資訊安全政策

目　　錄

壹、目的

為確保各項資訊資產之安全，防止機密資料外洩及意外發生時之應變措施，以維護公司正常營運。

一、提供本公司資訊安全運作的環境。

二、發展資訊系統使用程序的長期指導方針。

三、鑑別資訊安全活動的基本評估方法，確保資源有效地運用於資訊安全活動。

四、提供資訊系統與網路設計的基礎架構需求與相關採購規格的依據。

五、為本公司資訊安全手冊的根本。

六、為本公司使用資訊系統的行為準則，經由有效的資訊安全教育訓練，讓所有同仁瞭解，以避免相關人員以不知行為準則為藉口，而做出違反本公司規範的行為。

七、為本公司內部稽核單位與人員稽核之依據。

八、為本公司認知與提出關於資訊資產在法律規章與契約上需求的依據。

貳、範圍

適用範圍為全公司，包含資訊軟硬體設施、資訊紀錄、內部使用者、外部使用者及作業流程。

一、軟硬體設施 ： 各種應用系統、各式主機、工作站、伺服器及個人電腦。

二、資訊紀錄 ： 資料庫內容、資料檔、系統規劃與設計文件、使用與操作手冊、生產機台設定參數、合約以及教育練教材等。

三、內部使用者 ： 本公司全體員工。

四、外部使用者 ： 各外派人員、客戶、委外製造廠及供應商

五、作業流程:環境控管程序、業務流程、研發流程、系統發展流程、內部控制管理辦法以及其他相關典章制度等。

參、目標

本公司資訊安全管理目標為保護資訊資產之機密性、完整性與可用性，簡稱 CIA：

一、 機密性（Confidentiality）：合法取閱資訊。

任何資訊儲存在本公司的資訊系統中、資訊系統在處理中或在傳輸線上均要維持其機密性。

（一）由遠端存取本公司 Intranet 資訊必須要有防範機制，以防在資訊傳輸途中被竊取。

（二）本公司內部資訊系統中，較機密的資訊（包括電子檔或紙本）亦要有適當的保護，以防非法存取。

（三）稽核紀錄保有重要活動的詳細資料亦要妥善保護，僅授權予適當人員存取。

二、完整性（Integrity） ：資訊或系統維持正確與完整。

任何資料儲存在本公司的資訊系統中、資訊系統在處理中或在傳輸線上均要保護，以防不當竄改及資訊系統在運作中被不當的操縱或入侵。

（一）由遠端存取本公司 Intranet 資訊必須要有防範機制，以防在資訊傳輸途中被竄改。

（二）本公司內部資訊系統中，較機密的資訊亦要有適當的保護，以防非法存取。

（三）資訊系統的存取權限、威脅與脆弱點要加以控管以維持其完整性。

三、可用性（Availability）：資訊或系統需要時即可取用。

確保資訊與系統持續運轉無誤，當合法使用者要求使用資訊系統時，例如：收／送電子郵件、OA 應用系統等，使用者均可在適當的時間內獲得回應，並完成服務需求，此可用性需與前二項機密性與

完整性配合一起考慮，以符合既定的目標；線上資訊加密或記錄稽查資料會影響系統回覆時間或引來阻斷式服務而造成無法符合可用性。

而上述三目標具體呈現與實際執行方式說明如后：

四、訂定具體安全目標

以CIA為基準，訂定相關安全目標，包括下列項目：

（一）降低應用系統錯誤數10% 。

（二）降低中毒次數10% 。

（三）維持重要主機系統設備可用度為99.5% 。

（四）降低其他資安事件次數10%，全年資安事件 < 2 件。

(五)避免人為疏失意外。

(六)防止人為意圖不當及不法使用。

(七)防止駭客病毒等入侵及破壞。

(八)維護實體環境安全。

(九)維持資訊系統持續運作。

五、訂定安全指標

依據安全目標訂定安全指標，可包括下列各項：

（一）應用系統錯誤數量（Bug number)。

（二）中毒事件次數 。

（三）重要主機系統可用度。

肆、政策聲明

永續經營是依賴資訊的完整性和持續的可用性，遵循資訊安全的規範可保護資訊免於未經授權的使用、修改、公開或破壞，無論這些破壞來自意外的或蓄意的，保護這些資產是全體同仁的基本責任：

一、 確保這些資產是只被運用在經管理階層核可的目的。

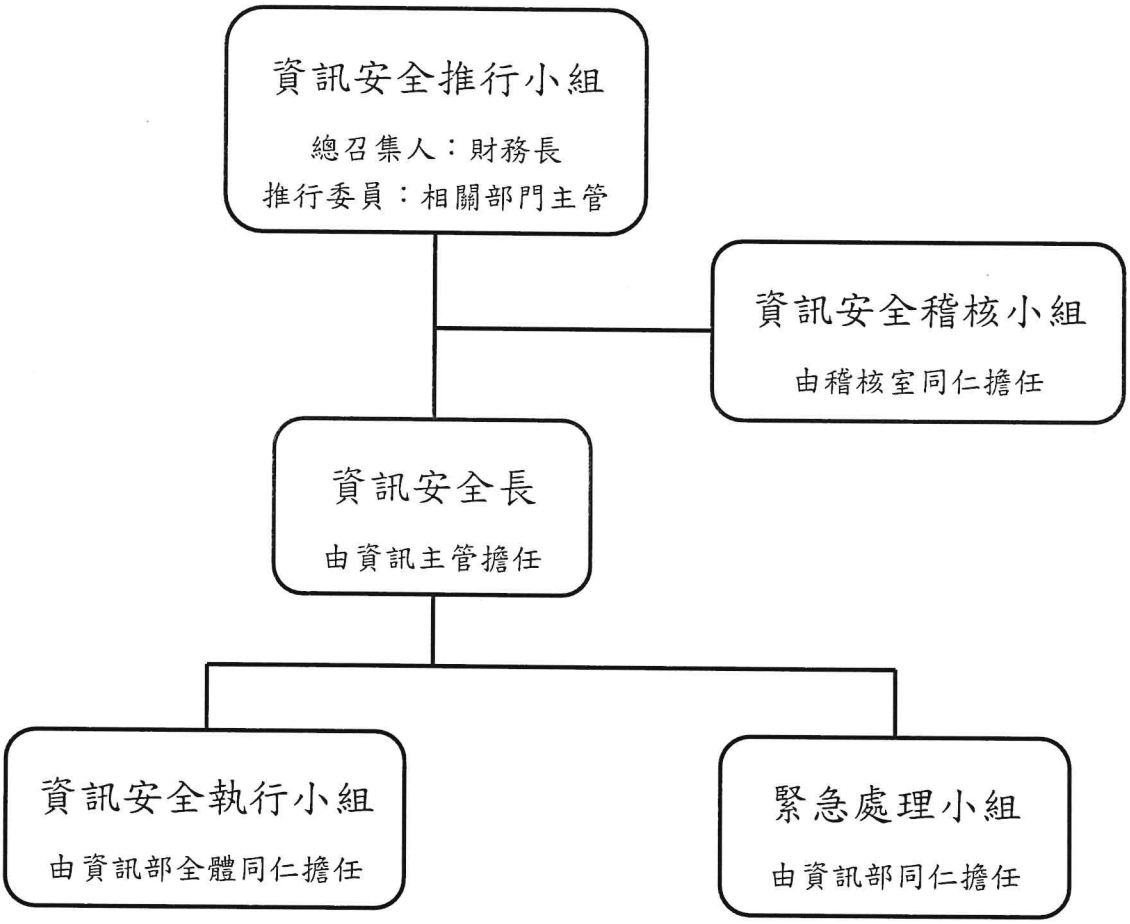
二、 遵循本公司資訊安全管理制度的安全規範和程序。

三、 所有同仁都應確實了解自己的責任去保護這些資產。

以一簡單、容易記憶與符合資訊安全管理目標為原則，訂定本公司的資訊安全政策聲明為：

系統服務不中斷 資訊安全有保障

伍、資訊安全組織



一、 資訊安全推動小組 ： 由本公司財務長擔任召集人，成員包含各部門推派一位單位主(副)管(經(副)理以上職級)為推行委員，討論資訊安全政策、分配各部門所需擔負的責任並協調各部門所需配合的相關事項。

1. 每年定期或視需要召開會議，審查資通安全管理相關事宜。

2. 視需要召開跨單位之資源協調會議，負責協調資通安全管理制度執行所需之相關資源分配。

二、 資訊安全長 ： 由資訊部門主管擔任。

1. 負責協調資訊安全執行小組與緊急處理小組執行資訊安全相關作業。

2. 負責對資訊安全狀況進行預警、監控，並對資通安全狀況與事件進行處置。

3. 對於資通安全管理之改善提出建議，以及協助執行資通安全之自我檢核。

4. 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

三、 資訊安全執行小組 ： 由資訊部全體同仁擔任。

1. 制定資訊安全管理相關規範。

2. 推動資訊安全相關活動。

3. 辦理資訊安全相關教育訓練。

5. 建立安全事件緊急應變暨復原措施。

6. 執行稽核改善建議事項。

7. 執行預防措施之改善。

8. 研討新資通安全產品或技術。

9. 執行資通安全委員會決議事項。

四、 資訊安全稽核小組 ： 由稽核室同仁擔任。

1. 擬定資通安全內部稽核計畫。

2. 執行資通安全內部稽核。

3. 撰寫資通安全內部稽核報告。

4. 追蹤不符合事項之改善執行情形。

五、緊急處理小組 ： 為任務編組方式組成，由資訊安全長指派資通安全相關技術人員擔任。

1. 負責規劃資安事件處理程序。
2. 查明資安事件原因。
3. 確定資安事件影響範圍並作損失評估。
4. 執行緊急應變措施、復原工作。

陸、權責

一、資訊單位為資訊安全之統籌單位，負責辦理下列事項：

（一）資訊安全政策、措施之研議、執行與管理。

（二）資訊安全技術之研究、評估及建置。

（三）資訊安全教育計畫之研擬及執行。

（四）其他與資訊安全統籌相關事項。

二、資料及資訊系統之安全需求研議、管理及保護等事項，由相關單位負責辦理。

三、資訊機密維護及安全稽核等事項，由資訊部會同相關單位負責辦理。

柒、資訊安全之權責控管

一、負責重要資訊業務之管理、設計及執行人員應分散權責，建立相互制衡機制，以避免資料或系統遭不法或不當使用。

二、下列資訊業務之執行，應於人力許可範圍內儘可能分由不同單位或人員負責：

（一）應用系統之使用。

（二）資料建檔。

（三）電腦操作。

（四）網路管理。

（五）系統發展及維護。

（六）變更管理。

（七）安全管理。

（八）安全稽核。

三、對可存取機密性與敏感性資訊或系統之人員，或因工作需要須配賦系統存取特別權限之人員，應審慎派任。

四、各單位應將成員適當配置，確定各成員之工作職掌，使每一員工均瞭解本身之職責與隸屬關係，並應妥適分工以達相互牽制防止弊端發生。

五、應對員工依其角色及職能，施以必要之資訊安全教育及訓練，提高員工資訊安全意識，促其遵守資訊安全規定。

六、各單位人員對其經辦業務須嚴守機密，必要時得簽署書面約定，以明責任。

七、人員調、離職時應申請取消其識別碼(USER ID)，或調整其相關之作業權限，並收繳其通行證、卡、相關證件、及歸還調用之文件、資料等，並列入人員職務異動之必要手續。

捌、管理原則

一、資訊安全是全體從業人員之責任。

二、必須建立適當的資訊安全管理組織，包括對於資訊安全的控制方法，執行必要的技術性檢核，對於資訊安全事件進行通報、處置、以及對於 ISMS 進行稽核及審查。

三、資訊安全管理系統必須符合本公司業務需求，並兼顧資訊投資之成本效益。

四、資訊安全管理須符合相關法令、本公司內部規範、以及契約之要求。

五、資訊資產應訂定分類分級程序，按照安全等級明確標示，分級管

理。

六、對處理重要機密資訊之從業人員與外部人員進行必要之安全查核。

七、ISMS 須依據 ISO/IEC 27001 過程導向之「規劃—執行—檢查—行動（Plan-Do-Check-Act, PDCA）」模型，持續執行「建立、實作、運作、監視、審查、維持與改進」之文件化過程。

八、從業人員如違反本政策及相關法令致危害本公司資訊安全，資訊部門應即報准停止其使用。依情節輕重報送本公司相關單位處置。

九、將國際資訊安全標準規範作為 ISMS 的重要參考。

玖、要求事項

一、資訊安全組織

- 設置資訊安全推行小組，負責 ISMS 相關事項之規劃、督導及協調溝通。
- 資訊安全組織工作職責
  - 審核資訊安全管理系統目標及實施範圍。
  - 審核資訊安全管理相關作業執行情形及改善的有效性。
  - 檢討資訊安全相關政策及規定，協調資源之分配及使用。
  - 監督營運持續演練之辦理。
  - 審核實施矯正預防措施所需之資源，包括人力、時間及經費。
  - 審核矯正預防措施之有效性。
  - 每年至少召開管理審查會議 1 次，必要時得召開臨時會議。

二、資訊資產分類分級

- 資訊資產須指派擁有者、使用者，且須依照資訊資產分類分級管理辦法，維持資訊資產清冊的正確性。資訊資產分為軟硬體設施、資訊紀錄、內部使用者、外部使用者及作業流程等五類，並依據資訊資產清冊之分級制定管理方式。

三、資訊資產風險評鑑

- 依資訊資產分類分級辦法所盤點出之資產清單分類分級評估其風險等級，並加以適當管理。
- 有關重要資訊資產之潛在風險，界定其威脅及脆弱點，並採行適當之控管機制，降低風險等級，以維公司業務順利運展。

四、文件及紀錄管制

- 為有效保護與管制本公司之所有資訊安全相關文件、表單及其紀錄，訂定「FT-2-03_文件管制程序」。
- 相關文件階層/表單編碼/文件格式、移除及廢除；文件機密等級、管制作業及編號方式等，規範於「FT-2-03_文件管制程序」。

五、人員暨教育訓練

- 為強化員工對資安相關責任之認知，應對所有使用資訊系統之人員，每年辦理資訊安全教育訓練，以提升員工對於資訊安全之意識。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。
- 資訊安全教育及訓練的內容應包括：資訊安全政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊科技設施之訓練等。

六、資訊安全事件管理

- 為確保本公司各單位於資訊安全事件發生時，有可遵循之處理程序並採取適當之控制對策，以有效達成即時應變、減少損害。
- 資訊安全事件發生時，應即向資訊部門通報，資訊部門應依緊急應變流程做處置。

七、營運持續管理

- 為確保業務營運遭受天然或人為災害以致中斷時，可於最短可接受時間內回復關鍵業務持續運作能力，研析並降低人為或是意外因素對重要業務運作可能導致的威脅，使重要業務在系統發生事故、設施失敗或是受損害時，仍可持續運作。

十一、員工資訊安全遵循

- 為瞭解人員與人員管理的重要性，以及人員在聘雇前、在職期間、聘僱終止或變更等之相關安全控制措施，特別對於電腦處理個人資料保護法、智慧財產權的規定，應嚴格遵守。

十二、資訊系統開發與維護

- 有關資訊系統開發與維護之具體要求，規範於「FT-2-09 資訊安全管制程序」。

十三、個人電腦使用

- 為維護個人電腦作業安全及運作順暢，有關人員使用個人電腦之具體要求，規範於「FT-2-09 資訊安全管制程序」。

拾、參考資料

- 資訊安全管理系統要求事項 ISO/IEC 27001
- 資訊安全管理系統作業規範 ISO/IEC 27002

拾壹、附件

- FT-2-09 資訊安全管制程序

- 為確保業務營運遭受天然或人為災害以致中斷時，可於最短可接受時間內回復關鍵業務持續運作能力，研析並降低人為或是意外因素對重要業務運作可能導致的威脅，使重要業務在系統發生事故、設施失敗或是受損害時，仍可持續運作。

十一、員工資訊安全遵循

- 為瞭解人員與人員管理的重要性，以及人員在聘雇前、在職期間、聘僱終止或變更等之相關安全控制措施，特別對於電腦處理個人資料保護法、智慧財產權的規定，應嚴格遵守。

十二、資訊系統開發與維護

- 有關資訊系統開發與維護之具體要求，規範於「FT-2-09 資訊安全管制程序」。

十三、個人電腦使用

- 為維護個人電腦作業安全及運作順暢，有關人員使用個人電腦之具體要求，規範於「FT-2-09 資訊安全管制程序」。

拾、參考資料

- 資訊安全管理系統要求事項 ISO/IEC 27001
- 資訊安全管理系統作業規範 ISO/IEC 27002

拾壹、附件

- FT-2-09 資訊安全管制程序

資訊安全政策由資訊部制訂，經董事長核准後公告實施，修訂時亦同。

董事長: