愛爾達科技股份有限公司

資通安全檢查規範及管理辦法

一、作業程序

(一)範圍：本作業程序適用於網路安全、電子郵件及公司資訊網路之管理。

(二)網路安全管理：

1.程序說明：

1.1 掃毒系統之管理

A. 個人電腦及網路系統伺服器均需裝置掃毒系統。

B. 個人電腦及網路系統伺服器的病毒碼須得隨時更新。

1.2 網路服務之管理

A. 系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理。

B. 網路系統管理人員應負責製發帳號，提供取得授權的人員使用；除非經權責主管核准後，否則不得製發匿名或多人共享的帳號。

C. 提供給內部人員使用的網路服務，與開放有關人員從遠端登入內部網路系統的網路服務，應執行嚴謹的身分辨識作業。

D. 如果系統使用者已非合法授權的使用者時，網路系統管理人員應立即撤銷其使用者帳號；離（停）職人員應取銷其存取網路之權利。

E. 網路系統管理人員除依公司規定，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權規定，使用自動搜尋工具檢查檔案。

F. 網路系統管理人員未經使用者同意，不得增加、刪除及修改私人檔案。如有特殊緊急狀況，須刪除私人檔案，應以電子郵件或其他方式事先知會檔案擁有者。

G. 對任何網路安全事件，網路系統管理人員應立即向權責主管反應。

H. 對於主機上任何進出入之紀錄均得予以保留。

I. 網路管理人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢之困擾。

1.3 網路使用者之管理

A. 被授權的網路使用者（以下簡稱網路使用者），只能在授權範圍內存取網路資源。

B. 網路使用者應遵守網路安全規定，並確實瞭解其應負的責任；如有違反網路安全情事，應限制或撤消其網路資源存取權利，並依公司規定及相關法律處理。

C. 網路使用者不得將自己的登入身份識別與登入網路的密碼交付他人使用。
D. 使用者離開座位時應將螢幕與桌面淨空避免重要資訊遭他人窺視及外流。
E. 禁止網路使用者以任何方法竊取他人的登入身份與登入密碼。
F. 禁止散佈電腦病毒或其他干擾或破壞系統機能之程式。
G. 禁止擅自截取網路傳輸訊息。
H. 禁止以破解、盜用或冒用其他人帳號及密碼等方式，未經授權使用網路資源，或無故洩漏他人之帳號及密碼。
I. 禁止無故將帳號借予他人使用。
J. 禁止隱藏帳號或使用虛假帳號，但經明確授權得匿名使用者不在此限。
K. 嚴禁窺視他人之電子郵件或檔案。
L. 禁止以任何方式濫用網路資源，包括以電子郵件大量傳送廣告信、連鎖信、色情信或無用之信息，或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。
M. 禁止以電子郵件、線上談話、電子佈告欄(BBS)或架設網站(如WWW、BBS、FTP)等方式散佈詐欺、誹謗、污辱、猥褻、非法軟體交易或其他違法之訊息。
N. 禁止及防範網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。
O. 禁止上網瀏覽與公司業務無關之網站，尤其上網打線上遊戲或瀏覽色情網站或玩電腦遊戲。
P. 禁止下載或燒錄 MP3 音樂、非法軟體。
Q. 禁止聆聽網路收音機，佔用網路資源。
R. 禁止利用公司之網路資源從事非公司研究等相關之活動或違法行為。

1.4 主機安全防護

存放機密性及敏感性資料之大型主機或伺服器主機(如 Domain Name Server 等)，需有安全設定，及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

1.5 防火牆之安全防護

A. 公司與外界網路連接的網點，應加裝防火牆，以控管外界與公司內部網路之間的資料傳輸與資源存取。
B. 防火牆應由網路系統管理人員執行控管設定，並依公司制定的資訊安全規定、資料安全等級及資源存取的控管策略，建立系統稽核的安全機制，有效地規範資源被讀取、更改、刪除、下載或上傳等行為以及系統存取權限等資訊。

C. 防火牆設置完成時,應測試防火牆是否依設定的功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定的安全目標。

D. 網路系統管理人員應配合公司政策及規定的更新,以及網路設備的變動，隨時檢討及調整防火牆系統的設定，調整系統存取權限，以反應最新的狀況。

1.6 網路資訊之管理

A. 對外開放的資訊系統,應儘可能安裝在一部專用的主機上，並以防火牆與公司內部網路區隔，提高內部網路的安全性。

B. 對外開放的資訊系統,應針對蓄意破壞者可能以發送作業系統指令或傳送大量資料(如電子郵件、註冊或申請資料)導致系統作業癱瘓等情事，預作有效的防範，以免影響公司業務正常之運作。

C. 機密性及敏感性的資料或文件,不得存放在對外開放的資訊系統中。

D. 網路系統管理人員應負責監督網路資料使用情形,檢查有無違反資訊安全規定之事件發生。

E. 對外開放的資訊系統所提供之網路服務(FTP,HTTP 等)，應做適當的存取控管，以維護系統正常運作。

(三)電子郵件安全管理：

1 程序說明：

1.1 涉及公司之商業機密文件資料，不得以電子郵件傳送；敏感性資訊如有電子傳送之必要，得經加密處理後傳送。

1.2 電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。另針對來路不明的電子郵件，應交由網路系統管理者處理，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

(四)網際網路資通安全之管理：

1 程序說明：

1.1 內部使用的瀏覽器，應作虛擬 IP 位址的設定，並針對下載的每一檔案做電腦病毒或惡意內容的掃描。

1.2 跨廠區間透過公眾網路做資料傳送，必須以 VPN 方式連線，以維持封包之安全性。

2.網路入侵之處理：

2.1 網路如發現有被入侵或有疑似被侵入情形，應立即通知權責主管，採取必要的行動。

2.2 網路入侵的處理步驟如下：

A.立即拒絕入侵者任何存取動作，防止災害

B.繼續擴大；當防火牆被突破時，系統應設定拒絕任何存取；或入侵者已被嚴密監控，

C.在不危害內部網路安全的前提下，得適度允許入侵者存取動作，以利追查入侵者。

D.切斷入侵者的連接，如無法切斷則必須關閉防火牆；或為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。

E.正式紀錄入侵的情形及評估影響的層面。

F.立即向權責主管人員報告入侵情形，以獲取必要的協助。

二、控制重點

(一)公司內部是否有專業人員負責處理有關資訊系統安全預防及危機處理相關事宜。

(二)是否建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，防止未經授權的系統存取。

(三)公司之電腦網路系統，是否對內安裝防毒軟體，對外設置網路防火牆。

(四)公司是否依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，是否立即撤銷該使用者之帳號及權限。

(五)個人電腦及網路系統伺服器，是否具備電腦病毒掃瞄工具。

(六)個人電腦及網路系統之資料，是否定期備份重要檔案及資料。

(七)應擬定適當之資通安全檢查機制與規範。

(八)應評估與指定適當之內部人員或委外執行資通安全檢查計劃之擬定，定期檢查內外部相關人員與單位遵循公司資通安全相關政策與施行規定之情形。

(九)是否已適當考量執行資通安全檢查之人員獨立性，並已接受適當之教育訓練。

(十)對於資通安全檢查之各項書面要求(如工作底稿、查核報告)是否訂定規範予以執行。管理階層並定期檢視該書面記錄，以瞭解其對規範之遵循與編製之完整性。並對檢查所提出之發現與問題，應予以瞭解、追蹤及覆核改善之情形

(十一)資通安全檢查之文件是否由專責人員保管，並擬定適當之保存程序。

三、本辦法訂定於中華民國 101 年 4 月 3 日經董事會通過後實施。