/取消單】進行取消作業、ERP 各系統內權限由 IT 根據該員工【移交清冊】予以取消。

六、原始資料與輸出入管制：

- (一) 使用終端機作登錄及查詢時先輸入識別碼，經電腦核對無誤後，方能進入系統作業，重要或具機密性資料，並應加設資料存取控制。識別碼嚴禁告訴他人，如發現有被他人探知情事，應即報告上級主管，適時更換新碼。
- (二) 單位主管依每位員工實務需求，賦予使用者不同授權度之識別碼及通行碼(指帳號及密碼)，以保護檔案資料之安全與機密。

七、資訊檔案管理：

- (一) 正式作業產出之資料，如發現有錯誤或異常情況，應立即查明更正，其屬程式錯誤應由資訊單位更正；其餘應由各單位依正常的錯誤處理程序處理，並留下異動單據以備查核。
- (二) 磁片、磁帶應直立放置，不可置放地上，切勿加壓於磁片或磁帶捲盤邊緣。媒體儲存環境應注意溫濕度控制。
- (三) 磁碟、磁帶檔案之借用應事先開具借用單，經檔案管理人員允許後，始可攜出。

八、人員管理：

- (一) 資料處理應予適當分工，資料登錄、系統執行、機器操作、作業管制各項作業，應儘量分由不同人員負責。
- (二) 公司員工應填具【保密合約暨資訊系統使用切結書】，約定所使用的電腦系統內僅能使用合法軟體，另本同意書也包括智財權協議、軟硬體與網路機密資料等協議，如有使用違反本同意書內容則依據本公司『工作規則』及『員工獎懲辦法』予以處分，若損害本公司權益者，應負全部法律責任。
- (三) 運用主機資料作業之人員，應填具保密切結書，約定不得於在職期間或離職後，洩漏其所知悉之機密或私自蒐集藏匿機密資料。
- (四) 前項人員離職時，應辦妥業務交代填寫【移交清冊】，收回各

種安全有關之物品文件，對遭開除或情緒不滿人員，應特別注意，避免其蓄意破壞之行為。

九、安全管制：

(一) 門禁安全

- 1、主機房應設置門禁之管制並設置【機房進出登記表】。
- 2、嚴禁攜帶外人進入機房內參觀。

(二) 主機房進出管制

除下列人員外，不得進入主機房：

- 1、各部門主機管理員、系統維護人員。
- 2、指定程式設計、測試人員。
- 3、經核定之電腦公司負責機器裝備、維修或軟體維護人員。
- 4、其他經核可之人員。

第五條 備援及災變回復

一、災變定義：

本要點所稱之災變，係指自然災害、人為過失及其他意外事故，導致電子作業人力、資料及設備之損毀，作業因而中斷，預期三天內無法正常作業之情況。所稱災變回復，係指災變發生時，短期間內，回復主要作業及處理能力之行動。

二、ERP Server 及每日因工作之需而會更新之檔案：

- (一) 於 ERP Server 安裝備份軟體，在凌晨時間(約 2:00)自動壓縮檔案備份於檔案伺服器之硬碟中。
- (二) 其他檔案：
設定檔案伺服器(File Server)每天定時自動備份。

三、資料檔案之備援：

(一) 登錄資料媒體

- 1、原始資料經登錄抄錄之媒體資料，除一套提供作業外，應複製一套儲存備用。
- 2、登錄中之原始資料，每日下班應妥適收存，以確保資料安全。

(二) 運轉資料媒體

- 1、各作業系統應於處理作業時，將主檔資料複製一套儲存備用。其中重要檔案於作業完成後，再行複製一套依限妥為保管。
- 2、採線上異動主檔者(ex：ERP)，均應於運轉過程中，視需要將主檔複製一套備援。
- 3、各作業系統於建檔完成後，應將經核定之重要異動資料複製一套儲存備用。

(三) 備援媒體資料之維護

- 1、備援媒體資料之儲存場所，應與主機房分屬不同之建築物，並且登錄在【資料備份作業記錄表】。
- 2、備援媒體庫房應備有專用消防設備，平時除注意環境安全、維護內部整潔及溫濕度控制。
- 3、備援媒體檔案，凡屬長期保留者，應每年定期運轉試讀或抄錄乙次，以確保品質。

四、系統程式之備援：

(一) 系統程式及作業文書

- 1、系統程式及各項作業文書均應複製一套分開保存，並妥善維護。
- 2、程式修改或翻新時，舊版本程式應繼續保留，惟當使用處理之主機設備汰換，檔案轉換完成後，可將失效之程式刪除。

(二) 電腦操作系統

- 1、電腦操作系統及有關係統程式，應依時序保存較新之二版。
- 2、要求電腦廠商保存該設備曾使用之各操作系統版本，以為備援。

五、應變措施：

(一) 災變發生時應變措施

- 1、立即通告全體同仁發生災變，必要時並即與警察、消防、醫院等單位聯絡，採取適當之處理。
- 2、迅速依序關機，切掉電源，啟用充電式照明設備。

- 3、重要檔案及文書，先行撤離現場。
- 4、在災情尚未波及機房時，以防水膠布罩住機器，以防消防水劑破壞機器。
- 5、使用所有救災設備，設法控制災害繼續擴大。
- 6、如有危及生命安全顧慮時，人員應即撤離疏散。
- 7、防止無關人員趁機進入機房。

(二) 平時演練

- 1、為確保具有應付災變之能力，每半應模擬災變回復作業並登錄【災害復原計劃測試報告表】。
- 2、依工作計畫進度實施災變回復模擬作業後，應即將作業情形與檢討事項，向主管報備。

六、災變回復作業：

- (一) 災變發生後，應迅即組成災變回復專案小組，迅速處理搶救事宜，並研訂災變回復計畫，排訂日程據以執行，各項作業如不能正常處理時應按重要性次序，優先處理。其對災變發生經過、設備資料損毀情形等應併同災變回復計畫報總經理核備。
- (二) 檔案資料損毀時，應即以備援檔案回復作業，程式或操作系統遭破壞時，並得請求維護單位協助回復作業。
- (三) 登錄設備損毀經洽請支援後仍有困難時，得報請核准外包。
- (四) 主要運轉設備損毀，除全力搶修以回復正常作業能力外，如預期一週內仍無法繼續作業時，應即洽支援設備單位協助作業。
- (五) 回復作業過程，應詳留紀錄以備查考。以支援設備執行作業時，有關資料媒體檔案之備援作業，仍應依正常作業時之規定辦理。

七、災變善後檢討：

災變回復專案小組，應就災變發生之原因、應變措施、回復作業、各單位配合情形等逐項檢討，研擬提改進意見並簽報。

第六條 本辦法呈總經理通過後公佈實施，修正時亦同。