# 陸海股份有限公司
# 電腦化資訊系統暨資安管理辦法
# 目　錄

# 依據

依據「公開發行公司建立內部控制制度處理準則」第九條，使用電腦化資訊系統處理者，其內部控制制度除資訊部門與使用者部門應明確劃分權責外，至少應包括之控制作業（共十一大項）。本辦法內容對照該處理準則分為十一章。

# 第一章 資訊部門之功能及職責劃分

## 一、資訊部門功能

- 擬定公司資訊科技發展短、中長期藍圖
- 協助公司資訊化的推動、訓練與導入
- 公司現行資訊系統的維護與改善
- 新系統的開發（或取得）與現行資訊系統的功能擴充
- 資訊通訊安全的控管與內部宣導
- 適時提供透明詳盡的營運資訊供各層級主管參考
- 電腦執行績效的持續性監控
- 提供公司內部同仁資訊系統使用諮詢與協助
- 安排資訊相關課程

為擬定公司資訊科技發展藍圖，應需持續對公司內部做需求調查，及對新興資訊科技之機會與問題的評估，以利適時進行「資訊科技架構」的規劃與修正，並期望達到以最低之成本與最有效之方法取得資訊科技的產品或服務，及針對提昇品質淘汰舊科技訂定優先順序。

## 二、資訊部門職責劃分

### (一) 資訊部門編組，一般區分為

1. 應用系統組
   - 負責公司應用系統的規劃、開發（或取得）、導入與維護。
   - 提供負責公司內部同仁資訊系統使用諮詢與協助。
2. 基礎建設組
   - 負責公司網路、系統、硬體及週邊的建置、管理與維護。
   - 協助資訊資產的採購、管理與處置。
3. 資通安全組：職掌說明，參第十章第二節「資通安全政策及推動組織」內容說明。

### (二) 資訊部門職責劃分

- 資訊部門職責劃分，詳見「附件一、資訊部門職責劃分表」。
- 工作項目異動或任務編組改變，須及時更新「附件一、資訊部門職責劃分表」，並保

留相關修改紀錄於資訊部門備查。

- 任務編組與人員對照，由資訊部門主管指派，並保留相關修改紀錄於資訊部門備查。

### （三）委外系統管理控制

另依資訊部門或承辦單位與協力商之協議或合約規範辦理。

# 第二章 系統開發及程式修改之控制

## 一、系統開發工作編組

進行系統開發時，參與人員應適當的工作編組，主要職務區分如下：

- 資訊部門專案負責人
- 系統分析師
- 程式設計師
- 測試人員
- 需求單位專案負責人
- 需求單位作業人員

## 二、系統發展階段

需依據系統發展階段訂定合理的進度表，標準的發展階段及各階段的產出如下：

1. 需求調查與分析規劃
   主要編制文件：會議記錄、現況與需求調查相關文件
2. 概述設計與詳細設計
   主要編制文件：系統規格書、程式規格書、檔案規格文件
3. 程式撰寫與單元測試
   主要產出：程式碼及相關軟體元件（函式庫）
4. 整體測試
   主要編制文件：測試問題單
5. 系統轉換
   主要編制文件：系統操作手冊
6. 平行測試
   主要編制文件：問題記錄表

## 三、系統開發及程式修改工作說明

1. 需求單位依實際作業需求，在單位內自行評估與討論後，依簽核流程向資訊部門提出「資訊工作支援申請單」，或由資訊部門主動提出建議，或由承辦單位專案提報。
2. 需求單位自行律定一位窗口負責人，負責於系統發展過程中的協調溝通、測試與督促，資訊部門同時也指定一位窗口與之對應。
3. 資訊部門依據申請內容進行評估，並進行工作編組及依各發展階段訂定進度表。
4. 工作編組人員，依訂定的進度表執行系統開發的工作，規範如下：
   - 系統分析結果需經雙方專案負責人確認。
   - 系統詳細設計應考慮對程式、檔案的擷取提供必要的控制及足夠的稽查證跡。
   - 程式設計師於程式撰寫後，需自行進行單元測試。
   - 整體測試需由撰寫該程式以外的人員擔任。

- 系統上線初期，需設置足夠的平行測試時間，以確認新系統的可靠性。

5. 新系統平行測試期間，若所有發生的疑難皆已排解，則由需求單位進行驗收。
6. 系統正式上線後，由資訊部門負責日常程式維護、使用諮詢與疑難排解。
7. 各系統發展階段，皆應編制必要的文件資料。

## 四、系統開發及程式修改控制

系統作業環境區分為兩套主機，管控方式說明如下：

### (一) 正式主機

- 正式作業運行主機，使用者僅能透過終端連線方式，操作經由系統審核並給予權限範圍的應用程式。
- 使用者的系統權限由單位主管審核賦予，並依「資訊工作支援申請單」流程提出申請，由資訊部門管理人員配合設定。
- 最高權限帳號及密碼，僅由資訊部門專責人員保管設定。
- 系統版本更新與帳號建立等工作，亦由資訊部門專責人員負責。
- 程式設計與測試不得於此正式主機作業。
- 正式主機所存放皆為正式使用之應用程式與原始碼。
- 正式主機應放置於有門禁管制之獨立機房。

### (二) 備份主機

- 程式撰寫與測試所使用之備份主機，所有開發中含測試之應用系統皆於此主機內作業。
- 備份主機的使用為程式設計師與系統分析師，在必要的系統測試時才能開放權限讓使用者透過終端連線進入執行測試工作。
- 備份主機應置放於有門禁管制之獨立機房。
- 其餘系統開發及程式修改控制，由資訊部門主管依前述系統發展階段設立查核點，進行各階段產出內容的查核。

# 第三章 編制系統文書之控制

## 一、編制系統文書

系統建置從初期規劃到完成系統過程中之資訊工作支援申請單、訪談、會議、規格文件…等，皆須留存備查相關文書資料，系統文書資料區分如下：

- 資訊工作支援申請單
- 會議紀錄或需求調查相關文件
- 系統規格書
- 程式規格書
- 測試記錄
- 系統操作手冊

## 二、系統設計文書控制

- 系統設計文書文件，應保存於有權限管制的資料區內。
- 系統設計文書文件，僅限定與該系統有關之系統管理、系統開發、系統維護人員得以取出閱讀或新增入檔。
- 系統設計文書文件，未經資訊部門主管許可，不得任意外借與再製新副本，若需進行資料銷毀，則需以碎紙方式處理，不得以一般廢紙方式處理棄置。
- 系統設計文書文件，應儘量以電子化方式保存，並設定相關使用與修改權限。

## 三、系統操作文書控制

- 系統操作文書文件需按照職權分類管理與存放。
- 非業務相關人員，不能閱讀職責權以外的操作文件。
- 系統設計文書文件，應儘量以電子化方式保存，並設定相關使用與修改權限。

## 四、安全控制

- 程式之使用需於電腦中留存記錄。
- 系統程式及正式程式之設置，由系統人員安排，並將之登錄程式的名稱呈核列管。
- 依本管理辦法之「第九章、硬體及系統軟體購置、使用及維護控制」，對於各項電腦及其附屬設備、硬體與系統，需與廠商訂立協定，能於故障通知後，在一定時間內維護完成，並對空調、電源等電腦關連設備，設置適當之備援機制。
- 依本管理辦法之「第九章、系統復原計劃制度及測試程序控制」及「第七章、檔案及設備安全控制」，為確保主檔之復原，主檔內容需定期抄錄備份檔案，存於公司外較為安全場所保管。

# 第四章 程式及資料之存取控制

## 一、程式存取控制

### (一) 正式主機程式存取控制

- 程式的載入或取出，皆由負責該程式的管理人員執行。
- 程式管理人員的所有帳號應不定期更換一次密碼。
- 正式主機最高權限者的密碼，由資訊部門專責人員保管與設定。

### (二) 備份主機程式存取控制

- 當使用者提出程式修改需求時，由系統管理者將要修改的程式下載到備份主機，再由程式設計師執行修改的工作。
- 非經申請，一般使用者不得以任何理由或方法提出或取得原始程式的下載需求。

## 二、資料存取控制

### (一) 正式主機資料存取控制

- 正式主機應安置有門禁管制的機房，非系統管理人員或是系統備份人員，不得到主機存取任何資料。
- 資料的存取權限為公司所賦予的職責範圍，需利用終端電腦連線方式存取。
- 正式主機之終端連線僅限於總分公司網路連結，不能有任何形式之存在能為公司外部存取。

### (二) 備份主機資料存取控制

- 備份主機之資料，由正式主機複製而來，皆作為程式測試與備份測試之用途。
- 備份主機資料之存取方式亦與正式主機相同。

## 三、權限控制

- 使用者進行系統作業之前，需輸入帳號及密碼，經系統確認通過，方能使用系統。
- 使用者密碼至少每 6 個月更新一次，每年至少核對一次使用者使用權限。
- 依本管理辦法之「第三章、編制系統文書控制」，資料管理者，負責管理包含原始程式在內的所有檔案文件，未經授權任何人不可取閱。
- 依本管理辦法之「第二章、系統開發及程式修改控制」，程式設計及修改需提出申請手續，程式撰寫完成後需交由使用者驗收，且修改後的程式需製作電腦檔案歸檔。
- 於使用許可範圍內，需依不同對象區分只能閱讀或可以更改檔案的權限。
- 系統密碼及檔案密碼需分別由不同人管理。
- 依本管理辦法之「第七章、檔案及設備安全控制」，機房需設立門禁管制，檔案備份需異地存放。

# 第五章 資料輸出入之控制

## 一、應用系統資料輸出入之控制

- 資料的輸出入皆經由授權並由電腦控制。
- 未授權之資料輸出入等，系統功能將會無法使用。
- 重要的資料列印輸出，系統將作一記載存檔。

## 二、個人電腦資料輸出入之控制

- 不論資料的輸出或輸入，皆會經由防毒系統的掃描與確認。
- 個人不得任意將有關公司業務之資料，下載或輸出供為個人或其他非公司授權範圍之使用。

## 三、大量資料批次輸出入之控制

- 若有大量資料需批次輸入或輸出，需由資料管制人員負責。
- 資料管制人員需檢查這些輸入與輸出資料是否完整，或有無任何明顯之錯誤，以及控制總數，並檢查相關系統訊息以決定在處理過程中是否發生任何問題，例如不正常之操作中斷，或者是否使用了正確之檔案格式、資料、程式等，然後再將批次處理的結果交給使用單位。

# 第六章 資料處理之控制

## 一、硬體設備控制

為使電腦設備維持正常運轉，降低故障減少問題發生，有以下之控制活動：

- 機器啟動是由電腦機房值班人員依開機操作程序執行，並由開機記錄(Log File)及訊息確定開機過程是否正常，及機器是否順利運轉。若出現異常情況時，值班人員先行採取排除異常之應變措施。如無法自行排除時，則應立即通知維護廠商派員前來處理，並將處理過程加以記錄備查。
- 機器運轉中如發生異常狀況,系統人員先判斷是否會影響進行中工作,如需立即停機時，應立刻通知使用者暫停作業，並隨即進行修復。待修復完畢並運轉正常後，再行通知使用者重新使用。
- 機器故障損及資料時，值班人員先進行資料回復作業，並通知使用者自行查驗，避免影響日後資料之正確性及完整性。

## 二、系統軟體控制

對於資料輸出／輸入及處理過程透過系統程式控制，以減少問題發生並提高執行效率，其控制方法如下：

- 電腦作業系統、系統應用軟體及執行程序(command procedure)不得任意修改其內容或參數，以確保作業正確性。
- 設置適當之日誌檔(log file)，以記錄統計人員對於有關硬體啟動、停用、輸出、輸入之運作過程，及系統故障錯誤訊息之查核。
- 電腦作業系統、系統應用軟體等系統軟體之電腦備份作業，由系統管理人員依電腦資料備份及管理程序辦理。
- 管理者分「資料庫管理員」與「系統管理員」,需分不同人擔任，並擁有不同的帳號及密碼，系統管理員無資料修改、刪除之權限。
- 資料庫管理員不得任意直接更改資料。任何資料庫的資料直接更改，皆需有使用者依規定提出申請，或有關系統維護與除錯的問題依據。

## 三、應用軟體控制

對於資料輸出／輸入及處理過程透過應用程式控制，將不合理或遺漏的資料加以處理，以減小問題發生降低錯誤率，其控制方法如下：

- 於程式中依不同使用單位或人員之使用權限及目的設定其資料擷取範圍及內容、以確保資料隱密性。
- 合理化之檢查，如極限值、範圍的控制、檢查號碼、資料型態檢查、帳務數字平衡檢查、四捨五入的原則等勾稽方式，以強化資料正確性。
- 於執行應用軟體時，若有錯誤發生時應查閱錯誤訊息資料，以研判是資料或程式錯誤，若資料錯誤應依使用者更正程序辦理，如屬程式錯誤應通知程式人員依程式修改程序處

理。

## 四、資料庫的管理

- 資料庫的最高權限帳號的密碼，至少每三個月需做一次變更。
- 資料庫的存取，需依不同的用途與角色，設定適當的存取權限。
- 資料庫資料的修改，需依循「資訊工作支援申請單」的處理流程，由需求單位提出申請，並經由需求單位主管審核認可後，再交由資訊部門專人進行工作指派。
- 資料庫管理人員或系統人員需於接受到工作指派後，才能更改資料。
- 資料修改後，需經原申請單位測試與驗收。
- 資料室主管需定期核驗「資訊工作支援申請單」的處理記錄，並歸檔備查。

## 五、文件的存放與領用

- 所有文件皆應存於安全處所。
- 文件的取用均需留有記錄。

# 第七章 檔案及設備安全之控制

## 一、電腦機房門禁管制

為防止非法入侵、危險物攜入、非法攜出等，必須對進出電腦機房等重要區域的人員與物品加以管制：

- 電腦機房除資訊部門特定人員外，其他人員（含服務廠商）須經許可後，方可進入電腦機房洽辦工作。
- 電腦機房內之作業人員應確實遵守規定。

## 二、檔案存放安全控制

### (一) 使用媒體管理辦法

資訊部門根據消耗品使用狀況，適時適量添購磁帶、磁片、光碟片，新購之媒體由資訊部門之專責人員保管使用。

檔案備份之內容、保存期限、備份週期、異地存放地點等，皆應定期評估檔案備份程序與保存期限的正確性。

### (二) 電腦資料儲存之管理

- 電腦資料每日由專責人員作完全備份。
- 磁帶備份以五天為一個備份周期。
- 每週二次固定將備份磁帶送至銀行保險庫存放，並取回後續要備份的磁帶。
- 定期測試備份磁帶回復是否正常。
- 上述工作皆應設立日誌記錄，以利查核。

# 第八章 硬體及系統軟體購置、使用及維護之控制

## 一、資訊設備及系統購置程序

依公司內部預算編製及控制、支付請款單、及固定資產管理等相關程序辦理。

## 二、資訊設備及系統之使用及維護控制

### (一) 網路/資安設備、電腦主機及其附屬設備

- 電腦相關設備之維修，採每年定期與服務廠商簽訂維護合約，由服務廠商定期進行保養、檢修。
- 電腦相關設備發生異常時，資訊部門管理人員應立即通知負責之服務廠商，依照合約所規定的時間之內，到場或是遠端遙控的方式排除故障。
- 上述處理皆應留存記錄，供日後追蹤評估。

### (二) 其他設備

1. 電源系統
   - 電腦機房之電源為獨立之電源迴路，以確保電路穩定
   - 電腦專用插作務必有電源接地，不可外接其他用電設備，此外，結束使用電腦設備時，請同時關閉電源。
   - 機房不斷電設備功率，需足夠停電時，有充分的時間執行資料儲存與關機作業，以確保資料完整及系統安全性。
   - 電源發生異常狀況時，先由機房管理人員故障排除，如無法處理時，應立即通知維護廠商檢修，檢修過程應有記錄，供日後追蹤評估。
2. 空調系統
   - 需設置空調、空調備援設備，電腦機房之溫度每日皆有記錄控管。
   - 溫度控制為 20 度至 24 度之間，溼度控制為 45% 至 65% 之間。
   - 採定期維護或臨時叫修方式維護空調設備的可用度與可靠性。
   - 設備發生異常狀況時，先由機房管理人員故障排除，如無法處理時，應立即通知維護廠商檢修。
   - 維修過程應留存記錄，以供日後追蹤評估。
3. 消防設備
   - 除建築物本身符合消防相關法規的消防設備外，另設置電腦機房專用之滅火設備，以增加保障。
   - 電腦機房專用之滅火設備，需定期檢視，以確認在有效期限內。
4. 資訊通訊線路
   - 通訊線路發生異常狀況時，先由機房管理人員故障排除，如無法處理時，應立即通知電信服務廠商維修。
   - 短時間如無法修復時，為避免資訊通訊中斷，可以改採備援線路。

### （三）資訊資產之分級

資訊資產之資訊安全等級大致區分為二類：

- 一般等級：個人使用資訊設備，如個人電腦，歸使用者個人保管，多人共用週邊設備，如印表機等，集中於辦公室之開放區域。
- 機房管制等級：所有主機、集中式儲存設備、網路設備、資安設備等，皆置於電腦機房中，電腦機房內除設置不斷電系統、空調系統及消防系統外，另特別設置門禁刷卡系統，以管控非相關人員未經允許不得進入操作或參觀設備。

# 第九章 系統復原計畫制度及測試程序之控制

為確保主檔之復原，主檔內容需定期抄錄備份檔案，並依本管理辦法之「第七章、檔案及設備安全控制」，存於公司外較為安全場所保管。
復原計畫依災難程度不同，執行不同的復原方式與測試程序控制，以下區分為三種狀況：

## 一、主機硬體與系統正常，資料異常

處理程序如下：

- 主機依正常方式關機與開機後測試是否回復正常。
- 系統人員瞭解資料異常的區塊。
- 取得最近的備份磁帶。
- 針對異常資料區塊或整體資料執行磁帶回復。
- 系統重新開機並檢查資料是否可以正常運作。

## 二、主機硬體正常，系統運作不正常

根據系統畫面所呈現的訊息，判定故障原因同時故障排除。

## 三、主機硬體毀損不可使用

處理程序如下：

- 聯絡主機系統廠商備機，並建構與原主機相同形式規格的硬體與系統環境。
- 主機硬體載運就位後，取得最近備份的磁帶並回覆整個資料及應用系統。
- 全面性測試系統運作是否正常。

# 第十章 資通安全檢查之控制

## 第一節 本章總則

依據「上市上櫃公司資通安全管控指引」(共九大項)，本章內容對照該指引分為九節。

## 第二節 資通安全政策及推動組織

1. 資通安全組配置適當之人力、物力與財力資源，並指派適當人員擔任資安專責主管及資安專責人員，以負責推動、協調監督及審查資通安全管理事項。
2. 資通安全政策及目標由核決主管核定，並檢視政策及目標且有效傳達員工其重要性。
3. 資通安全作業，包含
   (1) 核心業務及其重要性
   (2) 資通系統盤點及風險評估
   (3) 資通系統發展及維護安全
   (4) 資通安全防護及控制措施
   (5) 資通系統或資通服務委外辦理之管理措施
   (6) 資通安全事件通報應變及情資評估因應
   (7) 資通安全之持續精進及績效管理機制
4. 所有使用資訊系統之人員,每年接受資訊安全宣導課程,另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。

## 第三節 核心業務及其重要性

1. 檢視公司之核心業務及應保護之機敏性資料。
2. 遵守之法令及契約要求。
3. 檢視可能造成營運中斷事件之發生機率及影響程度，並擬訂核心業務之復原時間目標(RTO)及資料復原時間點目標(RPO)，設置適當之備份機制及備援計畫。
4. 制定核心業務持續運作計畫，不定期辦理核心業務持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善。

## 第四節 資通系統盤點及風險評估

1. 不定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。
2. 不定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等。

## 第五節　資通系統發展及維護安全

1. 將資安要求納入資通系統開發及維護需求規格，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。
2. 不定期執行資通系統安全性要求測試，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾測試等。
3. 妥善儲存及管理資通系統開發及維護相關文件。
4. 對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。
   - 定期辦理弱點掃描。
   - 定期辦理滲透測試。
   - 系統上線前執行源碼掃描安全檢測。

## 第六節　資通安全防護及控制措施

1. 依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。
2. 具備下列資安防護控制措施：
   - 防毒軟體。
   - 網路防火牆。
   - 如有郵件伺服器者，具備電子郵件過濾機制。
   - 入侵偵測及防禦機制。
   - 如有對外服務之核心資通系統者，具備應用程式防火牆。
   - 進階持續性威脅攻擊防禦措施。
   - 資通安全威脅偵測管理機制(SOC)。
3. 針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。
4. 到職、在職及離職管理：應簽署保密協議明確告知保密事項。
5. 建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。
6. 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。
7. 資通系統及相關設備適當之監控措施，包含身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。
8. 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。
9. 留意安全漏洞通告，即時修補高風險漏洞，不定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。
10. 資通設備回收再使用及汰除之安全控制，以確保機敏性資料確實刪除。

11. 人員裝置使用管理，包含軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。
12. 不定期辦理電子郵件社交工程演練或宣導，並對誤開啟信件或連結之人員進行教育訓練或宣導。

## 各項控制作業如下：

包含系統防毒檢查控制、系統防火牆檢查控制、遠端登入、使用者權限規範，其餘前面章節已說明之內容，在此不再贅述。

### (一) 系統防毒檢查控制

- 主機系統須設置防毒系統，以監控與檢查進出資料是否有病毒存在。
- 電子郵件系統需設置防毒系統，以過濾信件中有無夾帶病毒等程式。
- 個人電腦皆需安裝防毒系統，以保護使用者電腦不受病毒破壞。
- 防毒軟體每日定時自動下載最新病毒碼，並同時派送到各電腦。
- 當發現病毒無法處理警告時，系統管理人員應即時隔離該中毒電腦，同時連絡電腦防毒廠商之技術服務人員，以取得處理的方式。

### (二) 系統防火牆檢查控制

- 對外網際網路的電腦系統須設置防火牆系統，以監控並防堵外面不明人士的惡意試探、竊取與破壞資訊系統。
- 防火牆系統由委外廠商提供專業維護服務，並依合約所載方式定期診察檢核公司整體資通安全的完整性。
- 當發生系統入侵事件時，應即刻通知維護廠商，依合約方式與時間要求排除相關事件，同時並留有維護記錄，以供日後備查。

### (三) 遠端登入

- 廠商遠端登入：平時不做任何開放，僅在系統異常或定期檢修須委外廠商提供專業服務時，再依委外廠商提供登入電腦的識別 IP 等資料進行設定後，方得以開啟防火牆的通道以利委外廠商遠端登入，且通道僅限於委外廠商通報之電腦，在維護完畢後，應立即關閉該通道。
- 同仁遠端登入:目前僅提供外點人員透過SSL VPN 設定,並由資訊部門配發識別 IP、帳號及密碼等資料後才可登入。

### (四) 使用者權限規範

- 使用者的系統權限由單位主管審核賦予，並依「資訊工作支援申請單」流程執行申請與建立，資訊部門依此執行相關設定。
- 針對人員之調動、離職或退休，經由人事單位之「人員異動申請單」或「離職申請單」核定後，交由資訊部門做相關權限變更設定。
- 針對離職人員之 E-mail 帳號，若業務上需做保留以利交接之情形，原則上最多提供 3 個月保留期，期滿後由資訊部門主動做移除或轉換之處理。

## 第七節　資通系統或資通服務委外辦理之管理措施

1. 資訊作業委外安全管理，包含委外選商、監督管理及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。
2. 委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協議、資安要求及對委外廠商資安稽核權。
3. 公司於委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

## 第八節　資通安全事件通報應變及情資評估因應

1. 資安事件應變處置及通報作業，包含判定事件影響及損害評估、內外部通報。
2. 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊。
3. 發生符合「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，將依相關規定辦理。

## 第九節　資通安全之持續精進及績效管理機制

1. 資通安全組應向管理階層報告資通安全執行情形，確保運作之適切性及有效性。
2. 不定期辦理內部及委外廠商之資安稽核，並就發現事項擬訂改善措施，且追蹤改善情形。

# 第十一章 公開資訊申報相關作業之控制

## 一、申報人員

由公司指定專人執行此項作業。

## 二、申報內容程序

1. 依政府機關規定之格式製作電子文件資料。
2. 將資料列印一份呈核主管單位批准。
3. 於規定時間內上傳與發佈公開資訊。

## 三、資料上傳程序

1. 申報資料使用政府機關所發給的憑證磁片與密碼進入規定的加密網站執行申報，申報的過程資料皆需經過加密程序。
2. 加密的機制、執行憑證磁片、操作密碼等，由被申報單位提供。
3. 通過網路加密驗證機制後，方可上傳公開資訊資料。
4. 操作密碼依規定時間更改。

## 四、驗證磁片與密碼

申報使用的憑證磁片及密碼皆由專人妥善保存保管，資訊部門同時協助保管憑證磁片的備份，但不保管密碼與其相關設定更改。

## 五、申報需依相關機關單位規定之申報流程與時間執行

# 第十二章 附則

一、 本辦法於民國 111 年 X 月 X 日經董事會核准後實施，修改時亦同