大亞電線電纜股份有限公司

資通安全作業程序

一、目的：隨著資訊化程度的加深，為確保公司資料安全性、防止硬體、軟體與使用者資料遭受來自外部或內部的威脅，確保資訊系統持續運作，透過有效的資訊安全管理，來防止公司資訊系統受到潛在威脅的破壞，特訂定本作業程序。

二、適用範圍：凡連線使用公司網域之電腦系統、人員，悉依本作業程序之規定處理。

三、權責：資訊部進行資訊安全政策維護與檢討；資訊部最高主管負責資訊安全系統之協調、推動及監督等事項。

四、名詞解釋：

防火牆：是一個定位用來分隔兩個不同網路的網路安全裝置，通常是介於企業機構的內部、受信任的網路和網際網路。讓合法的使用者，可正常的取得公開於網路上的資料；防止非法的使用者，蓄意破壞、商業性破壞及保護公開與尚未公開的資料等。網際網路防火牆是一套軟體或硬體，可協助阻擋試圖透過網際網路進入公司電腦的駭客、病毒和電腦乳蠕蟲。

五、內容：

5.1 為避免網路駭客透過網際網路入侵公司電腦、破壞電腦檔案、偷竊電腦資料…等破壞動作，故安裝網路防火牆阻擋試圖入金公司網路之駭客。

5.2 軟體更新：電腦作業系統使用一段時間後，通常會出現一些安全漏洞，這些漏洞會是駭客容易利用的弱點，需隨時留意系統更新功能與提醒，定期執行各項系統漏洞修補程式。

5.3 存取控制：

5.3.1 使用者存取權限註冊與註銷：

新增使用者依據「電腦文件及媒體管理辦法」(AC-DE-I001)，需填寫“電腦系統程式資料申請書”(AC-DE-R01B)申請。員工離職或職務異動，依據文件「電腦文件及媒體管理辦法」(AC-DE-I001)，取消或修改使用者權限。

5.3.2 資訊存取控制，依職務、業務需要分別訂定，使用者依據「電腦文件媒體管理辦法」(AC-DE-I001)，給予適當授權。

5.3.3 自外部網路登入公司網域之管理：

架設防火牆設定相關存取權限，若公司員工在外部網路登入公司內部網路，須事先申請，並經過VPN或citrix憑證的認證，認證通過方能公司內部資源。

5.3.4 為避免資料被非法讀取，公司使用者用來登入網路、資料庫與e-mail的密

碼，應該妥善保管。

密碼設定/使用原則：

(1)勿隨意透露密碼給別人。

(2)設定不容易被猜出的密碼。

(3)一旦懷疑有人可能知道你的密碼時，即刻更改。

5.3.5 資料備份：

應定期執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。資訊部須依據「電腦主機資料備份及電腦機房管理作業辦法」(AC-DE-I002)，對系統資料進行備份。

5.4 公司內伺服器及個人電腦應採必要的事前預防及保護措施，防制及偵測電腦病毒及惡意軟體等的侵入；促使員工正確認知電腦病得的威脅，提升員工的資訊安全警覺，健全系統之存取控制機制。為避免病毒造成電腦的傷害，安裝防毒軟體，定期更新病毒碼，並定期對使用者電腦進行掃毒。電子郵件附件及下載檔案在使用前，檢查有無惡意軟體、病毒、後門程式。依據內控文件「個人電腦軟硬體周邊採購及管理作業程序」(AC-DE-P002)，控制電腦中毒事件。

5.5 可攜帶式資訊設備之規範：

5.5.1 公司員工非必要不可使用隨身碟、磁片、光碟片、燒錄器等可將資料複製之用品，避免公司資料外洩。

5.5.2 廠商或講師製公司簡報或上課，攜帶之隨身碟或光碟等儲存設備，承辦人員須拿至資訊部進行掃毒，確認無毒，方能使用該儲存設備，若未依規定而發生中毒，承辦人員將依未遵守公司管理規定進行懲處。

5.6 電子郵件管理

5.6.1 公司員工要對外收發e-mail，需填寫異動單經過主管授權，再由資訊部開放並建立e-mail位址。

5.6.2 架設SPAM SERVER，外部信件須透過SPAM SERVER過濾及判斷是否為垃圾信件或病毒，防止電腦病毒侵入公司內部或是對外攻擊，並防止病毒擴散傳遞到使用者的工作站。

5.6.3 非公司內部員工的e-mail無法傳送即轉遞。

5.6.4 收發internet郵件，內容超過15MB無法收發，10MB至15MB於凌晨12:00才收發，以保持e-mail收發的順暢。