滿心企業股份有限公司

資訊通訊安全管理辦法

壹、目的

為確保本公司資訊業務之永續運作，強化資訊通訊安全管理，建立安全及可信賴之電子化環境，以確保電腦資料、資訊系統、資訊設備及網路設備之安全。

貳、範圍

凡本公司庶務用個人電腦與資訊系統、檔案，分享系統等直接網路連線之個人電腦、伺服主機、網路設備以及運用上述設備、系統的公司員工均適用本管理辦法。

參、資訊安全政策

1.確保資訊資產之機密性、完整性。

2.確保依據部門職能規範資料存取。

3.確保資訊系統之持續運作。

4.防止未經授權修改或使用資料與系統。

5.定期執行資安稽核作業，確保資訊安全落實執行。

6.加入台灣電腦網路危機處理暨協調中心，隨時取得資安事件資訊防範之，及如發生重大資安事件隨時回報。

肆、通訊與操作管理

一、組織架構

(1)本公司為統籌資訊業務之整體規劃、評估、督導、協調、推動以及安全等事項，特設電腦室。

(2)電腦室設置主管 1 人，資訊人員 2 人 ，共 3 人。

二、組織任務

(1)負責規劃、執行與控管全公司資訊安全工作，辦理風險評估、系統安全控管措施。

(2)監督資訊安全管理事項，進行資訊安全政策符合性檢查。

(3)資訊機密維護及稽核資訊設備、網路的使用管理事項。

(4)公司內因業務需要開放給外部單位存取資訊之風險評估與存取權限之嚴格控管。

伍、人員安全與管理

一、工作說明及資源分配安全

(1)對於人員之進用、調派、離職或退休，進行適當之安全評估。

(2)對於可存取機密性、敏感性資訊或系統之員工以及賦予系統存取特別權限之員工有妥適分工，分散權責。

二、使用者訓練

(1)員工必須瞭解公司之資訊安全政策。

(2)依員工職務層級進行適當的資訊安全教育訓練。

(3)隨時公告資訊安全相關訊息。

(4)不定期派員參與外界舉辦的相關訓練、研討會、產品展示會。

三、安全及失效事件反映及處理

(1)訂定規範員工的資訊安全作業程序與權責(含保管使用設備及作業須知)。

(2)訂定有關資訊安全狀況授權處理層級。

陸、實體及環境安全管理

一、安全區域

(1)電腦機房，對於進出人員必須由管理人員作必要之限制及監督其活動。

(2)訂定電腦機房安全管理規定(如禁止抽煙及飲用食物等)。

(3)機密性電腦主機/伺服器必須由專人管理。

二、設備安全

(1)設備之維護必須由授權之維護人員執行。

(2)訂定設備安全管理規定(如電源之供應及備援電源等)。

(3)需特別保護之設備應該規劃與一般設備作適當區隔。

(4)資訊設備之放置與擺設必須作安全上之考量。

(5)資訊設備之放置應該檢視及評估火、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害的可能性。

(6)各項安全設備必須定期檢查，員工必須施予適當的安全設備使用訓練。

三、一般控制措施

(1)攜帶型的電腦設備訂有嚴謹的保護措施(如設密碼保護、檔案加密、專人看管)並落實執行。

(2)處理敏感性資料的電腦，不使用時應加以關機、登出、設定螢幕密碼或是以其他控制措施進行保護。

柒、通訊與操作管理

一、作業程序與責任

(1)訂定各項重要資訊處理設備的安全作業程序。

(2)訂定資訊安全事件通報程序並確實依規定通報。

(3)重要資訊處理設備，應適切訂定操作程序及管理責任。

(4)建立重要系統變更之程序記錄。

(5)系統開發及正式作業必須區隔在不同的系統環境下處理。

(6)與業者簽訂資訊安全處理協定時，應賦與相關的安全維護責任，並納入契約條款。

(7)資訊系統之使用、資料建檔、系統操作、網路管理、系統發展維護、變更管理、安全管理等工作原則上必須權分由不同的人員執行。

(8)對安全要求高的資訊業務，必須將資訊安全管理及執行的責任分散。

(9)資訊安全事件處理的過程均應留有完整記錄，以利追蹤檢討。

(10)資訊安全緊急應變處理程序，包含定期演練及測試。

(11)訂定電腦當機及服務中斷後之緊急處理程序。

二、惡意軟體防範

(1)定期對電腦系統及資料儲存媒體進行病毒以及惡意程式掃瞄。

(2)伺服器與個人電腦全面使用防毒軟體並即時更新病毒碼。

(3)應即時公告有關電腦病毒的最新資訊。

(4)經常性宣導對於外來及內容不確定的檔案或 E-mail 在開啟使用前，要先作電腦病毒掃瞄。

(5)軟體授權規定：禁止使用未取得授權的軟體。

三、日常事務處理

(1)對重要的資料及軟體，應定期作備份處理。

(2)定期檢測備份資料，以確保備份資料之可用性。

(3)備份資料原則上採用異地存放，存放於符合安全標準之場所。

(4)重要資料的備份應保留(每日備份)。

四、網路管理

(1)適切的使用網路防火牆機制，以防禦資訊系統安全。

(2)對網路運作環境之安全漏洞，原則上應定期進行檢測。

(3)隨時公告有關電腦網路安全之事項。

(4)定期檢討電腦網路安全控管事項之執行。

五、儲存媒體的處理與安全

(1)儲存媒體依保存規格要求，存放在安全的環境。

(2)對於敏感性資訊之傳送，應採取資料加密等保護措施。

(3)存放在可攜式媒體內之敏感性資料，需使用加解密或其他保護措施。

(4)對於內含機密性或敏感性資料的媒體報廢，應指定專人處理。

(5)儲存媒體之報廢，必須協同部門主管進行資料檢核確認後，並簽報上級主管核可後，方可進行實體報廢作業。

六、資訊與軟體間交換

(1)重要系統文件發送對象，必須經由系統負責人的授權。

(2)重要系統文件的存取，應結合帳號密碼賦予適當的存取權限，以保護系統文件的安全。

(3)對於重要資料文件及軟體之更替使用，需詳細記載版本、數量及其他詳細相關資訊文件。

(4)採行電子交換之資料交換(EDI)，須視資料之安全等級採行帳號密碼管制、電子資料加密或電子簽章認證等保護措施。

七、個人電子信箱使用原則

(1)有鑒於電子郵件的濫發可能衍生的相關問題（如散佈不實謠言、轉寄色情圖片或文字、轉寄他人文章、廣告郵件、洩漏企業營業秘密等），故個人電子信箱的使用應該加以規範與宣導。

(2)電子郵件(e-mail)的使用原則

I.電子郵件的使用如牽涉散佈不實謠言、轉寄色情圖片或文字、轉寄他人文章、不實內容的電子郵件毀謗名譽、廣告郵件、涉嫌洩漏機密等，將由員工個人負起相關的法律責任。

II.使用本公司的電子郵件，須遵守行政倫理、智慧財產權、國家機密保護辦法、個人資料保護法等等相關規定。

III.員工接收電子郵件後，原則上應立即自郵件伺服器中刪除該郵件，以避免過度佔用郵件伺服器空間。

(3)電子信箱之申請及取消

I.員工到職時，應填寫[系統權限申請表]，經單位主管簽核後，資訊單位開放其系統權限時，同時賦予個人電子信箱。

II.員工離職後，資訊單位取消系統使用權後，其電子信箱一併刪除或暫作停用。

捌、存取控制

一、存取控制之營運要求

(1)訂定開放給外部單位作資料存取之程序。

(2)開放給維護廠商作系統維護或資料存取，應於書面文件(如維護合約)中包含雙方權利義務及違約處分方式。

(3)嚴格控管因業務需要開放給外部單位之存取權限(含上下游業者、維護廠商、委外承包商、臨僱人員等)，並應該經過風險評估後才開放。

(4)訂定資訊存取控制之政策及相關說明文件，並定期向員工說明。

二、使用者存取管理

(1)使用者存取權限的檢視，應訂定管制機制，避免被非相關人員知曉。

(2)對於使用者異動申請資料，隨時更新並保留相關文件資料。

I.嚴密保存使用者帳號密碼之申請資料。

II.定期檢查並刪除重覆或閒置的使用者帳號。

III.對於忘記密碼之處理，應有嚴格的身份確認程序。

(3)對所有員工宣導，避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）當做密碼，並不得借用他人帳號密碼使用。

(4)密碼的使用須依規定的期限，進行密碼變更設定。

(5)密碼設定應規範至少六碼(含)以上。

三、網路存取控制措施

(1)依據個別應用系統的安全需求，制定安全等級或分類。

(2)依據網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式。

(3)資訊系統與網路服務，原則上儘量避免使用共同帳號。

(4)網路服務須建立完整的使用授權程序。

(5)依環境或業務需要，於網路防火牆作適當之設定。

(6)依業務性質或任務分配來建置邏輯性網域的存取權限機制(如虛擬私有網路 VPN)。

(7)設置專櫃連線的來源位址與目的位址網路路由之控管措施。

四、作業系統存取控制措施

(1)對於異常的登入程序，應保留紀錄(LOG FILE)，並有專人定期檢視。

(2)使用者均應有專屬的識別碼可供追蹤。

(3)系統軟體安裝完畢後，須立即更新廠商所預設之密碼。

五、應用系統存取控制措施

(1)應用系統的密碼檔，原則上應以亂數加密法則加密後再存入檔案。

(2)對風險性高的應用程式或資料庫系統必須嚴格限制其連線作業需求。

(3)機密性資料的處理必須於獨立或專屬的電腦作業環境中執行。

(4)妥善保存應用系統的各種更新版本。

六、監控系統存取控制措施

(1)例外事件、系統存取異常及資訊安全事件必須建立紀錄作必要處置。

(2)事件之記錄內容儘可能包括使用者識別碼、電腦的識別資料或其網址、

登入登出系統之日期時間及事件描述等事項。

(3)定期查核系統存取權限的帳號使用及配置情形。

(4)敏感性資料的存取情形，原則上必須留有紀錄備查。

(5)指定專人管理應用程式原始碼、資料庫及執行檔的存取與保管。

七、行動式電腦作業

(1)可攜式電腦使用，由資訊單位列冊管理，使用者應負保管實體以及管理軟體資料安全的責任。

玖、系統開發與維護

一、系統之安全要求

(1)伺服器更新作業系統應依正當的授權程序辦理，並確實評估檢視更新作業妥適與否，以確保更正作業未破壞系統原有的安控措施。

(2)系統有重大變更前，應主動公告異動的範圍、時間以及可能的影響。

二、應用系統之安全

(1)應用系統變更後，其相關控管措施與程序應檢查以確保仍然有效。

(2)應用系統在規劃時，應將安全需求納入考量。

(3)建立應用程式執行碼的更新紀錄。

(4)版本更新須保留舊版軟體及系統文件。

(5)應用程式執行碼更新作業，應限定只能由授權的管理人員才可執行。

三、密碼控制措施

對高敏感性的資料在傳輸或儲存過程中，應使用加密技術。

四、系統檔案之安全

系統檔案安全控管方式，可依實際狀況訂定採用系統自動控管或者人工控管兩種方式來處理。

五、開發資訊系統的安全

(1)委外開發合約中，應對著作權之歸屬訂有規範內容。

(2)開發、測試與正式作業，應區隔使用不同的伺服主機。

(3)與廠商訂約開發資訊系統時，應簽訂履行條款與相關罰則。

六、訂定軟體使用規範

(1)使用原廠購買之版權軟體，不安裝非法或來源不明之軟體。

(2)定期進行套裝軟體之 Servic pack 的更新評估及更新作業。

拾、內部稽查，法規及其他

一、安全政策與技術符合性之考量

(1)相關措施必須留下相關記錄檔案供內部稽核。

(2)定期審閱系統內與資訊安全相關的記錄檔案(系統 Log)。

(3)定期審閱資訊安全相關的記錄檔案(如工作日誌、備份記錄）。

(4)應有專人負責管理與資訊安全相關的記錄檔案。

(5)不定期檢查所有個人電腦內使用之軟體。

(6)訂定軟體使用記錄與資料的儲存、處理及報廢的規則。

(7)建置可保留資訊安全相關的記錄檔案之系統，並且足以做為追蹤駭客入侵的證據。

二、內部稽核考量

(1)訂定本公司內部稽核管理規定。

(2)定期稽查資訊安全事項辦理情形。

(3)應訂有資訊安全作業稽查計畫(含稽查內容、範圍、程序、人員)，並公布。

(4)稽查人員須經過訓練並作事前工作分配。

(5)稽查結果包括背景描述、稽查項目、過程、結果、改進建議等內容。

(6)稽查結果應該製成文件留存備查。

三、符合法規要求

(1)資訊單位或稽核人員應隨時執行有關個人資料保護法規、組織紀錄保護法、智慧財產權保護法、之蒐集、公告、實施作為。

(2)資訊安全相關的記錄檔案，應依「個人資料保護法」規定辦理保存規範。