資訊安全管理作業辦法

編號：

版次：01

頁數：4

一、 目的

為確保營運活動因天然災害、意外、設備故障及蓄意行為、突發事件等意外之下，能使企業重要資訊系統及資產資料獲得保護且在最短時間內恢復運作，避免造成資訊系統及資料的損失，進而導致營運無法持續，必須建立完整的資訊系統及資料保護管理辦法，預防災難及降低損失的程度，以利企業營運持續運作。

二、 適用範圍及權責單位

(一) 適用範圍：凡與營運活動維持有關之系統皆適用本辦法。

包含：

1. 人員安全管理及教育訓練
2. 電腦主機安全管理
3. 資料安全管理
4. 網路安全及病毒防範管理
5. 網路設備存取之安全控制
6. 委外資訊單位安全管理
7. 實體環境安全管理

(二) 權責單位：總管理處資訊單位

三、 資訊安全管理執行細則

(一) 人員資訊安全管理及教育訓練

1. 新進同仁
   (1) 權責單位依據核准之「資訊資源申請單」，建立新進同仁帳號權限。
   (2) 新進同仁於新人訓練期間內完成資訊安全教育課程。
   (3) 新進同仁到職時需由總管理處資訊單位人員協助設定二階段驗證(多因素驗證)。
2. 使用者管理
   (1) 在系統使用者尚未完成正式授權程序之前，系統管理者不得對任何人提供任何系統存取服務來存取公司資訊。
   (2) 應以「資訊資源申請單」為基準賦予使用者系統權限。
   (3) 應要求使用者確實了解系統存取的各項條件及要求，只能在授權範圍內存取系統資源。
   (4) 使用者不得將個人登入身分識別碼與密碼交付他人使用，使用者亦不得以任何方法竊取他人的登入身分識別碼與密碼。
   (5) 使用者辦理調整職務及離職時，應盡速進行統存取權限異動。
   (6) 應定期檢查及註銷閒置的登入身分識別碼與密碼。
3. 使用者密碼管理
   (1) 使用者應負責保管及定期更換個人密碼，維持密碼的機密性。

(2) 使用者初次登入系統時，系統應要求更改臨時性密碼。

(3) 若有跡象顯示使用者密碼有遭破解之可能性時，應立即更改密碼。

(4) 開啟二階段驗證(多因素驗證)，減低密碼遭破解。

(二) 電腦主機安全管理

1. 電腦主機及伺服器操作程序，權責單位應確保同仁正確及安全的操作使用。
2. 各項電腦主機及伺服器設備均應指定專人管理，非經核准不得任意使用、拆卸及更動零組件。
3. 各類電腦主機、伺服器及重要之個人電腦皆應設定密碼。
4. 電腦主機之作業環境如溫度、溼度及電源供應之品質等，應隨時監測，並採取必要的防護補救措施。
5. 嚴禁使用非經授權及來路不明之軟硬體，並遵守智慧財產權相關規定。
6. 存放機密性及敏感性資料之電腦主機或伺服器，除作業系統既有的安全設定外，應強化身份辨識之安全機制，防止非法使用者透過遠端撥接或網際網路傳送資料時，被偷窺或截取登入密碼，及防制假冒合法使用者身分登入主機進行偷竊或破壞等情事。
7. 定期修補系統漏洞程式。
8. 應訂定電腦主機不正常停機之立即回復作業程序，尤其是對高使用率的系統應有妥適的回復措施。

(三) 資料安全管理

1. 藉由加密方式保護重要資訊之機密性、完整性、安全性。
2. 重要資訊檔案包含：人事資料、財務資料、智慧財產權、研發資料、業務資料、客戶資料等，確保資料之安全性及機密性。
3. 應落實定期備份作業及電腦媒體異地備援作業之執行，以利發生災害或儲存媒體失效時，可迅速恢復正常作業。
4. 重要資料須區分機密等級並依權限使用。
5. 應依使用者所負責業務性質及職掌，賦予不同資料存取權限，並保存重要檔案或敏感性資料之存取紀錄以備查考，避免重要資訊外露或遭不經意之更動。
6. 應加強資訊媒體與資訊文件之安全管理。
7. 儲存媒體應依媒體保存規格，存放於安全環境。
8. 電腦媒體檔案名稱應採代碼或簡碼標示，以防有心人士輕易辨識或洞悉資料內涵。
9. 與其他單位進行電子資訊交換，應採取適當之保護措施，以防止資訊受損或未經授權之資訊存取與竄改；重要資訊交換時需有加密及電子簽章之機制進行控管。

(四) 網路安全及病毒防範管理

1. 建立電腦病毒防範機制，電腦病毒碼及防毒軟體應定期進行更新。
2. 網路設備需有專人管理，隨時監測網路狀況。
3. 聯外網路需安裝防護措施，適時注意可能之漏洞。
4. 應禁止及防範網路使用者以任何儀器設備或軟體工具竊取網路上之通訊。
5. 網路系統管理者未經權責主管許可，不得任意閱覽使用者之私人檔案；惟若發現有網路安全之虞時，得授權網路系統管理者檢查使用者檔案。
6. 網路系統使用之各主機伺服器應有備援主機，以因應主要之主機伺服器無法正常運作時使用。

(五) 網路設備存取之安全控制

1. 網路連線作業之控制
   (1) 為確保系統安全，跨機關的網路系統應限制使用者之連線作業能力。例如，以網路閘門技術依事前訂定之系統存取規定，過濾網路之傳輸作業。
   (2) 網路連線使用者應遵守相關安全規定，如有違反，依相關法規處理，並取消其網路資源存取權限。
   (3) 訪客對網路的存取，非經內部人員允許，否則拒絕其存取內部資訊系統。
2. 網路路由控制
   (1) 分享式的網路系統，應建立網路路由的控制，以確保電腦連線作業及資訊流動不會影響應用系統的存取政策。
   (2) 網路路由的控制，應建立實際來源及終點位址之檢查機制，並應事先評估瞭解不同方式的安全控制能力。

(六) 委外資訊單位安全管理

1. 需委外服務作業時，與廠商簽訂委外服務合約，並簽署書面的保密契約，以確保廠商人員了解並遵循安全管理相關規定。
2. 委外資訊單位若需使用 USB、外接式硬碟進行存取動作時應取得本公司權責主管同意。
3. 委外資訊單位應禁止直接存取公司內部網路，以降低資料外流風險。
4. 委外資訊單位攜出存有本公司相關資訊設備時，取得本公司權責主管同意後，才能放行。
5. 人員進出機房, 須有委外資訊同仁陪同，且須填寫「機房出入管制表」。

(七) 實體環境安全管理

1. 一般辦公環境安全管理
   (1) 實體環境安全管制，應以事前劃定之各項資訊設施為基礎，並設置必要之認證措施(例：使用員工識別證之門禁系統)，以達成安全控管之目的。

(2) 各項資訊設備之實體保護程度及設置位置，應依資訊資產及服務系統之價值與風險考量而異。

(3) 電腦設備、資訊、軟體，應取得權責主管授權後，方可攜出。

2. 電腦機房安全管理

(1) 公司有自行建構之電腦機房時適用。

(2) 電腦機房應考量天然災害之實體防護措施，並考量鄰近空間設備可能造成之安全威脅。

(3) 危險性及易燃性物品，應遠離電腦機房並予以存放至安全地點。非有必要電腦相關文具設備不應存放於電腦機房內。

(4) 備援作業使用之設備及媒體，應存放於電腦機房安全距離之外，以避免電腦機房受到損害時亦遭受損失。

(5) 進出電腦機房之人員應有適當之管制與紀錄，非經授權之人員不得進入。

(6) 應有適當之安全偵測與防制設備(例：熱度及煙霧偵測設備、火災警報設備、滅火設備及火災逃生設備)，並依廠商提供之使用說明書定期檢查。

(7) 應設置電腦機房之火警、空調、溫溼度、電源供應等警示自動通報系統，全天候掌握機房運作情形，以確保機房設施之安全。

3. 辦公桌面安全管理

(1) 個人電腦及電腦終端機不再使用時，應關機、上鎖或是其他控制措施保護。

(2) 個人電腦嚴禁使用非經授權及來路不明之軟硬體。

(3) 列印之文件及磁性媒體在不使用或非上班時段，應存放在櫃子內，機密性及敏感性資訊並應上鎖保護。

四、 訓練與宣導

本辦法供同仁上網查閱，並同時利用權責單位之不定期教育訓練進行時，同時宣告公司之資訊安全政策；新進人員則於新人教育訓練時由權責單位負責相關訓練與宣導課程，或自行上網閱讀相關文件。

五、 實施

本辦法呈請核准後公佈實施，修正時亦同。