資通安全管理

(1)資訊安全風險管理架構:

本公司資訊安全由資訊室負責，訂定內部資安規範與制度、規劃暨執行資訊安全作業與資安政策推動與落實，並依需求適時調整。

內部稽核負責查核內部資安執行狀況，每年稽核一次。

一.資訊安全政策

1.管理階層應瞭解資訊安全目的並予支持。

2.應訂定資訊安全政策的的說明文件及資料

3.資訊安全政策應定期評估。

4.定期對單位人員及資訊設備進行安全評估，確定其遵守資訊安全政策及相關規定。

5.於委外契約中有關安全需求得依實際需要隨時修改安全控管措施及作業程序等。

二.建立資訊安全組織

1.設置資安推動小組，由總經理核定成立，設置召集人一名，由總經理任命技術長或資訊長擔任；並由各部門指派主管級或資深人員擔任個資代表，組織圖如下圖。

2.指定單位辦理風險評估、安全分級、系統安全控管措施。

3.單位內若開放給外單位作資料存取，應訂定控管程序。

三.人員安全與管理

1.依員工職務層級進行適當的資訊安全講習。

2.對員工的私人資訊設備作必要之安全控管程序。

四.資產分類及控制

1.資產清冊應隨時更新。

2.公司應建置資訊安全等級分類標準。

五.實體及環境安全管理

1.公司對攜帶型的資訊財產應訂有安全之攜出管理規則及嚴謹的保護措施並落實執行。

六.通訊與操作管理

1.公司應與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款。

2.公司應使用網路防火牆並定期檢討電腦網路安全控管事項之執行。

3.公司對於敏感性資訊之傳送應採取資料加密等保護措施。

4.公司對於輸出及輸入機密性、敏感性資料應有處理程序及標示。

七.存取控制

1.公司應依網路型態訂定適當的存取權限管理方式。

2.公司應規範於不使用時用上鎖或密碼等管制措施以不讓電腦或終端機遭非法使用。

3.公司資訊及應用系統應設有作業結束後或在一定期間未操作時即自動登出或中斷連線之保護機制，若需再登入需重新取得授權。

4.公司應依環境或業務需要於網路防火牆作適當之設定。

5.公司應管制使用者的連線功能，並針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段做通盤連線控管考量。

6.公司應指定專人管理應用程式原始碼、資料庫及執行檔。

7.公司的機密及敏感性資料的處理應於獨立或專屬的電腦作業環境中執行。

八.系統開發與維護

定期對使用軟體實施病毒偵測。

九.永續經營管理

1.辨識關鍵性業務及執行其風險評估、衝擊影響、優先順序。

2.定期作風險估並調整永續經營政策。

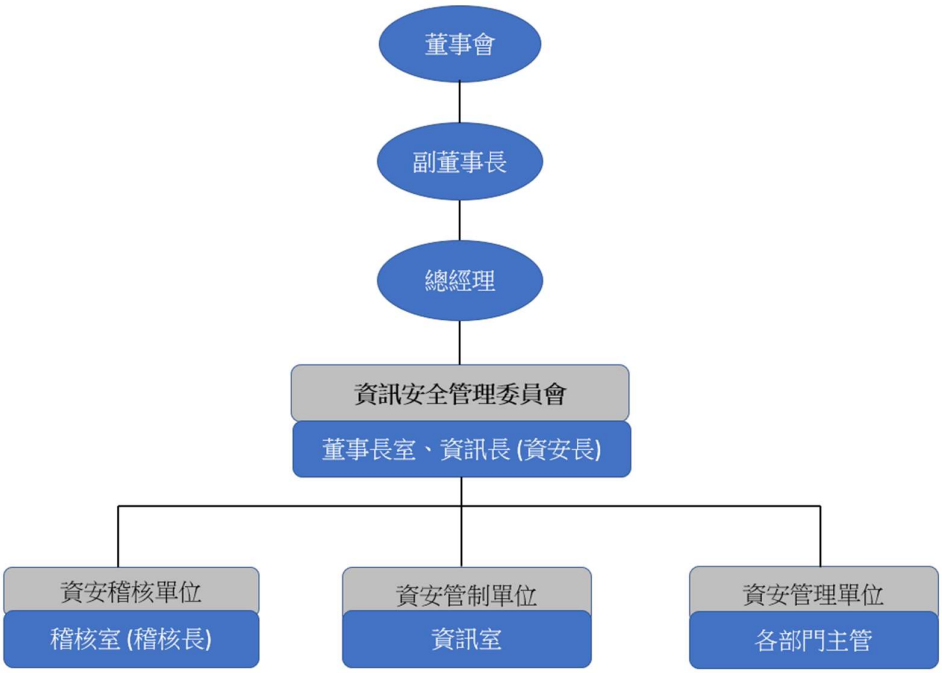
十.內部稽查及其他

1.單位應使用合法軟體。

2.軟體之使用及資料之儲存、處理和報廢，應有適當之控制。

十一.評估與修正

本辦法訂於每年十二月由「資訊安全處理小組」召開資訊安全顧問會議，以獨立公正客觀原則，辦理本公司資訊作業安全事項重行評估與修正事宜，以反映相關法令、資訊技術及本公司業務發展現況，俾使本辦法確實符合安全需求。



(2)資通安全政策:

1. 本公司為維護資通系統持續營運，建立資通安全維護計畫及資通安全事件應變機制，並應定期辦理事件演練。
2. 本公司依角色及職能為基礎，針對不同業務類別之人員辦理資訊安全教育訓練及宣導，使本公司人員瞭解資通安全重要性，以提高資通安全意識並熟悉相關職責。
3. 本公司資訊室每年檢視本政策，或於發生重大變動時重新檢視，以符合資通安全相關法令、技術、組織及營運之最新發展趨勢。

資通安全具體管理方案

一. 資訊安全規劃說明

1. 內部組織管理面

規劃流程	策略作法
組織設立	(A) 設置資安推動小組，由總經理核定成立，設置召集人一名，由總經理任命技術長或資訊長擔任；並由各部門指派主管級或資深人員擔任個資代表。 (B) 資安推動小組下設秘書組，由資訊長協同外部資安顧問，以及內部工程師及人力資源等部門組成。 (C) 完成資安推動小組人選推派。
組織成員職責	(A) 總經理及本計畫協同計畫主持人 i 核定資安相關政策 ii 任命資安小組召集人 iii 核定資安事件之因應措施與個資事件檢討報告 (B) 召集人 i 召集並主持個資推動小組會議 ii 向總經理提出資安管理執行成效與改善方案報告。 iii 成立當事人行使權利申訴案件調查小組並核定調查報告。 (C) 資安推動小組 i 審查公司資安資料保護政策及隱私權聲明。 ii 審查個人資料管理年度工作計畫、檔案盤點、風險評估等規劃。 (D) 資安代表 i 執行資安推動小組決議事項。 ii 協助執行個人資料管理規章及部門內部個人資料管理程序之各項工作。 iii 即時反應部門內個人資料管理風險及資安事故。 (E) 秘書組 i 研擬及公告個人資料保護政策及隱私權聲明。 ii 研擬個人資料管理年度工作計畫、檔案盤點、風險評估等規劃。 iii 辦理教育訓練。 iv 協助部門進行個人資料檔案盤點及風險評估作業。

規劃流程	策略作法
	v 落實個人資料管理所需推動措施、安排會議、製作會議紀錄並追蹤決議執行狀況。 vi 協助部門應變及處理個資事故。

2. 資安管理推動面

以上述內部組織管理模式，初步建構資安推動小組後，將透過下述的流程步驟，將資訊安全概念深植企業文化當中，以下進行歸納說明：

規劃流程	策略作法
固定會議規劃	(A) 資安推動小組會議每季至少召開一次，如遇重大事項得由召集人召開臨時會。 (B) 資安代表因故無法出席會議時，應由部門主管指定代表出席。 (C) 資安推動小組會議之決議，應有過半數個資代表出席，並以出席代表過半數之同意行之。
個資蒐集、處理及利用原則	由於智慧公益案主要進行弱勢族族之視力檢測，最首先面臨的便是受測者的個資蒐集問題，因此在資安規劃上，需明訂個資蒐集、處理及利用原則：蒐集、處理及利用個人資料，應遵守下列原則： (A) 尊重當事人之權益。 (B) 依誠實及信用方法。 (C) 不得逾越特定目的之必要範圍。 (D) 與蒐集之目的具有正當合理之關聯。
個資蒐集 前置工作	以電腦網站等蒐集個人資料時，先提供當事人閱讀「蒐集個人資料告知事項暨當事人同意書」，並經當事人勾選「同意」後，始由當事人填寫個人資料。
個資的儲存	(A) 儲存於檔案伺服器者，相關保管人員施以加密措施。 (B) 儲存於系統時，會設定存取權限且備份檔案加密。
個人資料刪除及載體銷燬	(A) 相關人員刪除載有個人資料之電子文件時，應確認儲存設備中，未留存任何應予刪除之電子文件。 (B) 儲存設備（硬碟、光碟片、隨身硬碟、隨身碟、記憶卡等）報廢時，相關人員會以格式化或物理破壞等方式，永久刪除個人資料使他人無法還原利用。 (C) 刪除或銷燬個人資料，會留存紀錄。

規劃流程	策略作法
利用原則與方式	(A) 相關人員利用個人資料時，會視情況採取適當方式（如遮蔽特定欄位），避免洩漏個人資料。 (B) 公司利用當事人電子郵件帳號等方式向當事人發送行銷資訊，會提供拒絕接受行銷之方式，同時置於網站等明顯易見的地方。 (C) 公司收到當事人拒絕行銷之通知時，會立即停止發送行銷資訊，並妥善保存紀錄。

二. 多層資安防護

1. 網路安全
   1. 導入先進技術執行電腦掃描及系統與軟體更新 .
   2. 強化網路防火牆與網路控管，防止電腦與病毒跨網段擴散 .
2. 裝置安全
   1. 建置防毒軟體機制，防止惡意軟體入侵.
   2. 建置端點防毒措施，強化惡意軟體行為偵測 .
3. 應用程式安全
   1. 制定開發應用系統安全程序 .
   2. 強化應用程式安控機制，整合於開發流程及平台.
4. 資料安全保護技術強化
   文件及資料加密控管及有效追蹤
5. 教育訓練及宣導
   1. 加強員工對郵件社交軟體攻擊的警覺性，提高員工資安意識 .

三. 內容說明

項次	內容	規劃方案
1	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	建置網管系統，自動盤點資通設備並產生報表，另可於服務中斷時告警
2	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輸用戶輸入輸出之檢查過濾等	由於特權帳號可存取最多的敏感性資料與有價值的資產，因此建議要加強保護
3	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	建置全方位的端點DLP（端點資料外洩防護），探索及保護機密資料的同時，也嚴密監控與機密資訊相關的作業
4	條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
5	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。	建置內網防火牆，且建議與現有防火牆不同廠牌

四. 資源投入與軟硬體設備優化

本公司定期檢視公司資訊安全管理運作情形，與資安相關法規及最新趨勢，持續投入相關資源以保護公司資產。113 年度投入 WAF、MDR 等資安相關軟硬體設備資源合計共超過 700 萬元。

2.列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實: 無。