天品聯合企業股份有限公司

電腦資訊安全管理辦法

1.目的

為確保公司網路及資訊保護安全，以利公司整合整體網路資源，發揮企業電腦化之最大效能，及為強化資訊安全管理，督促改善資訊安全防護，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，特訂定本辦法。

2.適用範圍

本公司(含子公司)全體員工皆適用。

3.電腦使用規範

3.1 登入密碼管理

3.1.1 使用者登入帳號及密碼對每一合法使用者是絕對唯一。

3.1.2 登入密碼至少由四位字母與數字符號構成。

3.1.3 登入密碼需定期更改，以提高安全性。

3.1.4 嘗試登入數次失敗後，暫停使用者帳號，並將失敗登入紀錄於登錄檔中，以便日後查詢。

3.2 軟體使用

3.2.1 新進同仁須簽屬禁止使用非法軟體同意書。

3.2.2 禁止使用任何非法或未經資訊部授權之軟體。

3.2.3 禁止任意移除資訊部所安裝之軟體。

3.2.4 經由網際網路下載之軟體，須由各同仁以防毒軟體測試、掃描，並確認安全無誤後方可安裝或執行。

3.2.5 如同仁自行安裝使用非法軟體，同仁將需自行負責相關法律責任，本公司(含子公司)將不負任何法律責任。

3.2.6 防火牆對網路病毒或木馬攻擊無法做有效防禦，因此所有同仁不要點選或進入任何不明網頁、郵件，以免遭到網路病毒或木馬攻擊。

3.2.7 使用者如偵測到病毒入侵，或有任何中毒跡象，應馬上通知資訊部，避免病毒的擴散。

3.2.8 如有機器遭受病毒感染，應立即拔除網路線，直到資訊部確認病毒已移除，才可重新連線。

3.3 電子郵件

3.3.1 對於來路不明的電子郵件(垃圾郵件)，應有垃圾郵件處理及信件附檔掃毒機制，同仁切勿隨意打開郵件而啓動惡意執行檔，使公司網路系統遭到破壞。

3.3.2 公司郵件帳號乃提供同仁公務所需之用，切勿使用公司郵件進行與公務無關且違法之情事，資訊部同時進行必要之郵件監控。

3.4 OA設備

3.4.1 OA設備範圍：

3.4.1.1 任何連線至公司網路之個人電腦、筆記型電腦。

3.4.1.2 週邊產品：螢幕、印表機、光碟機、USB隨身碟…等，資訊周邊相關產品。

3.4.1.3 耗材：印表機碳粉、墨水、空白燒錄片…等，耗用性質產品。

3.4.1.4 非上述類型，但經資訊部判斷爲資訊產品皆屬之。

3.4.2 非公司電腦財產（也就是沒有 OA 財編）的筆記型電腦（NoteBook），除廠商筆記型電腦（NoteBook）外或因業務需求等，同仁不得攜帶私人筆記型電腦

（NoteBook）進入公司。

3.4.3 爲確保公司資料之安全,除業務需求外,嚴禁使用私人之筆記型電腦(NoteBook)來處理公司業務，應使用公司所配發之個人電腦或筆記型電腦（NoteBook）來辦公。

3.5 硬體及系統軟體之購置、使用及維護

3.5.1 請購

由需求單位向資訊部提出需求，並經該部門相關主管簽核完成後，由資訊部進行需求評估，並向廠商取得報價，填寫請購單會簽需求單位後，交由採購部門進入採購流程。

3.5.2 驗收

軟硬體之購置須經資訊部會同需求單位進行測試及驗收程序。

3.5.3 軟體使用

3.5.3.1 軟體統一集中由資訊部管理。

3.5.3.2 員工欲借用軟體時，可逕向資訊部軟體負責人員登記借用。唯借用之軟體，僅能在公司內之電腦上使用，且須於三個工作日歸還，若確有需要延長使用時間，則需先向資訊部申請核准後，再行使用。

3.5.3.3 借用或歸還軟體，須直接洽詢資訊部軟體負責人，不得私自轉借。

3.5.3.4 電腦軟體之使用，應以工作上之需要及研究爲目的。若被借用之軟體，涉及非法拷貝、販售、或有違智慧財產權之法律規定，則該軟體借用者須自行負責賠償及所有法律責任。

3.5.4 硬體使用

3.5.4.1 所有電腦設備都要有其對應之保管人，每一台 PC 都要有財產編號，並於 ERP 系統中記錄該設備之保管人及相關資料，供管理之用。設備保管人需確保其使用 PC 及其週邊設備之完整性，並不得任意變動相關配備。

3.5.4.2 公用設備如伺服器及印表機…等，由資訊部統一保管。

3.5.4.3 保管之硬體設備若遺失,或不正常使用導致毀損,則須報請資訊部處理。資訊部視實際狀況決定賠償方式。（正常使用之毀損不在此限）

3.5.5 維護

3.5.5.1 資訊部負責與軟硬體之維護供應商簽訂定期維護合約。

3.5.5.2 更新系統軟體須經適當核准，有關之設定文件須適當存檔與保管。

3.5.6 報廢/出售

3.5.6.1 不堪使用或無法使用之電腦設備，需將硬碟完全消磁或銷毀後再進行設備報廢或出售作業。

3.6 網際網路使用管理

3.6.1 E-mail收發、WWW、FTP 及 DNS 等網路服務之相關規範。

公司之 Internet 服務主要是提供 WWW 網站查詢服務，以及同仁之 E-mail 信箱及FTP 檔案下載服務。同仁切勿進入任何不明網站或下載安裝任何不明元件，以免誤植病毒、木馬等具破壞性之惡意軟體，並且嚴禁瀏覽色情或任何與工作業務無關之網站。Intranet 部分則是提供內部公文交換以及其他同仁訊息流通。其中涉及機密及個人資料者，一律設定密碼認證控管。同時爲避免造成內部網路之安全漏洞。

3.6.2 即時傳訊軟體（MSN、Skype、Line 等）之使用

上班時間應從事公司業務相關事務，即時傳訊軟體（簡稱 IM）也應使用於公務連絡。同仁禁止任意接收或傳送檔案、網址、圖片，以免增加中毒風險或甚至洩漏公司機密。若因 IM 而影響工作效率，公司有權禁止同仁 IM 之使用。

3.6.3 防毒軟體之使用及規劃。

配合公司整體網路規劃，針對電腦病毒爲提供快速且通用有效的因應措施，公司提供 Microsoft Security Essentials 為電腦提供即時保護，免受病毒、間諜軟體和其他惡意軟體的危害。

4.機房管理：

4.1 電腦機房設有門禁管制，非資訊部人員或未取得核准人員不得進入。

4.2 非資訊部同仁需進入機房，請用資訊需求單向資訊部主管提出申請核准。

4.3 人員進出請一律在「機房進出入管制表」記載進出人員及時間並註明原由。

4.4 電腦機房管理人員需於每上班日至機房依檢查表所列舉項目逐一檢查，包含溫度、空調、電力及UPS，並在「資訊機房曰檢查表」登錄。

4.5 網路管理人員需在每上班日檢查防火牆和防入侵設備，查看有無異常的資料，如有請立即通報資訊主管，並記錄在「資訊機房曰檢查表」並作定期追蹤。

4.6 公司對外系統如 Mail Server、VPN Server、WWW Server 會做定期檢查更新版本。

5.資料備份還原

5.1 各資訊系統應定期執行系統、資料及記錄之備份工作。

5.2 資料庫依作業需求可採用曰備份機制或自動循環的備份機制。

5.3 應定期進行備份媒體復原測試，每半年應進行一次還原測試工作。

5.4 復原測試得選定任一系統或資料庫進行還原，測試備份系統及復原程序的有效性。相關執行成果須紀錄於「資訊系統復原測試報告單」

5.5 重要資訊系統欲辦理備份資料還原時，應提出「資訊需求單」，經單位主管簽核，並由資訊部做資料回復作業。

6.緊急應變

6.1 天然災害應變：

6.1.1 火災應變：

6.1.1.1 電腦機房裝置有消防系統，機房管理員應熟悉機房內各項安全設備〈如緊急電源、消防設備〉之使用方法，有關消防設備之使用由管理部定期舉辦相關教育訓練，操作人員都要熟悉操作。

6.1.1.2 機房管理員應定期檢測機房內消防設備之使用期限,有逾期者立即更換。

6.1.1.3 遇火災狀況時，電腦機房內易燃物品及相關設備、媒體應即時移離，並向主管報告請求支援。

6.1.1.4 系統負責人員研判故障類型，並先行設法排除，如無法解決時，應詳細記錄當時狀況及顯示之訊息後，立即就故障問題通知相關人員前來維修。

6.1.1.5 如主機硬體嚴重受損時，應與維修人員連絡，並詳述損壞情形，以減少維修人員修復之時間，並於最短時間內回復硬體設備，如短時間內無法回復硬體設備時，應協調商借主機暫時使用。

6.1.2 震災應變：

6.1.2.1 遇有強烈地震發生，應大聲的提醒週遭人員保護自身安全爲首務，如狀況稍有紓解時即進行緊急關機。

6.1.2.2 系統負責人員研判故障類型，並先行設法排除，如無法解決時，應詳細記錄當時狀況及顯示之訊息後，立即就故障問題通知相關人員前來維修。

6.1.2.3 如主機硬體嚴重受損時，應與維修人員連絡，並詳述損壞情形，以減少維修人員修復之時間，並於最短時間內回復硬體設備，如短時間內無法回

復硬體設備時，應協調商借主機暫時使用。

6.2 人爲破壞應變

6.2.1 人員闖入

6.2.1.1 機房設有門禁管制，如遇有陌生人員擅自闖入機房，應即刻予以查問其來意，並引導至正確場所洽辦。

6.2.1.2 如有來意不善人員闖入，立刻轉請駐衛保全派員前來處理，並通報上級主管。

6.3網路入侵

6.3.1 主機重要資料應即時備份，如發現有駭客侵入，應立即報告資訊部單位主管並將該主機先行隔離，隨即展開執行檢查與回復作業；事後應即時檢討改進並將處理情況依規定逐級呈報。

6.3.2 電腦機房應指派網路安全監控人員，運用相關網路稽核軟體不定期監控網路使用概況，遇有疑似駭客入侵，應立即報告資訊部單位主管，得運用有關軟體予以追綜、查察，必要時得以予以斷訊等。

6.4 電腦病毒

6.4.1 如有因病毒事件造成網路故障，應立即運用電腦機房所購置之防毒軟體進行解除病毒處理，並設法排除網路障礙使恢復正常。

6.4.2 如無法自行排除,應立即與合約廠商連繫尋求支援。

6.5應變小組

6.5.1 因應緊急事故的處理，需成立資訊應變小組.組長爲資訊部主管，組員爲資訊部同仁，並設置指揮官一名由資訊部上一級主管擔任。

7.使用表單

7.1 軟體切結書（FM-247）

7.2 資訊帳號及權限申請表（FM-248）

7.3 資訊系統復原測試報告單（FM-287A）

7.4 機房進出入管制表（FM-288-A）

7.5 資訊機房日檢查表