文件號碼	資訊安全管理辦法	頁次/總頁次	1/4
C3-05-A		發 行 日 期	2006/05/09
		版次/變更次	A

1. 目的

本辦法旨在說明使用網路與資訊系統時，必須考量的安全注意事項，防止公司資訊系統及其資料遭致不當使用、洩漏、竄改、破壞等情事，特訂定此管理辦法以供依循。

2. 範圍

包括人員管理、電腦硬體設備、基本作業軟體(作業系統)、應用軟體及各類型之資料等。

3. 定義

無。

4. 權責

4.1 資訊主管：負責擬定及更新此辦法，並確保本辦法確實執行。

4.2 系統管理員：依循此辦法，實際執行各項資訊安全管理作業之人員。

5 作業程序

5.1 人員管理

對於與資訊系統有接觸的人員，規定個人對資訊系統的使用權限和責任歸屬。

5.1.1 使用單位人員

5.1.1.1 賦與使用人員存取資訊系統之權限，應僅限於執行法定任務，需求單位依其需求填寫【系統使用需求申請表】（7.1表單）或【ERP系統權限申請表】（7.2表單）。

5.1.1.2 若違反資訊安全規定之行為，應告知相關人員，俾利其遵循。

5.1.1.3 使用單位人員離(休)職時，應依規定取消其使用機關內資訊資源之所有權限。

5.1.1.4 使用單位人員應遵守公司相關保密規定，約定在職期間或離職後均不可洩漏機密資料。

5.1.2 資訊系統內使用者管理

5.1.2.1 資訊系統應該提供使用者個別的安全屬性，包括等級、部門等影響其所能接觸資料的因素。

5.1.2.2 資訊系統內部使用者的權限必須與其實際職務之權限相配合。

5.1.2.3 資訊系統內部使用者帳號之建立、終止和刪除必須經由權責部門主管核准。

5.1.3 網路使用者

5.1.3.1 使用者不允許將自己的登入身份與登入網路密碼供他人使用。

5.1.3.2 使用者禁止以任何方法竊取其他合法使用者的登入身份與登入網路密碼。

5.1.3.3 使用者禁止存取網路上未經許可的檔案或企圖獲得存取的權限。

5.1.3.4 使用者不准持有色情或猥褻檔案，並禁止在網路上散播色情文字、圖片、影像、聲音等。

5.1.3.5 使用者禁止發送電子郵件去騷擾其他使用者，而導致別人不安與焦慮。

5.1.3.6 使用者禁止發送匿名或偽造電子郵件。

5.1.3.7 使用者禁止以任何手段蓄意干擾或防害網路系統的正常運作。

5.1.4 網路系統管理者

5.1.4.1 網路系統管理者應負責網路安全政策的制定與執行，及網管工具系統設定與操作，以確保各單位內部系統主機與資料的安全與完整。

5.1.4.2 若使用者已不再是合法使用者，網路系統管理者應負責將使用者帳號移除。

5.1.4.3 網路系統管理者未經許可禁止閱覽使用者私人檔案。

5.1.4.4 網路系統管理者未經使用者同意，不可增加、刪除、修改私人檔案。如有特殊緊急狀況，必須刪除私人檔案，則須先知會檔案擁有者。(電子郵件是可接受的知會管道之一)

5.1.4.5 對任何網路安全違例事件，網路系統管理者應立即向單位主管反應。

5.1.4.6 網路系統管理者不得新增、刪除、修改稽核資料檔案，以避免安全違例發生時，追蹤查詢的困擾。

5.2 軟體及資料管理

5.2.1 軟體維護

5.2.1.1 應有專人負責維持資訊系統的正常運作。

5.2.1.2 資訊系統的變更須經過權責單位核定，並應妥善管制記錄變更的過程以備查詢。

5.2.1.3 軟體安裝需經申請，透過資訊人員安裝，並留下紀錄以備查詢。需求單位依其需求填寫【故障維修紀錄表】（7.3表單）。

5.2.2 資料管理

5.2.2.1 各類資料因其特性及內容不同，應該給予不同的公開或銷毀期限。

5.2.2.2 各類資料建檔若因資料量過於龐大而必需委外處理時，應先行通報權責單位核准。

5.2.2.3 資訊檔案若因特殊原因外借時，須確保其外借機關之安全屬性符合其所接觸資料之安全等級。

5.2.2.4 任何先前遺留的資訊內容，一旦遇到新的資源配置時，應立即刪除。

5.2.3 資訊流控制功能

5.2.3.1 應嚴密監視系統中的資訊流，以確保資訊流的安全。

5.2.3.2 系統中資訊流的合法性應受資訊系統的監控，以防範非法的資訊流傳輸。

5.2.4 內部資料傳輸

5.2.4.1 系統內部應施行存取控制和資訊流控制，以確保使用者資料的安全。

5.2.4.2 資訊系統應提供被授權的管理者選擇他們想要的資料保護方式，以確保各個分離子系統在傳輸資訊時的安全性。

5.3 實體及網路管理

實體及網路管理包含硬體資源和電腦網路的管理。這裡所稱的硬體資源包括：電腦主機、周邊設備等。

5.3.1 電腦設備保護

5.3.1.1 資訊系統的硬體設備應放置在適當的場所。

5.3.1.2 電腦機房之安全維護應指派專人負責。

5.3.1.3 資訊系統的重要硬體設備應限制其接觸人員，必要時可加裝監視或門禁設施。

5.3.1.4 電壓不穩地區應加裝穩壓設備或不斷電系統。

5.3.2 網路連線作業

5.3.2.1 資訊系統中各主體之對外連線作業須受到適當的管制和稽核。

5.3.2.2 網路應加裝防火牆以保護內部系統及資訊。

5.3.2.3 各單位提供給內部人員與各單位業務有關人員經由遠端登入內部網路系統的網路服務，應作嚴謹的身份辨識。

5.3.3 登入網路密碼管理

5.3.3.1 使用者登入代碼和登入密碼對每一合法使用者是絕對唯一。

5.3.3.2 登入密碼至少由六位字母與數字符號構成。

5.3.3.3 登入密碼檔案必須儲存於安全隱蔽之處，並加密處理。

5.3.3.4 登入密碼需定期更改，以提高安全性。

5.3.3.5 嘗試登入數次失敗後，應暫停使用者帳號，並將失敗登入記錄於稽核檔中，以便日後查詢。

5.3.3.6 使用者在規定期限內若無使用其帳號，網路系統管理者應暫停使用者之帳號。

5.3.4 傳輸資料加密

5.3.4.1 資訊系統應該提供加密機制。

5.3.4.2 資訊系統應可調整或選擇所使用的加密機制。

5.3.5 軟體輸入控制

5.3.5.1 各單位網路使用者禁止使用非法軟體。

5.3.5.2 各單位應在網路上各檔案伺服器安裝防毒軟體，防止病毒在網路上擴散。

5.3.5.3 使用者如偵測到病毒入侵，應馬上通知網路管理者。網路管理者須告知使用者受病毒感染的資料及程式，避免病毒的擴散。

5.3.5.4 如有機器遭受病毒感染，應立即與網路離線，直到網管人員確認病毒已移除，才可重新與網路連線。

6 參考文件

6.1 『資訊系統開發辦法』

7 附件

7.1 【系統使用需求申請表】

7.2 【ERP系統權限申請表】

7.3 【故障維修紀錄表】

8 流程圖

無。

9 本辦法依文件作業管制作業程序相關規定核准公告，修訂時亦同。

10 沿革

制定公佈日期：2006年5月8日，制定部門：資訊服務部。