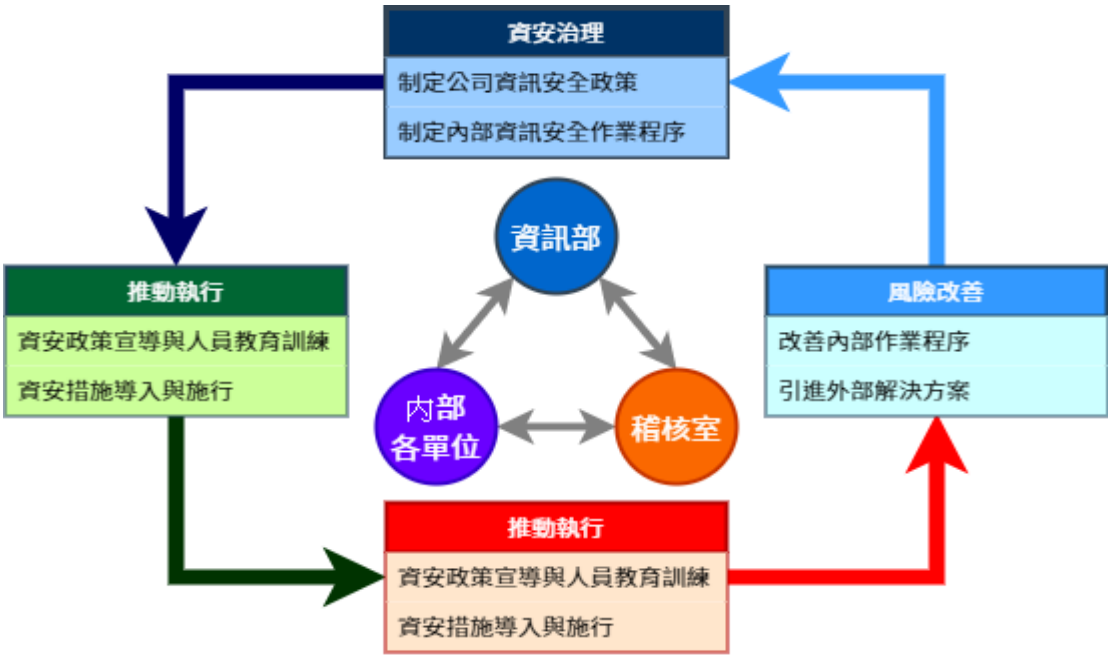
# 資訊安全政策及管理方案

## 資訊安全管理

資訊安全風險管理架構

- 本公司資訊安全之權責單位為資訊部，該部設置資訊主管乙名，與專業資訊人員數名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，並定期報告公司資安治理概況。
- 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，與專職稽核人員數名，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
- 組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



資訊安全政策及具體管理方案

本公司資訊安全管理機制，包含以下三個面向：

（一）制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

（二）科技運用：建置資訊安全管理設備，落實資安管理措施。

（三）人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識。

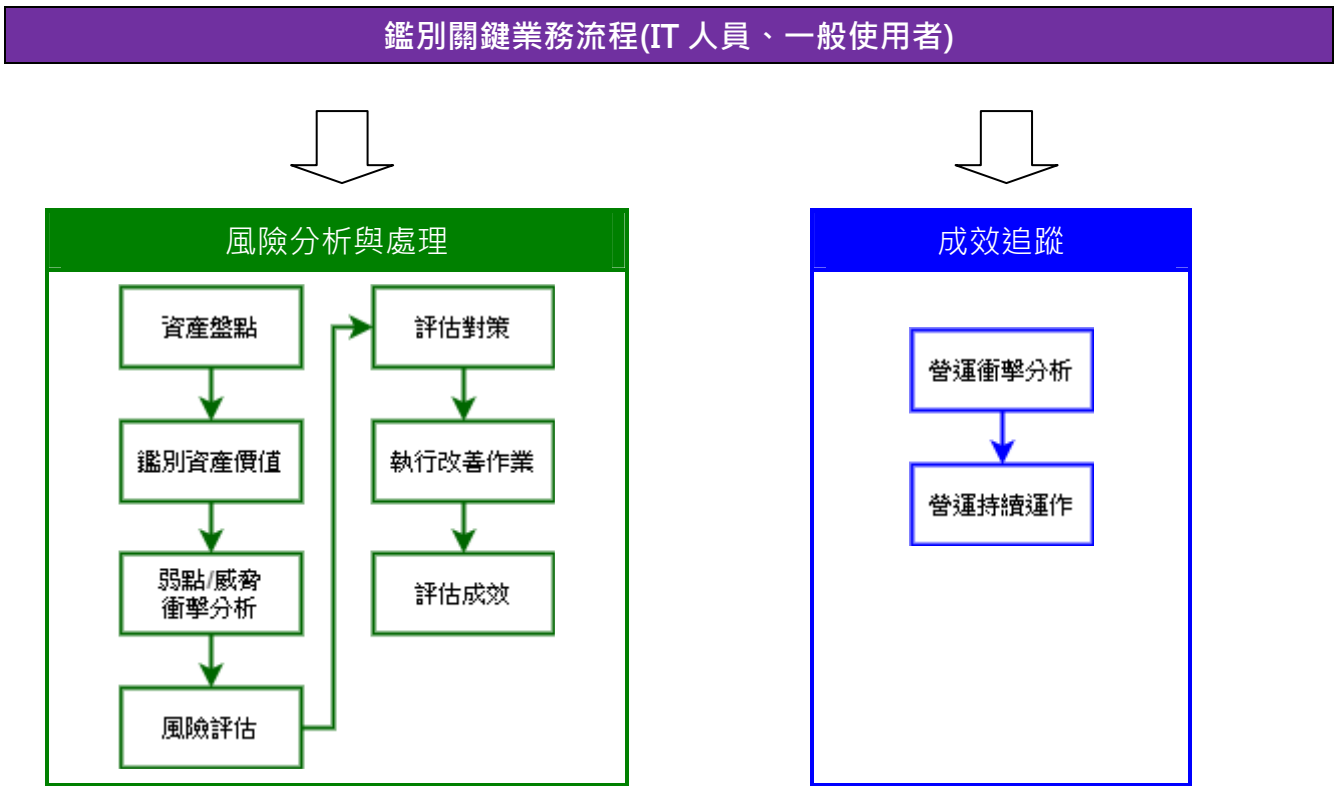
管理措施說明如下：

- 制度規範：本公司內部訂定多項資安規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。
- 科技運用：本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦設計作業程序和導入資安系統工具，落實人員資訊安全管理措施。
- 人員訓練：本公司每季定期實施新進人員資訊安全教育訓練實務課程，並建置數堂線上學習 (E-Learining) 資訊安全課程，藉以提昇內部人員資安知識與專業技能。

資訊安全管理措施

本公司定期審視內部資訊安全規範並報告資安治理概況。

本公司資訊風險評估程序如下：

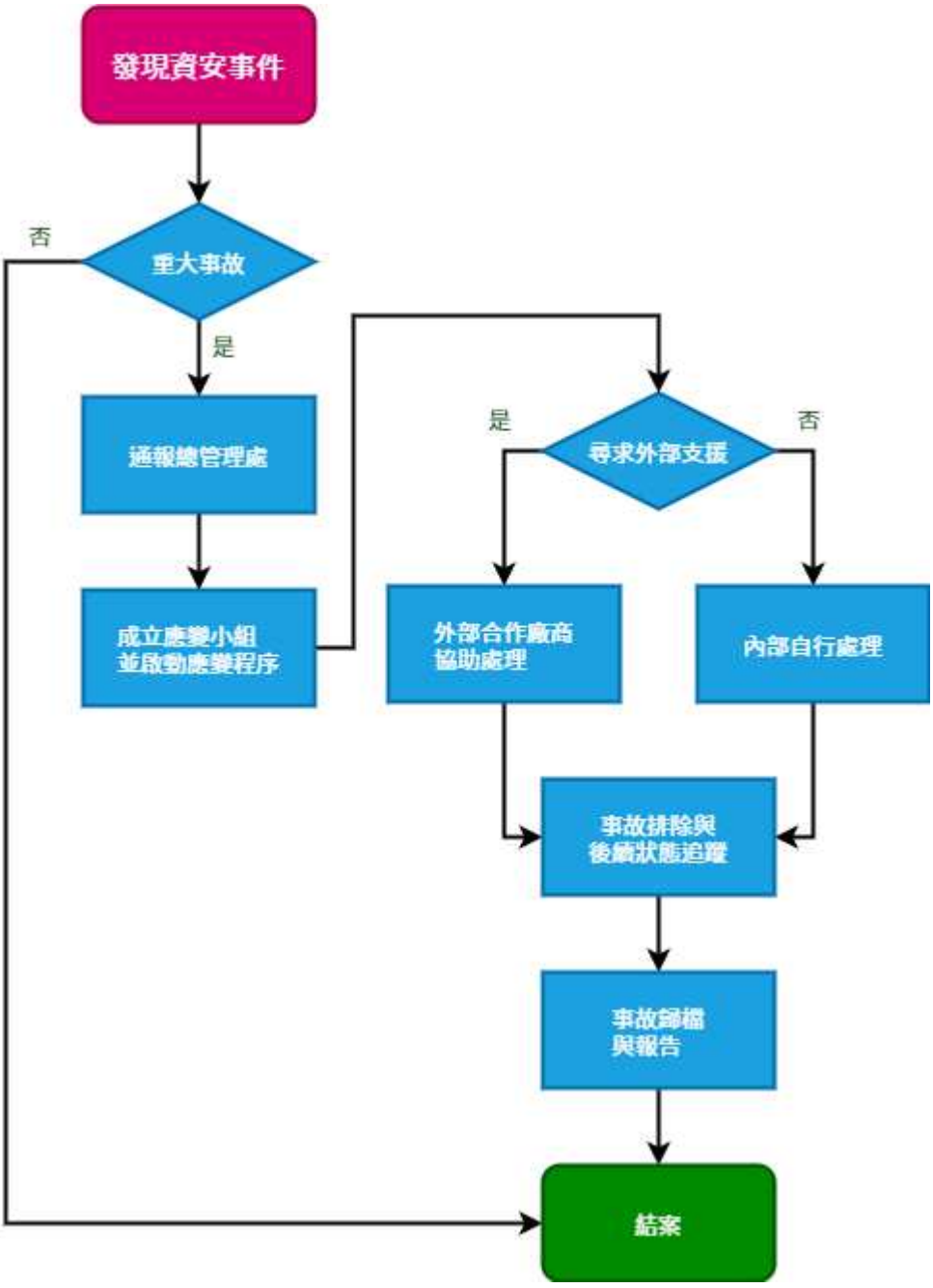



本公司實施之資訊安全管理措施，包含如下：

| 資訊安全管理措施 | | |
|---|---|---|
| 類型 | 說明 | 相關作業 |
| 權限管理 | 人員帳號、權限管理、與系統操作行為之管理措施 | 人員帳號權限管理與審核<br>人員帳號權限定期盤點 |
| 存取管控 | 人員存取內外部系統、及資料傳輸管道之控制措施 | 內/外部存取管控措施<br>資料外洩管道之控制措施<br>操作行為軌跡記錄分析 |
| 外部威脅 | 內部系統潛在弱點、中毒管道、與防護措施 | 主機/電腦弱點檢測及更新措施<br>病毒防護與惡意程式偵測 |
| 系統可用性 | 系統可用狀態,與服務中斷時之處置措施 | 系統/網路可用狀態監控及通報機制<br>服務中斷之應變措施<br>資料備份備援措施、本/異地備援機制<br>定期災害還原演練 |

資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。



# 三商投資控股股份有限公司
# 資訊安全管理辦法

## 壹、資訊安全管理管理規範

### 第一章、總則

第　一　條（制訂宗旨）

確保本公司資訊安全之作業,並保障本公司電腦處理資料之機密性與完整性，制定本辦法。

### 第二章、適用範圍

第　二　條（適用範圍）

本辦法適用範圍為本公司所屬各事業部門(含未公開發行子公司)對於資訊系統使用的安全規範，悉依本辦法之規定；本辦法未規定者，適用其他規範之規定。除特定作業之另行頒佈不適用聲明外，相關資訊安全細則的產生均以此為資訊安全辦法基準。

### 第三章、資訊安全組織及權責

第　三　條　資訊安全辦法、計劃及技術規範之研議、建置及評估等事項，由總管理處權責單位負責辦理。資料及資訊系統之安全使用及保護事宜由各業務行政單位依本辦法負責辦理。必要時，得委外由專家提供資訊安全顧問諮詢服務及技術支援協助。

第　四　條　稽核作業的執行及管理事項的追蹤由稽核權責單位負責辦理。

第　五　條　高層主管應授權資訊安全方案職務負責人員,就資訊安全方案之健全與相關法規之適法性，主導建立各資訊系統的資訊安全控制點。各資訊負責人員亦有義務配合建立相關的資訊安全控制點。

### 第四章、資訊安全政策的評估

第　六　條　資訊安全政策、管理規範及相關管理辦法應每年定期進行獨立及客觀的評估，以反映資訊安全管理政策、法令、技術及單位業務之最新狀況，確保資訊安全實務作業之可行性及有效性。

### 第五章、人員安全管理及教育訓練

第　七　條　對於資訊相關職務及工作，應進行安全評估，並於人員晉用、工作及任務指派時，審慎評估人員之適任性，並進行資訊安全考核。

第　八　條　新進人員於報到時，需依照規定填寫到職單，並簽署保密協定。保密協定涵蓋期間包括從業期間與離職後，均有保密之責任，任何因未遵守本資訊安全管理規範導致之資訊安全意外事件將嚴格懲處。

第　九　條　委外開發維護之廠商人員,必須簽署保密協定及切結遵守本資訊安全管理規範之規範。

第　十　條　各單位離(休)職人員，須依照人事規定填寫離職單，資訊處接獲通知後，應立即取消各項資源存取權限，始完成離職程序。

第 十一 條　新進人員應施以適當的系統操作訓練，避免使用者不當之操作。

第 十二 條　資訊系統之設計、管理、維護與操作人員，應適當分工，委派權責，並視需要建立人力備援制度。

第 十三 條　所有人員、須接受資訊安全權責單位所辦理的資訊安全教育訓練或確實了解資訊安全宣導事項，以建立全體員工資訊安全之認知，藉以提升全體員工資訊安全水準。

**第六章、資訊資產安全管理**

第 十四 條　應建立資訊系統資產等級之分類，以及相對應之管控層級作業。

**第七章、資訊系統管理**

第 十五 條　應採行防範及保護措施，以偵測及預防電腦之惡意軟體或行為之危害，確保系統正常運作。

第 十六 條　所有資訊系統資產的新增、刪除與修改皆須保存記錄，並依其所應保存層級保存之。

**第八章、 網路安全管理**

第 十七 條　與外界網路連接之網路，應以防火牆及其他安全設施，控管外界與本公司對組織內部的網路傳輸與資源存取。

第 十八 條　對於通訊設備的新增、變更與使用等作業須設置控管措施，以避免遭未經授權之存取或使用而致使資訊遭竄改、損毀、揭露及影響設備的穩定性。

第 十九 條　為預防網路設備使用或中斷，須定期維護網路系統之可用性，避免因無法取用網路資源而發生漏失。

**第九章、 存取控制**

第 二十 條　組織人員職務調整及異動時，應依資訊系統存取授權規定，調整其資源存取。

第二十一條　對於以遠端登入方式進行系統維修者，應加強安全控管，並克盡其安全保密權責。

第二十二條　為保護資訊處理系統的完整性，控制變更程序有其必要。系統變更及手動程序改變都須有控制變更程序。

第二十三條　員工須依照公司規定安裝及使用軟體，以避免造成資源或資訊之不正當使用。員工對於使用的軟體應為執行組織業務行為而使用之。

第二十四條　各單位須依據智慧財產權之相關規定，以避免因未取得或超出廠商授權之軟體，而引起的訴訟或糾紛。

**第十章、 實體及環境安全管理**

第二十五條　為保護資訊處理中心免遭實體傷害，應建立門禁管控。

第二十六條　系統伺服器應安置於機房內，並由資訊作業人員專責管理，並管制相關人員進出及記錄。

第二十七條　主機應安裝適當於安全偵測及防制設備、各項安全設備應依廠商的使用說明定期檢查。

**第十一章、 業務永續運作計劃管理**

第二十八條　各單位開發之資訊系統於上線運作後，應對該系統之原始程式碼進行備份2份，進行異地儲存保管。

第二十九條　評估各種人為及天然災害對公司正常業務運作之影響，訂定緊急應變及回復作業程序及相關人員權責，並視調整更新計劃

**第十二章、 資訊系統使用記錄**

第 三十 條　所有資訊系統的使用，須落實保留使用紀錄。

第三十一條　資訊系統使用記錄的保存，須符合企業需求以及主管本公司相關法規要求。

**第十三章、施行日期**

第三十二條　本辦法自 104 年 1 月 1 日起施行。

## 貳、資訊安全管理執行要點

### 第一章、 資訊系統作業及管理

(一)、資訊處理部門之功能及職責劃分

1. 總管理處，負責本公司所屬各事業部門(含子公司)之資訊評估、整合及建置等事項。
2. 資訊處其部門組織劃分為「資訊管理課」及「資訊研發課」。
3. 資訊管理課主要負責機房硬體、網路管理、資訊設備採購及門市設備維護處理。
4. 資訊研發課主要負責軟體評估、設計、程序開發及測試。其所屬人員依系統別劃分，並指派專人負責。

(二)、系統開發及程式修改之控制

1. 系統需求之發起，由各事業單位依需求提出，且經該事業單位主管簽核，交資訊處編號列管。
2. 資訊處依需求評估適合的系統架構及開發工具，並且評估自行開發或委外開發。
3. 系統架構區分為 Client-Server 架構及 3-Tire 架構，依所需之架購採用適合之開發工具。
4. 資訊處需建置相對應的測試環境，提供使用者進行測試。程式上線前需經使用者測試無誤，才可依上線計畫進行啟用。

(三)、編程系統文書之控制

1. 系統開發時，需撰寫系統文件及操作手冊。
2. 接獲修改需求時，需將修改內容記錄於需求單上，以利後續追蹤。
3. 系統文件及操作手冊，得以電子檔型式儲存及發佈。

(四)、資料輸入及處理之控制

1. 使用者使用程式，需登入帳號密碼，經驗證無誤後，始可登入執行。
2. 系統需依使用者職掌，設定可使用的程式權限。
3. 使用者於系統執行重要資料的新增修改，需記錄異動人員資訊。
4. 程式於處理重要的號碼，需經過檢核計算，避免寫入錯誤的資訊。
5. 所有使用者，得經由程式權限控管，產生已定義好的格式資料。若要取得非定義的資料，皆需填寫系統需求單，並經事業單位副總級以上主管簽核，始得執行。

### 第二章、網路安全規劃與管理

(一)、網路安全規劃

1. 電腦網路規劃為內部網段、DMZ、及外部網段，其間以防火牆區隔。
2. 內部網段完全與外界隔絕，外部網段不得直接存取內部網段；由 DMZ 區網段對內部網段之存取，限定於單點對單點在特定通訊協定(經防火牆)的方式下連結。
3. DMZ 區網段需明確限定允許之通訊協定（如 HTTP、FTP）對 Internet 開放。

4. 不開放 Internet 對 DMZ 區網段 TELNET 之通訊協定。
5. 網路安全相關的記錄檔案訂有保存規範。
6. 定期審閱網路安全相關的記錄檔案。
7. 專人負責管理與網路安全相關的記錄檔案。
8. 網路安全相關的記錄檔案需可以追蹤駭客入侵的證據。
9. 定期檢討網路安全控管事項之執行。

(二)、網路服務之管理

1. 設置網路系統管理人員負責網路管理。
2. 網路系統管理人員應負責系統安全規範的擬訂，執行系統管理工具之設定與操作，確保系統與資料的安全性與完整性。
3. 如果網路系統使用者已非合法授權的使用者時，系統管理人員應立即撤銷其使用者帳號；離（休）職人員應依本公司資訊安全規定及程序，取消其存取系統之權利。
4. 網路系統管理人員除依相關法令或本公司規定，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。
5. 如有發現任何網路安全事件，應及時通知相關網路系統管理人員進行處理，並向主管報告；如果事情無法獨立處理，需迅速連絡相關廠商或其他電腦安全事件緊急處理小組反應。
6. 系統管理人員不得新增、刪除、修改 LOG 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。

(三)、網路使用者之管理

1. 員工利用網路使用任何電腦資源，均需恪遵被授權的權限。
2. 員工應遵守公司網路安全規定相關規定，並確實瞭解其應負的責任，以免發生違反網路安全情事，遭致懲處。
3. 員工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. 員工不得以任何方法竊取他人的登入網路的身份識別與路通行碼。
5. 員工不得以任何儀器設備或軟體工具竊聽網路上的通訊。
6. 員工不得將色情檔案建置在本公司網路,亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。
7. 員工不得發送電子郵件騷擾他人，導致其他使用者之不安與不便；亦不得發送匿名信，或偽造他人名義發送電子郵件。
8. 員工不得以任何手段蓄意干擾或妨害網路系統的正常運作。
9. 非本公司員工需經授權後才得使用網路及電腦資源，並須遵守員工使用網路之一切規定。

(四)、主機安全防護

1. 機密性及敏感性資料之大型主機或伺服器主機，應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。
2. 為提升大型主機或伺服器主機連線作業之安全性，應視需要使用電子簽章及電子信封等各種安全控管技術，以建立安全及可信賴的通信管道。

(五)、防火牆之安全管理

1. 與外界網路連接的網點加裝防火牆，以控管外界與內部網路之間的資料傳輸與資源存取。
2. 防火牆為整個網路之樞紐，對於防火牆主機，應有一套備份，以因應一旦防火牆出問題之即時替代。
3. 防火牆之記錄檔(log)應由防火牆管理人員檢視分析有無異常狀況並定期備份。
4. 防火牆主機只能由內部系統登入，並設定登入密碼，以確保防火牆主機安全。
5. 防火牆之安全控管設定應經常檢討，並作必要之調整，以確定發揮應有的安全控管目標。
6. 防火牆系統軟體，應經常更新版本，以因應各種網路攻擊。
7. 防火牆只開放放必要的通訊協定，並限制可使用的時間，於非上班時間關閉對外的通道。目前只開放 HTTP、POP3、SMTP 等三個主要通訊協定，於晚上 23:00 到次日早上 7:00 關閉對外的通道。

(六)、軟體使用與控制

1. 員工不得經由網際網路下載非制式軟體使用，若需要下載制式軟體，亦應注意預防電腦病毒感染。
2. 員工不得使用來路不明之軟體，亦不得測試來路不明之軟體，以免引入「木馬」。
3. 員工於網路下載軟體使用之初期，應勤於掃瞄病毒，以確定下載軟體安全無虞。
4. 員工應全面使用防毒軟體並即時更新病毒碼。
5. 應即時公告有關病毒最新資訊。
6. 軟體需妥善保存授權證明、原版程式、使用手冊。
7. 訂定軟體採購作業程序，並建立軟體目錄且即時辦理軟體異動登記，軟體使用記錄和資料的儲存、處理和報廢的規則及使用記錄和資料的保存時限。
8. 指派專人負責有關個人資料保護法規之蒐集、公告、實施，全面依照「電腦處理個人資料保護法」規定辦理。
9. 經費許可下可使用適當稽查軟體工具檢查所有個人電腦內使用之軟體，確定個人電腦中只載入合法軟體。

(七)、網路資訊之管理

1. 對外開放的 web 資訊系統，所提供之資料內容由各事業部負責，總管理處負責設備及安全權限之設定。
2. 對外開放資訊系統的主機，應架設於 DMZ，並以防火牆與本公司內部網路區隔，提高內部網路的安全性。
3. 存放對外開放的 web 資訊系統的主機，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，以免影響服務品質。
4. 所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。

## 第三章、電子郵件之安全管理

1. 主機使用防毒軟體過濾信件，並設定主機禁止轉信功能，防止有心人士利用公郵件伺服器做非法信件的轉寄，而增加追查作業的複雜度。
2. 非本公司員工不得申請建立電子郵件帳號。
3. 郵件伺服器上需設定使用人員可使用的空間大小,及單封email可轉寄的人數，以避免而影響其郵件伺服器的正常運作。
4. 禁止以遠程終端機模擬的形式來開啟電子郵件，以避免因開啟帶有病毒的郵件需影響到系統的穩定。
5. 郵件信箱密碼需不定期更換,密碼需包含大小寫、符號及數字並不得小於七位，若密碼遺失則可申請重建密碼，並於三日內重建後告知使用者啟用。
6. 確實做好離職人員管制，人員離職需會簽總管理處，刪除其使用帳號。
7. 電子郵件伺服器主機需裝有防毒軟體，寄出及收入郵件皆事先經過掃毒。
8. 員工接收電子郵件後，應自郵件伺服器刪除以避免磁碟空間不足。
9. 不提供於公司外使用 Outlook 方式收發信件，必須使用 web 方式收發 email。

## 第四章、全球資訊網之安全管理

(一)、網路設備備援

1. 網路設備均應使用不斷電設備之電源，以防止不正常的斷電狀況並定期備援。
2. 防火牆主機需以另一同質主機，作成防火牆主機之備用主機，平常可做一般用途，一旦防火牆主機無法正常運作，即可以此備用主機取而代之，以避免整個網路癱瘓。
3. 規劃第二條專線，作為網際網路專線之備份，平常讓上傳及下載之業務分由此二專線各司一職，一旦其中一條專線無法正常運作，即可以將所有上傳及下載暫由另一專線負全責，使網際網路之運作全時不中斷。

(二)、網路入侵之處理

如發現網站遭入侵，應處理下列事宜。

1. 關閉專線對外之路由器。
2. 備份被入侵主機當時之系統，作為日後檢驗之用。
3. 聯絡廠商一同檢視被入侵之程度，決定後續處理之方式。
4. 全面檢討網路安全措施及修正防火牆的設定，以防禦類似入侵與攻擊。
5. 提出整個入侵檢討報告。

## 第五章、電腦機房管理

為維持電腦系統與資訊環境正常運作，並防止非法入侵本系統及非法攜出資料、設備，務必針對進出本室電腦機房之人員、物品及環境實施有效管理，特訂定「電腦機房管理手冊」。

機房安全管理，包括：門禁管制、安全防護、環境維護及系統作業故障排除等管理工作，並規範作業規定如次：

(一)、門禁管制：

1. 本機房應派有專職管理人員，負責管理門禁管制及相關安全防護措施。
2. 機房應備「機房進出管制表」、「廢品記錄表」。

3. 列表單詳載事項：

3.1「機房進出管制表」：確實記錄所有人員進出機房起訖時間。

3.2「廢品記錄表」：詳實記錄毀損需報廢設備、物品之名稱及數量。

4. 為加強管制及安全防護，本機房設置磁卡門禁管制系統，並列為管制區域。由資訊主管及機房管理員各持正、副卡管制門禁。
5. 機房管理員須明確告知獲准進出本機房人員所能執行的工作及禁止事項。
6. 本機房設備〈含軟、硬體等〉除機房管理員及合約廠商系統維護員，基於業務需要執行操作外，其它人員不得擅自操作。
7. 除維護或施工目的外，凡危險或易燃物品及器具均不得攜入本機房內，且非經資管主管核准不得攝影拍照。
8. 設備及物品之進出皆須填寫「電腦設備\物品出入紀錄表」。

(二)、安全防護：

為確保本機房內電腦設備運轉正常，務必確實執行本機房安全措施，以防意外發生，並在意外發生時，應及時因應，以減少損失。安全防護主要工作如下：

1. 本機房需保持標準之溫度〈二十二至二十六度〉及濕度〈四十至六十度〉，以維持電腦系統之正常運作。如發現異常，機房管理員應立即通知總務請廠商派員緊急處理。
2. 機房管理員應隨時注意電力、空調、消防及不斷電系統是否正常運作，如有異常立即通知檢修及採取應變措施。
3. 機房管理員應熟悉機房內各項安全設備〈如緊急電源、消防設備〉之使用方法。如遇火警，立即設法撲滅，並通知警衛及總務人員。若無法連絡到警衛及總務人員且未能即時撲滅，應撥一一九通知消防單位，鎮靜說清楚災變地點及起火原因。
4. 各項廢品應確實填具「廢品記錄表」並依規定分「機密性」與「一般性」送主管及財務部核定後分別銷毀，個人不得私自處理、拋棄或外帶。
5. 本機房內各種警示〈報〉系統應定期檢查〈每季至少檢查一次〉，以確保其功能。
6. 電腦設備以外的電器用品〈如電燈、電扇等〉，嚴禁使用不斷電系統所供應的電力。
7. 機房管理員應依規定管理及操作機房內各項設備之開關並確實執行資料備份及磁帶保存的工作。
8. 如遇緊急事故或電力維修或主機系統維修須關閉主機時，機房管理員須依正常程序關閉主機，並通知各樓層或事業部資訊窗口，並使用 E-MAIL 或 Intranet 系統中公告關機訊息。
9. 本機房門口應懸掛本手冊供參閱，所有進出本機房人員須確實遵守。

(三)、環境維護：

1. 進入本機房人員一律著拖鞋，以保持機房地板的清潔。
2. 本機房內嚴禁嬉戲、吸煙、飲食以及存放私人物品。
3. 本機房須隨時保持整潔，地板應定期打掃，廢報表紙應放置於指定容器內。
4. 本機房內各種設備手冊、儲存媒體應整齊放置於指定位置，不得任意堆放。

5. 本機房應定期實施防制鼠、蟲害等措施，以保持電纜及電腦等設備之完整。

(四)、系統作業故障排除：

1. 各主機系統遇有故障時，應立即由各系統負責人員研判故障類型，並先行設法排除，如無法解決時，應詳細記錄當時狀況及顯示之訊息後，立即就故障問題通知相關人員前來維修，如逾半小時無法修復時，應於 Intranet 系統中公告，如於兩小時內尚無法修復時，應通報主管得知相關訊息，並督促合約廠商儘快修復。
2. 系統修復完畢後應提出相關維修報告。

## 第六章、資料備份管理

資料備份是公司為了應變各種天災或是人為的破壞，導致公司的資料流失，造成公司無法正常的營運，為了防範必須訂出相關的管理辦法，遇到問題時能迅速反應各種問題。

(一)、資料儲存備份原則：

1. 異地備援機制:資料在此備份系統上儲存二份(一份儲存在本地節點，另一份在另一節點) 。
2. 總管理處製作一份備份存於磁帶中長久保存。
3. 資料以磁帶備份，分為星期一至星期五與防災備份兩種。
4. 備份方式分為完整備份與差異性備份兩種。
5. 備份內容分成資料庫備份與 system down 兩種。
6. 要完整記錄備份過程。
7. 定期實施資料還原測試並檢查資料是否維持完整性。

(二)、資料儲存備份執行：

1. 每日下午 17:30 人工執行各種資料備份，而自動排程備份排於凌晨執行。
2. 備份磁帶分為星期一至星期五與防災 A、B，防災備份於每星期五早上執行，單週執行 A、雙週執行 B。
3. SQL 資料庫備份由 SEVER 自動排程備份，透過網路傳輸至備份主機。
4. ORACLE 資料庫由自動磁帶機備份，每日自動循環備份。
5. 資料備份完畢後，隔天由單位主管帶回保管，再將前一天所備份的磁帶帶回公司，以達到異地備援機制。

(三)、備份維護：

1. 每月 5、10、15、20、25、30 執行磁帶清潔動作。
2. 每卷磁帶必須註明備份主機的內容與相關指令。
3. 每年必須更換新的磁帶，防止磁帶損壞或發霉。
4. 定期實施資料還原測試，確保備份資料的完整性。
5. 磁帶必須存放至乾燥的地方。

(四)、資料管制原則：

1. 資料借出必須經過單位主管的同意，並填寫資料借出申請單，送至總管理處審核由總管理處主管簽核後通知相關人員，將資料轉出後通知該人員完成借出手續。
2. 各系統負責人必須維護資料的隱密性，不可隨意透露相關資料內容。

## 第七章、系統復原計畫

當系統因任何突發意外事故，造成系統無法正常運作時，擬定異常事件處理程序，以增加處理時效，並減低異常事件發生之影響。

(一)、當機處理原則

1. 當系統主機發生無法正常運作，需先判斷其原因為何。將異常原因區分為「程式錯誤」「資料錯誤」「作業系統」「硬體設備」。
2. 「程式錯誤」及「資料錯誤」處理方式:由資訊研發人員找出問題，並提出修改程式方案，經相關人員確認後修改程式，避免相同問題再發生。
3. 「作業系統」處理方式:依據系統錯誤事件記錄，找出問題。若因軟體原廠(Microsoft、Sun)程式漏洞問題，需進行版本更新時，需先完成資料及程式備份後，始可進行。
4. 「硬體設備」處理方式: 依據系統錯誤事件記錄，找出問題。若為硬體設備，如記憶體，硬碟或主機板等問題，則盡速依報修程序，通知維護廠商到場處理。

(二)、系統復原處理原則

1. 當系統主機發生無法正常運作，且經排除問題後，必需重新安裝系統時，須先保存錯誤記錄，以便找出系統損毀原因。
2. 發佈系統維護公告，並註明預計修復完成日期時間。
3. 重新安裝系統時，需確認備援資料版本，及硬體設備規格和穩定性皆無問題，始可將備援資料回復。
4. 完成復原後，需請系統負責人及業務單位窗口，依檢核表進行系統測試。並確認系統版本及回復之資料皆無誤後，始可通知使用者上線。並且填寫復原報告。
5. 依所回復資料的截止日，判斷是否有需補登資料，若有通過相關業務單位需於限時內完成補登。