資訊管理辦法

目　　錄

第一章　網 路 管 理

訂定日期：91.07.15

第一條、目的：

為有效提昇公司員工工作效率的目標下，建立網路管理之機制，防止網路資源之誤用及駭客之入侵，避免主機被破壞或公司機密被竊取，造成公司無法復原的有形、無形損失。

第二條、適用範圍：

本辦法適用於公司內部網路及對外網路之使用管理。

第三條、 權責：

本公司所有員工，皆需遵守政策。

第四條、作業流程與說明：

一、網路服務之管理：

1. 應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，保護連網作業，防止未經授權的系統存取。
2. 對於跨企業之電腦網路系統，應特別加強網路安全管理。
3. 利用公共網路傳送機密性資訊，應採取特別的安全保護措施，以保護資料在公共網路傳輸的完整性及機密性，並保護連線作業系統之安全性。
4. 系統的最高使用權，應經權責主管人員審慎評估後，交付可信賴的資訊部人員管理。
5. 資訊部應負責製發帳號，供授權的人員使用。
6. 提供給內部人員使用的網路服務，與開放業務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，或使用防火牆代理伺服器(ProxyServer)進行安全控管。
7. 離(休)職人員應依「員工工作規則」規定及程序，取銷其存取網路之權利。
8. 資訊部人員未經權責主管許可，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，資訊部得依授權規定檢查其檔案。

9. 資訊部未經使用者同意，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。
10. 資訊部不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。
11. 網路系統中各主要主機伺服器應有備援主機，以備主要作業主機無法正常運作時之用。
12. 網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。

二、網路使用者之管理

1. 在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。
2. 被授權的網路使用者，只能在授權範圍內存取網路資訊。
3. 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。
4. 禁止網路使用者以任何方法竊取他人的登入身份與登入網路密碼。
5. 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。
6. 禁止網路使用者在網路上取用未經授權的檔案。
7. 網路使用者不得將不合法或不正當的資訊建置在公司網路，或在網路上散播。
8. 禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便。
9. 禁止網路使用者發送匿名信，或偽造他人名義發送電子郵件。
10. 網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。
11. 公司外部取得授權的電腦主機或網路設備，與公司內部網路連線作業時，應確實遵守之網路安全規定及連線作業程序。
12. 必要時應要求使用者簽訂約定，使其確實瞭解系統存取的各項條件及要求。
13. 當有跡象足以顯示使用者密碼可能遭破解時，應立即更改密碼。
14. 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。

15. 登入密碼至少由六位字母與數字符號構成(系統具備有此項功能者)登入密碼需定期更改，以提高安全性。(系統具備有此項功能者)。
16. 嘗試登入三次失敗後，應暫停使用者帳號，並將失敗記錄登入於稽核檔中，以便日後查詢。(系統具備有此項功能者)。
17. 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。(系統具備有此項功能者)。
18. 使用者調整職務及離(休)職時應儘速調整其系統存取權限。
19. 應檢查及取銷閒置不用的識別碼及帳號。

三、主機安全防護

存放機密性及敏感性資料之大小型主機或伺服器主機(如 Domain Name Server)等，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，防止遠端撥接或遠端登入。資料經由電話線路或網際網路傳送時，應防制被偷窺或截取(如一般網路服務 HTTP、Telent、FTP 等的登入密碼)，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。

四、防火牆安全防護

1. 應安裝防火牆(代理伺服器 Proxy Server)以提供 HTTP、FTP、WWW、Gopher 等網路服務的轉送與控管。
2. 防火牆應由網路系統管理者執行控管的設定，並依據所制定的安全政策，亦即存取資源的管控策略，它包含了身份辨識的機制、進入服務(incoming service)、連外服務(outgoing service)與稽核上的需求以及那些資源可被讀取、更改、刪除、下載或上載等行為規範及以那些人擁有這些權限等資訊。
3. 網路系統管理者應由系統終端機登入防火牆，禁止採取遠端登入，以避免登入資料遭竊取進而危害網路系統的安全。

4. 防火牆設置完成時，應測試防火牆運作的正常性。如有缺失，應立即修正，直到達成規劃之目標。
5. 由於安全政策的更新或網路設備的變動，網路系統管理者應對防火牆系統的設定或允許權限上做適當的調整，以反應現狀。
6. 防火牆系統軟體，應定期檢討版本升級問題，以因應新而未知的網路攻擊。

五、遠端登入之安全控制

1. 遠端登入之使用權限，需申請該核准後方可遠端登入。
2. 遠端登入之安全驗證，須驗證是否有遠端撥入之權限，若否，則拒絕登入。
3. 記錄遠端登入之事項應包括使用者識別碼、登入及登出系統之日期及時間。

六、電子郵件安全管理

應建立電子郵件的安全管理機制，以降低電子郵件可能帶來的業務上及安全上的風險。

七 、全球資訊網之安全管理

1. 內部使用的瀏覽器，應作防火牆代理伺服器的設定。
2. 內部使用的瀏覽器，應設定為對下載的每一檔案做電腦病毒的掃描。
3. 應考量網際網路新技術(如 Java、ActiveX 等)的可能安全弱點，並採取適當的防護措施以確保內部網路安全。
4. HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身份。
5. 應對 HTTP 伺服器可存取的範圍，限制在僅能存取檔案系統的某一特定區域。

八、網路設備備援與系統備援

1. 為維持網路的持續正常運作，各重要網路設備應有備援。
2. 網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。
3. 為確保內部網路與外界的服務持續暢通，內部網路與外界網路的連接，應有一個以上的替代路徑。
4. 網路系統中各主要主機伺服器應有備援主機，以備主要作業主機無法正常運作時之用。
5. 網路系統之各主機應定期做系統備份，包括完整系統備份，系統架構設定備份以及稽核資料備份。

第五條、簽立『使用個人電腦軟體及員工網際網路使用政策』之公司員工同意書：

當員工以不當的方式使用網際網路時 ，可能置企業的安全性、私密行於險境，並且為了避免員工利用公司網際網路，從事觸犯散播播送販賣製造猥褻物品罪、賭博罪、毀謗罪、妨害秘密罪或侵害著作權的行為，所有員工應閱讀以下之『使用個人電腦軟體及員工網際網路使用政策』，並於該使用政策上簽名，以免造成公司之損失。

茂綸股份有限公司

使用個人電腦軟體及員工網際網路使用政策

公 司 員 工 同 意 書

一、使用個人電腦軟體

1. 茂綸股份有限公司獲得多家公司授權使用其電腦軟體,本公司並未擁有本軟體或其相關之文件，除非獲得軟體商之許可，無權加以複製，除例外為備份之用途。

2. 在客戶端/伺服器及網路應用程式方面，本公司員工僅能依符合授權合約條款而使用該軟體。

3. 公司員工若未依規定使用合法軟體者，其發生之法律責任需自行負責。

4. 根據適用的著作權法規定,涉及非法軟體複製的個人可能遭受包括罰金和徒刑在內的民事賠償和刑事處分。本公司絕不許可非法軟體複製。本公司員工如有複製、取得、或使用未獲授權電腦軟體的行為，請按情節輕重遭受處分(包括開除在內)。

5. 如對任何一員工是否能複製或使用某一軟體程式有疑問，請於採取行動前先向有權責的資訊部門洽詢。

6. 禁止安裝或下載非法軟體。若認為某種資訊工具會對工作有特別的幫助，請向公司建議考慮購買該軟體。

7. 個人電腦或其他可攜式電腦，應以密碼或其他經授權之方式保護，並安裝公司所提供之防毒或防火牆軟體，非經資訊單位或管理階層允許，不得私自移除或停用。

二、使用網際網路

公司提供員工使用網際網路之主要目的，在於協助員工完成其分內之職務，員工亦得在合理的私人目的下使用網際網路,但須符合公司所定合理使用政策。員工不得以「將嚴重影響工作應盡之責任」或「將使公司陷於遭受法律非難或重大損失之危險」的方式使用公司所提供之網際網路。

1. 公司網際網路的合理使用：

（1）與工作相關之目的

（2）經公司同意後，以個人目的使用即時通訊聯繫軟體。

（3）經公司同意後，以個人目的使用網際網路(全球資訊網 www、ftp、email)。

（4）經公司同意後，以個人目的利用其他網路服務或協定。

2. 非合理之使用：

（1）個人商業使用

（2）上載或下載未經授權之軟體

（3）寄發垃圾郵件、故意散播電腦病毒。

（4）散播公司機密。

（5）任何非法目的。

（6）故意造成任何網路、資訊服務與設備之中斷或干擾。

（7）故意使他人閱讀「將導致公司須對該他人負妨害風化或平等工作機會」等相關法律責任之內容。

（8）故意下載檔案，或要求軟體或資料，而有理由相信將會佔用過多的頻寬。

（9）網路相關帳號密碼之監聽或竊取盜用。

三、智慧財產權保護與機密資料保護

1. 非經智慧財產之提供人或所有權人明確同意，不得使用、散布、重製、出版或傳輸智慧財產或其任何部份，亦不可藉由任何人於非經授權之網站使用智慧財產。(舉凡工作上取得之任何 商品型錄、說明書、手冊、圖文稿、設計資料、技術、製程、軟體、協議文件...等，均列為保護範圍)

2. 非經法律允許或智慧財產之提供人或所有權人同意,不得對智慧財產或其任何部份進行修改、還原工程、反編譯或反組譯，亦不得製造智慧財產或其任何部份之衍生作品。

3. 非經智慧財產之提供人或所有權人同意外,不得將其所有權利之一部或全部移轉或讓與任何第三人。

4. 任何工作上所取得之供應商或客戶資訊，除經供應商或客戶之同意外，不得洩漏，並應妥善保存防止外洩。亦不得以任何形式，輸出或複製任何足以辨識供應商或客戶之資料至任何媒體，而使公司外部之第三人得以接觸。

5. 不得以任何形式，輸出或複製有關客戶買賣訂單、供應商訂單、商品價格、存貨、會計／財政情況及人力資源等商業資料至任何媒體，而使本公司外部之第三人得以接觸。

6. 任何工作上所取得之公司之營業秘密或員工資料，應負保密義務，非經允許，禁止將相關資料以任何形式交予他人。

7. 非經管理階層之同意，不得提供 POS 資料或足以辨識客戶之銷售預測資料給供應商。

四、違反政策之報告與懲處

1. 一旦發現有任何違反本政策之可疑行為，所有員工皆有義務向公司或公司相關企業之資訊部門、內部稽核、法務部門、管理階層報告，任何隱密或包庇之行為均可能予以處分。

2. 本公司人員違反本政策者，應依員工工作規則中之規定依情節輕重採取必要之紀律處分或解僱。若因違反致生損害於本公司財產或利益者，本公司應循相關途徑追究其法律責任。

本人充分瞭解茂綸股份有限公司上述之政策，且同意遵守。

_____

（員工簽名及日期）

第二章：軟 體 使 用 管 理

訂定日期：91.07.15
修訂日期：91.12.01
修訂日期：94.08.02
修訂日期：94.09.05

第一條、目的：

為尊重智慧財產權，倡導合法使用軟體觀念，保障公司及同仁權益，避免公司或個人因疏忽等因素，使用非法或未授權之軟體。並希望透過此規定，有效提昇電腦使用效率，增進員工之生產力。

第二條、軟體之驗收、保管與配發：

一、驗收部門：行政管理部、資訊部。

行政管理部負責版權軟體之驗收及資訊部會同驗收。

資訊部負責授權數量記錄以及分配各部門可用之合法授權數。

二、保管部門：資訊部。

所有軟體版權之正本，應由專人統一保管，以方便統計配發及配合有關部門查核。

三、配發：由使用部門提出申請。

第三條、合法軟體授權統計

資訊部應統計並呈報公司現有合法軟體總數以及各部門可使用軟體之合法授權數量。

第四條、員工軟體使用規範：

公司內所有同仁依其所屬職務不同，可使用之軟體種類亦有所不同。除公司可使用之合法授權軟體外，公司同仁**不得自行複製、備份及使用任何非合法授權之軟體**。一經資訊部查獲，將馬上強制要求移除該非法軟體。

第五條、特殊應用軟體使用規範：

公司內之研發處可安裝測試版軟體，但須合法取得測試版本之授權。對於工作所需之軟體，使用之個人依照公司採購程序，填寫 「電腦作業需求申請單」，經核決權限核准後，由行政管理部統一採購。

第六條、軟體需求及授權數增加之申請：

各使用人依其工作性質，可申請(請購)所需之軟體和增加現有軟體授權。由使用人依照公司採購程序，填寫 「電腦作業需求申請單」，經核決權限核准後，由行政管理部統一採購。

第七條、重大軟體違法使用之處分：

凡公司同仁自行使用非法軟體致**觸犯法律，該同仁*自付其責*，與公司無關。**且因此而導致公司蒙受損失，除依著作權法送辦外，以員工工作規則作處分並要求賠償公司之損失。

第八條、簽立『使用個人電腦軟體及員工網際網路使用政策』之公司員工同意書:

員工應與公司簽立同意書，以確保及明瞭不使用非法軟體，以免造成公司之損失。

第三章：電腦軟硬體購置、使用與處份

訂定日期:91.07.15
修訂日期:94.09.05
修訂日期:94.11.09
修訂日期:99.11.08
修訂日期:100.12.07

第一條、目的：

明確訂立公司政策，使公司購置電腦軟硬體、使用及處份作業有所遵循，以利公司作業之進行。

第二條、範圍：

本辦法適用於全公司購置、使用與處份電腦軟硬體(不論金額大小)作業。

第三條、購置程序：

一、請購需求：

(一) 電腦暨週邊設備新增、更換、升級：

使用部門因各項因素(例如：引進新人)需新增、更換、升級各項電腦暨週邊設備，使用部門填寫「電腦暨週邊設備新增、更換、升級需求申請紀錄表」，由申請人、該權責主管簽核，並由資訊部進行會簽，若採購金額超過新台幣一萬元以上者，需請申請人呈核總經理。

(二)新套裝軟體、新作業系統等：

使用部門若申請增添新套裝軟體、新作業系統等，需先填寫「電腦作業需求申請單」，可包含可行性評估等文件，由申請人、該權責主管簽核，並由資訊部進行會簽，若採購金額超過新台幣一萬元以上者，需請申請人呈核總經理。

(三) 資訊部為協助行政管理部採購作業，需洽詢廠商並取得廠商報價單資料，若採購對象非長期搭配之廠商或非特定規格之廠商，需附上二家以上的報價資料(詢比議價資料可由欲請購部門進行蒐集，但資訊部應依其專業判斷是否要再附上其他廠商報價資料)，以提供總經理作決策。

二、採購作業：

(一) 資訊部依照核准後的「電腦暨週邊設備新增、更換、升級需求申請紀錄表」及「電腦作業需求申請單」，填寫「請採驗收單」(後附申請紀錄表或電腦作業需求申請單、報價單資料)，經部門主管、總經理簽核後，轉交給行政管理部。

(二) 採購人員應依「財產管理辦法」中的第三條(二)規定，進行採購作業。

三、驗收作業：

(一) 驗收人員由行政管理部人員進行驗收，及由資訊部*會同驗收*，驗收人均需於「請採驗收單」簽名。

(二) 資訊部需將電腦軟硬體安裝測試無問題後，才完成驗收作業。

(三) 若公司採買新電腦軟硬體設備，資訊部應填「硬體簽收表」，將原始廠商送交物品的規格作登記，並請使用部門簽收，並將此表影印一份給行政管理部備查。

若有 License、版權等，應由行政管理部或使用人員負責保管。

同時，行政管理部同步更新「資產盤點表」、「軟體名稱表」。

四、請款作業：

採購人員應依「財產管理辦法」第三條(四)作業規定，進行請款作業。

第四條、保管及投保作業：

一、保管作業：

(一) 行政管理部應於平時更新「資產盤點表」，以維資料的正確性。

(二) 使用人員應當愛惜電腦資源，若有發生電腦損壞情形，應即通知資訊部進行處理。

(三) 資訊部應將處理情形，簡要填寫於「電腦維修記錄」，並請使用人員進行驗收。

二、*投保作業：*

行政管理部進行每年例行性投保作業時，應發聯絡單通知資訊部，並請資訊部檢視其保單是否充分，資訊部亦需發聯絡單表示其意見後，行政管理部才進行投保作業。

第五條、處份作業：

一、若使用部門已採購新設備，舊電腦軟硬體原則上由資訊部自行處理。

二、資訊部依舊電腦軟硬體的狀態，進行下列方式處理：

(一) 完全不堪使用者：由資訊部洽適當方式丟棄。

(二) 尚可使用者：由資訊部公告五個工作日拍賣，拍賣價格由資訊部部門主管決定，並發聯絡單公告；自五個工作日後即第六個工作日後若無買主，由資訊部自行處理。

(三) 資訊部需將處理情形造冊管理(後附聯絡單)。

第六條、盤點作業：

行政管理部應維護財產資料，並不定期盤點；稽核主管(得會同資訊部)進行不定期盤點，至少每年一次，並記錄及追查盤點差異原因。

第四章：電 腦 機 房 管 理

訂定日期：90.10.01
修訂日期：91.07.15
修訂日期：100.12.07

第一條、目的：

機房為公司電腦設施及資料重要地點，設立管理辦法，以確保安全。

第二條、範圍：

電腦機房。

第三條、作業程序：

1. 機房重地非資訊單位人員禁止進入，若確實有要事需進出者，應填「進出機房管制登記表」(詳附件四)。
2. 嚴禁非資訊人員擅自使用資訊部電腦設備。
3. 外來之維修人員進入電腦機房，須由資訊部人員陪同進入。
4. 資訊部人員不在時，可設定內部電話跟隨等方式，以便立即聯絡。
5. 資訊部人員均外出時必須將機房房門上鎖。
6. 機房保持清潔、整理線路、嚴防水患。
7. 機房空調應保持適當溫度，以使設備運轉順暢。
8. 消防設備需備妥就定位，並了解使用方法，應定期檢查。
9. 機器設備故障時，應即與維護廠商聯絡修復事宜。
10. 電腦設備應裝設不斷電設備，以防止電力臨時中斷致使電腦設備或資料檔案毀損。

第五章：資料保全管理

訂定日期：91.07.15
修訂日期：100.12.07

第一條、目的：

為有效保全公司資料、檔案及系統，訂定程序以供資訊部與使用部門遵守。

第二條、範圍：

全體公司員工，均需遵守此規定。

第三條、作業程序：

一、MIS 系統部分

1. 備份作業 :每周一至五固定於凌晨自動執行備份, 並於系統建立備份記錄. 每周六再將備份之資料經由網路備份至外點辦公室之一(外點辦公室: 新竹、寶橋、高雄。)
2. 備份資料確認 : 每季(一, 四, 七, 十月)於外點之備份主機執行資料回復測試，確保備份媒體及資料之正確性

二、個人資料部分

(一)資料：

公司提供可燒錄式光碟片給有需求之各個員工可燒錄其檔案，及 E-MAIL 資料。

(二)E-MAIL：

個人之重要資料可存放於公司之 File Server 中, 由公司統一備份.

三、媒體輸出部分

(一)定義：

公司相關部門為因應政府機構、銀行等需使用以電子媒體作傳輸作業者。

(二)各部門於執行其業務後，將磁片等交至資訊部登錄，資訊部需設簿記錄媒體編號、資料檔名、存放位置及送達處所等。

四、銷毀部分

重要及機密性之財務會計及營業資料逾法定保存限欲銷毀者，依「資訊管理作業 MS-10」規定，經部門主管核准後，會同稽核人員執行。

第六章：災害復原

訂定日期：91.07.15

第一條、目的：

對於災害發生時，能採取事先訂定之步驟及因應措施，並按既定之復原程序作完整而有秩序之復原，以減少因災害而造成之損失至最低程度。

第二條、防範措施(可降低風險)：

透過適當的風險評估分析而得適當之防範措施，風險評估之步驟及目標為：

(一)可能之威脅及弱點，包括

1. 不當之電腦及資料安全性
2. 電腦機房及相關設備防衛不足
3. 不當之水災、火災預警/防護措施
4. 重要區域擺置易燃物等危險物品
5. 不當之緊急防護措施
6. 不當之資料備援計劃
7. 重要文件及資料無廠外備份

(二)潛在的災害影響，包括

1. 公司收益的損失
2. 市場佔有率的損失
3. 業務機會的喪失
4. 災害的賠償

(三)確認重要資源，包括

1. 電腦設備
2. 各項作業準則及操作程序
3. 各項維護合約正式文件
4. 資料之備份

(四)列出恢復策略，包括

1. 備援之辦公作業環境
2. 備援之各項備份資料之相關文件合約及程序

(五)風險降低之措施，包括

1. 機房等重要地區安全管制
2. 機房及重要設備環境安裝滅火器
3. 安裝不斷電設備，維持電腦及通訊設備之運作
4. 進行緊急應變措施訓練及測試
5. 評估及測試資料備份之完整性
6. 相關重要文件於廠外備份儲存
7. 擬定災害復原程序

＊ 防範措施由 MIS 資管單位負責協調、擬定、維護及執行

第三條、重要資源之準備：

災害復原之能力除詳盡之復原程序計劃外，完全依賴於相關重要資源之有效性，各有關人員必須切實負起維護其完整性有效性的責任。

重要資源包括：

一、執行每日之資料備份

二、以圖案文件或檔案副本方式同時於廠外存放

三、復原計劃：計劃因需要而更新

第四條、復原程序：

一、立即採取應變措施訂定處理原則(資訊部)

1. 資訊部於災變發生時，應立即通知相關電腦及通訊設備廠商至現場檢視受損狀況，提出維修報告並儘速安排修復。
2. 由資訊部通知各相關部門開會，並報告損失狀況及影響作業層面。
3. 準備各項相關資料，如需要則收集置於廠外之各項備份副本。
4. 立即評估網路通訊損壞情形，並聯絡電信局修復事宜。
5. 調查受損資料之影響層面，並研討如何與備份資料銜接，採取補救措施。
6. 訂定回復程序及所需時間。
7. 檢討各項安全防護及管制作業，儘速採取改進措施。

二、成立災害復原作業執行小組

1. MIS及各部主管及執行人員擔任成員。
2. 立即召開小組會議並請相關設備提供廠商參加。
3. 災害復原作業分工。

三、訂定復原作業程序並執行：

1. 成立執行小組。
2. 災害評估，估計恢復各作業所需時間及完全恢復正常處理作業所需時間。
3. 作業中斷影響評估。
4. 內部資源需求決定。
5. 內部支援策略。
6. 災害復原計劃執行。
7. 檢討及撰寫報告。

第五條、電腦中心災變處理程序

一、範圍：

(一)硬體設備

1. UPS 供電設備
2. Switch / Hub：網路交換式集線器/集線器
3. Router：ADSL 路由器
4. ERP Server
5. File Sever.

(二)系統軟體

1. Linux 作業系統
2. oracle ERP 系統
3. HR 系統

(三)日常資料

交易記錄：DATABASE RECORD

二、程度：

1. 一級災害：主機設備及系統均毀損，無法自行修補
2. 二級災害：主機或應用系統毀損
3. 三級災害：交易記錄毀損

三、內容：

(一) 防範作業

1. 備份作業

A. 每日例行性備份：依公司行事曆排定執行時程並固定於每晚自動執行備份。

B. 每次備份均由系統產生備份記錄。

C. 定期將備份資料執行資料回復測試，確保備份媒體及資料之正確性。

D. 工具軟體燒錄：日常作業必須使用之合法軟體、驅動程式另以燒錄機將資料存於光碟片集中放置。

2. 系統檢測

A. 主機系統：每日一早均執行系統，查驗 ERP SERVER/WEB SERVER 是否出現異常訊息、主機運作是否正常，若有錯誤，執行者填寫檢測記錄。

B. InterNet：隨時偵測公司內外部 E-mail 是否暢通。

(二)因應措施：

1.災害通報

A. 災害通報：

以人事單位為災害通報中心，若為颱風、水災等可預期之災害，應由人事主管發出通告、各單位提前防備；若發生突發性災害如地震、火災時應以各樓層為單位、聽從各級主管指揮，人事主管立即對外聯絡消防勤務中心、對內進行廣播、啟動警報系統。

B. 受災區斷電：

為避免Client端個人電腦受損，強制關閉受災區域電源，啟動各樓層的備用照明。

C. 例假日處理：

各部門主管為主要負責人，接獲通報應立即趕至現場並成立臨時指揮中心協助救災工作。

2.緊急停機：

A. 災害尚未擴及機房時，應循正常程序關閉主機再拔掉電源插座、關閉冷氣機。

B. 將機器移至較安全之處。

C. 災區位於機房附近時，應儘速進入機房直接關閉主電源。

3.資料搶救：取出備份磁帶。

4.安全疏散：循指定的疏散方向迅速離開現場。

5.災情呈報：待警報解除後，應清點電腦中心設備、各單位保管之個人電腦及週邊設備受損情形，作為資源調配或修繕統計之參考。

(三)復原計劃

1.設備測試

A.恢復供電

A-1.穩壓測試：以測試用個人電腦接上UPS，啟動UPS不斷電系統進行監控。

A-2.主機供電：逐一將主機週邊接至不斷電系統，監控負載及穩定度；確定部份供電正常，再將主機電源接上

B.通訊設備

檢測數據機功能，啟動Router試著與ISP連繫，若無法連線則立即通知ISP廠商更換設備

C.網路設備

A-1.Client 端網路接線損壞，應重新拉線或更換接頭。

A-2.開啟各樓層及機房 Switch/Hub，檢查集線器是否故障，若無法以跳接方式解決則應報請送修或更換新品。

A-3.檢測各樓層網路印表機、印表連接埠訊號。

D.電腦週邊

A-1.試著單獨開機以觀察設備運作是否正常。

A-2.逐一開啟主機，觀察其元件運作，若出現異常應立即維修。

A-3.監視主機串連之週邊與主機間的訊息傳遞。

2.備援系統：選取 Client 端與主機同等級之個人電腦作為備援用主機，再加裝原主機硬碟作為備援系統。

3.一級災害

A. 當主機設備及系統毀損時，首先啟動備援主機使用原硬碟開機進入系統或重新安裝系統。

B. 決定系統資料時點，將備份資料寫回主機。

C. 通知各單位資料負責人查核、重建資料。

4.二級災害

A. 主機系統：執行自動修護程式修補錯誤。

B. 應用系統：重新安裝或將備份資料寫回主機。

C. 通知資料負責人查核、重建資料。

5.三級災害

A. 交易記錄、郵件資料毀損時，取出備份日期最近的備份寫回主機。

B. 通知單據負責人查核、重建資料。

C. 將遺失的郵件重新傳遞。

6.異常報告：針對災害發生之原因及處理情形呈報給上級主管，除了復原處理呈序外對於受害較嚴重的部份應提出特別說明，藉此檢討電腦中心之應變能力。

第七章：網路申報公開資訊處理程序

訂定日期：91.12.01
修訂日期：96.08.17
修訂日期：99.11.08

第一條、目的：

為確保網路申報公開資訊之管理及具體作業，特訂定此程序。

第二條、適用對象：

凡使用電子憑證之部門主管及經辦。

使用單位	單位主管	經辦	憑證保管人	憑證編號	資料保存
股務單位	阮成琦	高巧燕	阮成琦	993460-2	高巧燕
財會單位	阮成琦	廖淑美	阮成琦	993460-1	廖淑美
稽核單位	李沛霆	陳俊男	阮成琦	993460-2	陳俊男

第三條、申報程序：

一、申請：

經辦填具「使用印鑑證照請准單」，並檢據上傳資料，呈請單位主管核准。

二、核准：

單位主管核准後交予經辦「電子憑證」上傳資料。

三、網路申報資料：

上傳後應將網路申報資料，統一歸檔並保存五年。

第四條、 應公告或向證期會申報項目，由負責申報單位隨時檢視。