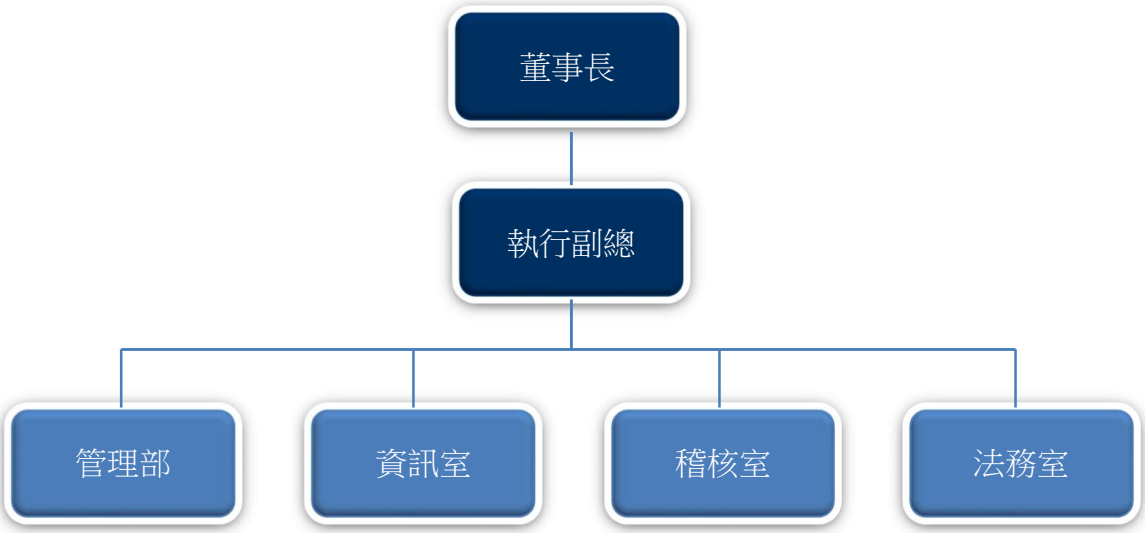
資通安全風險管理架構

本公司由執行副總統籌，組織管理部，資訊室，稽核室，法務室設立資訊安全治理組織，檢視各項安全管理，統整資訊及建議改善計劃，由執行副總決議各項安全管理政策，提報董事長，指派政策執行專責人員推動與執行。



資通安全政策

1. 進行資訊資產風險評鑑，針對系統架構、網路安全、資源管理，軟硬體授權檢核其與企業環境是否合規性及高可用性，並對風險事項進行調整或納入改善計劃。

2. 保密政策與資料保護宣導、檔案及記錄管理、移動設備管控、層級權限管制，以及稽核與法務單位不定時檢核與彙整記錄，協同運作，彙報各項異常資訊，降低資訊外洩風險，維護企業重要資產及競爭力。

3. 與時俱進之資訊安全認知宣導，及社交工程演練(電子郵件釣魚測試），提昇員工資安意識、以落實於日常工作之中。

4. 與各家資安公司保持密切合作關係，並申請加入 CERT 聯盟，針對各地不斷發生的資訊安全事件及安全弱點，即時通知、調查及處理，確保弱點及早修復以防範未然。

資通安全資源投入

（一）外對內，內對內多層防護

1）**架構多層且不同廠牌防火牆設備**，啟用各優勢功能，進階偵測技術，監控流量，識別應用程式，分析未知惡意軟體，預先阻斷不明連線行為與滲透。

2）**跨廠區或跨機種網路控管**，廠區間增設防火牆設備，防止病毒與攻擊跨廠區擴散。

3）**增設多道多層式郵件防禦閘道**，啟用 Attachment Defense，URL 即時檢測，BEC 詐騙，網路釣魚，勒索病毒防護等功能，多維度檢測，反規避偵測，禦防進階式郵件滲透，攔截先進式攻擊威脅。

（二）系統與網路備份備援

1）建立全方位資安韌性架構，透過**異地備份**確保資料具備跨地域之容災能力，建置**網段隔離**（邏輯隔離）機制，阻隔網路威脅之橫向擴散；同時導入**加密備份**技術，強化存放資料之隱密性與完整性；最後藉由**每年定期災害演練**，實測復原流程並驗證備份機制之有效性，以落實業務連續性管理目標。

（三）端點防護

1）電腦依不同類型安裝一種以上防護軟體，除了增強基本防毒防護，更導入新世代端點 APT 端點防護，利用行為偵測功能，對於不尋常的操作行為零時差監控，即時阻擋及刪除惡意程式與降低橫向感染，另外更利用機械學習和行為分析，阻止無檔案惡意軟體與記憶體攻擊。

2）入入侵防護服務，即時警示與回應，阻止大規模入侵。

3）建立機台入廠檢測機制，防止惡意軟體伴隨著系統漏洞進入廠內。

4）端點裝置控管，禁止可攜式儲存設備或無線設備使用。

5）上網行為控管與隔離防護，文書作業與瀏覽外部網頁區分不同作業環境降低誤觸釣魚網站進而下載惡意軟體至個人電腦中，阻斷駭客外對內潛伏連線。

（四）資料安全防護與保密規範

1）導入文件加密防護系統，限制人員存取，管制檔案行為權限，記錄檔案操作，防止資料外洩。

2）複印及掃瞄設備控管，導入列印與掃瞄記錄保存軟體，未經授權之使用者無法操作設備、記錄任一登入與操控設備行為、被複印或掃瞄紙本文件將電子檔方式完整保存。

3）郵件外寄及寄內權限管控，依個人任務期間需求申請對外收發權限。

4）雲端空間存取限制，預設禁止使用雲端空間服務。

5）導入資料備份系統，訂定備份機制並離線保存，不定期備份還原演練，更新還原 SOP，驗證還原程序可行性與資料可用性。

6）個人電腦或終端機，均設有分層授權使用重要資訊許可權的帳號與密碼，未經上級主管同意，不應將帳號密碼提供他人使用，違者將視情

節輕重懲處之。

7）禁用侵權軟體：公司使用軟體授權必須合法化，未經軟體合法授權，私自安裝於包括：所配備電腦設備或自行帶入公司之私人電腦，一律屬侵權行為，將視情節輕重及監督缺失予以懲處。

8）員工不得利用本公司資源，透過侵入、密碼探勘、盜用他人密碼或任何其他方式來嘗試未經授權地存取他人網站或資料、其他帳戶、電腦系統，或是使用未授權軟體，或於職務上使用因前述行為而取得之資訊與電腦/軟體存取權限。

9）員工就其職務上所知悉、掌管之營業秘密及機密資料，應採取適當之保護措施，包括下列措施：

9-1)經授權向第三人揭露前，應簽訂保密合約。

9-2)確實遵守勞動契約及其他相關之保密管理規範。

9-3)採取必要合理防護措施，避免未經授權接觸機密資料，取得營業秘密或機密資料。

10）公司資料揭露原則：員工就本公司之資產，包括資訊、業務、技術資料以及其他任何有形或無形之營業秘密、機密資料等，不得在未經許可情形下，揭露予其他任何第三人。

資通安全事件管理

資通安全事件定義

資通安全事件(Information security event)：指系統、服務或網路或與資安相關發生違例、失效，或是未可預期的異常現象。

資通安全事件分級

第 1 級 (低)輕微 (Low)

(1). 個別員工電腦異常且已隔離。

(2). 單機硬體異常但不影響其他服務。

第 2 級 (中)中等 (Medium)

(1). 非核心系統功能失效。

(2). 非核心資料損失，但不影響資料準確性。

第 3 級 (高)嚴重 (High)

(1). 單一重要業務中斷。

(2). 小範圍敏感資料受損。

第 4 級 (極高)災難性 (Catastrophic)

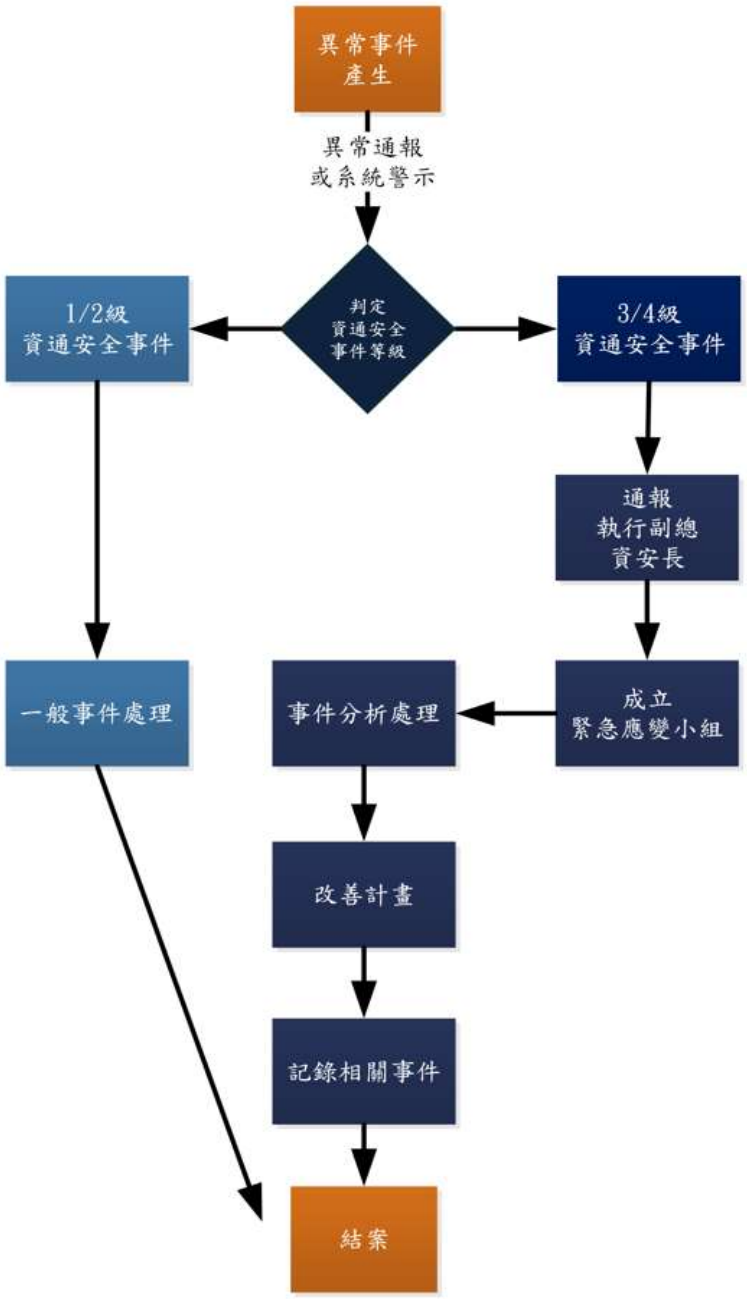
(1). 核心系統完全停擺。

(2). 大規模核心資料或公司機密外洩。

資通安全事件處理流程

資訊單位收到通報或發現系統警示，進行事件處理如下列流程圖

資訊安全事件處理過程中，如發現事件造成影響大於原先判定等級，應立即採取相對應流程。



資通安全事件作業要求：

4 級事件須於發現事件於 1 小時內完成通報，12 小時內復原或完成損害管制，

3 級事件須於發現事件於 4 小時內完成通報，24 小時內復原或完成損害管制，

1/2 級事件須於發現資安事件 36 小時內復原或完成損害管制。

3/4 級事件須記載於異常處理事件，追蹤及後續改善計畫

資訊安全事件危及人員生命或設備遭到破壞等，涉及民、刑事案件時，應通報法務室請求處理。

資安與網路風險控制

本公司除了與各資安廠商保持密切合作關係，並配合政府資通安全政策逐步建立內部管控制度。

持續了解資安產品防護功能，了解新型攻擊手法與防禦技術，評估各種防範產品可行性。

持續簽定保固維護與設備更新及升級合約，確保設備可獲得更完整的特徵碼與惡意軟體流量分類，以及最新防禦偵測功能，以辨別新型威脅並自動啟動保護政策。

定期宣導資訊安全資訊，針對誤動作觸發資安警訊之員工，呈報其上級長官，並指派專人加強應對訓練或取消其權限。

定期弱點掃瞄及資料備份還原演練。

制定緊急應變計劃，包含應變組織，人員通報，實體安全，技術及緊急作業程序。

訂閱身份保護服務，補捉有關使用者活動日誌、身份驗證事件、授權事件、系統配置變更、管理操作記錄等資訊，集成各種事件日誌，幫助公司監控和應對與身份相關的潛在威脅。

風險管理組織

平時，公司內部專任稽核人員定期了解其遵循情形及不定期抽查行為記錄並做成稽核報告，每年呈上檢討，以確保公司政策落實及機制改善。最近一次報告為114年第四季。

危機處理時，由執行副總擔任指揮官，直屬單位擔任會議召集人，召開跨部門會議，了解風險擴散狀況，協調指揮各部門配合彈性生產方式，追蹤事件狀況與處理進度，定時發佈更新狀況。

最近年度，本公司未發生衝擊公司營運的重大網路攻擊事件。