目的及適用範圍

為加強資通安全事件發生時之應變能力，避免資通安全事件失去控制成為影響組織營運持續的危機，訂定「資通安全事件通報與應變機制」。

發生於本公司之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

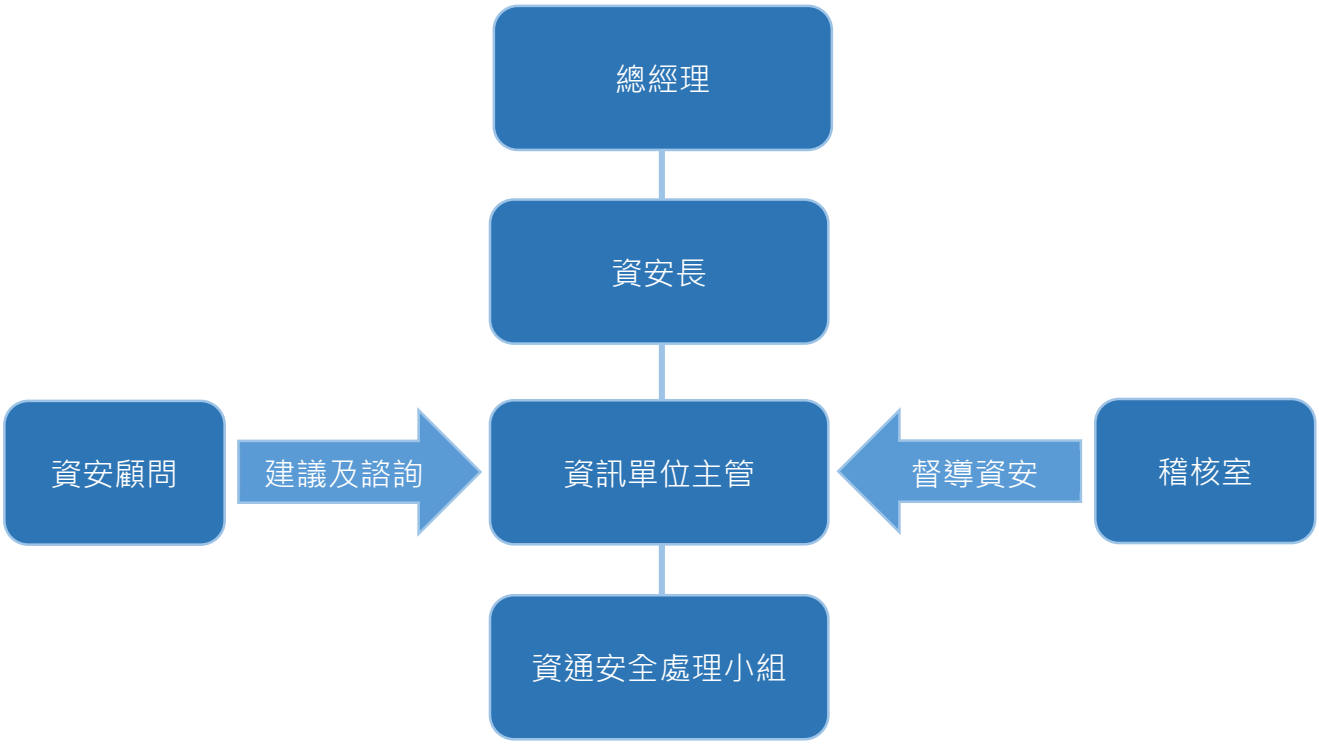
資通安全風險管理架構

(一)本公司由資訊管理處負責資訊安全政策管理與規劃，並有資安小組負責資訊安全相關事件處理與通報。

- 資訊安全技術與專案評估規劃。
- 機房維護與管理。
- 硬體設備、系統維護與管理。

(二)針對資訊安全之防毒、防災、防駭、防漏等之機制，定期向權責主管進行彙整報告。

(三)資通安全架構



資通安全事件等級

本公司所討論的資通安全事件，泛指一切對於資通安全之機密性、完整性或可用性方面造成危害的突發事件，將資通安全事件分為三級，由重至輕分別為「3 級」、「2 級」及「1 級」。

(一)3 級事件

符合下列任一情形者，屬 3 級事件：

1. 機房設備電力異常、停電，無法正常供電，導致系統無法運作或停頓，無法於可容忍中斷時間內回復正常運作。
2. 機房因強烈地震、火災造成災害發生，導致系統無法運作或停頓，無法於可容忍中斷時間內回復正常運作。

(二)2 級事件

符合下列任一情形者，屬 2 級事件：

1. 資通系統硬體損壞，導致系統無法運作或停頓，無法於可容忍中斷時間內回復正常運作。
2. 資通系統遭駭客攻擊、病毒感染、惡意程式攻擊，導致系統無法運作或停頓，無法於可容忍中斷時間內回復正常運作。
3. 資通系統網路通訊中斷，導致系統無法運作或停頓，無法於可容忍中斷時間內回復正常運作。

(三)1 級事件

符合下列任一情形者，屬 1 級事件：

1. 資通系統遭輕微洩漏、遭輕微竄改、資料異常。
2. 資通系統運作受影響或停頓，於可容忍中斷時間內回復正常運作。

資通安全事件通報窗口及應變作業流程

(一)資通安全事件通報窗口及聯繫專線為：02-2917-5770#751
Mail：Jimi_chiang@wendell.com.tw

(二)人員發現資通安全事件後，應立即向所屬單位主管及資訊部之通報窗口通報。

(三)應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

(四)事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向行政主管報告，由資訊部主管成立緊急處理小組，立即開會討論應變計畫。

(五)各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

資通安全事件通報程序

(一)判定事件等級之流程及權責

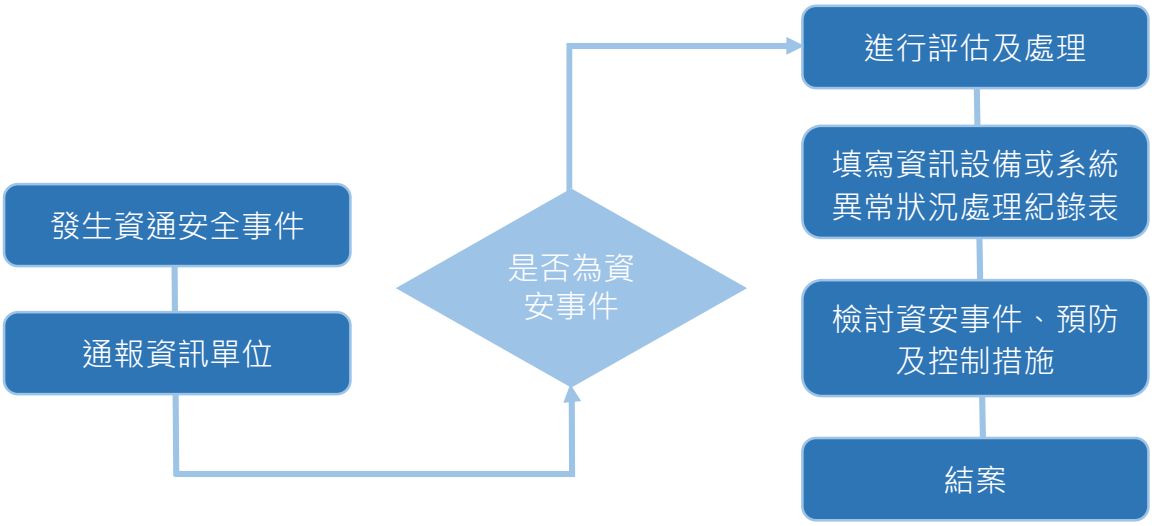
權責人員或緊急處理小組應依據以下事項，知悉資通安全事件後，依規定完成「資通安全事件通報及應變機制」之資通安全事件等級判斷：

1. 事件導致資通系統遭竄改之影響程度，屬嚴重或輕微。
2. 事件導致資通系統遭中毒、惡意攻擊或電力設備異常，機房發生災害等而影響系統停頓，是否可容忍中斷時間內能回復正常運作。
3. 事件其他足以影響資通安全事件等級之因素。

(二)除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度因應之能力進行評估。

(三)權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應盡速報權責主管代表核准。

(四)資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。



資通安全事件應變程序

(一)事件發生前之防護措施規劃

本公司應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

(二)損害控制機制

負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄：

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 資安事件之調查與處理及改善報告之方式。
4. 資安事件後續發展及與其他事件關聯性之監控。
5. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本所事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
6. 其他資通安全事件應變之相關事項。

對於第一級、第二級資通安全事件，本公司應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級資通安全事件，應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

紀錄留存及管理程序之調整

(一)本公司應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「資訊設備或系統異常狀況處理紀錄表」上留存完整之紀錄，該文件並應經承辦人員、權責主管簽核。

(二)本公司於完成資通安全事件之通報及應變程序後，應依據「資訊設備或系統異常狀況處理紀錄表」之內容及實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

輸出文件／紀錄

(一)資訊設備或系統異常狀況處理紀錄表

(二)資通安全事件應變機制與檢查表

(三)非法軟體定期檢查表

資通安全具體管理方案

設備管理
✓ 資訊斷線備援演練
✓ 備援資產盤點
✓ 設備定期維護

軟體防護
✓ 防火牆機制
✓ 郵件服務搭配 SPAM 機制
✓ 防毒模組
✓ 作業系統更新

資料保存
✓ 定期備份
✓ 異地存放
✓ 伺服器虛擬化技術

資訊安全
✓ 系統密碼強化
✓ 定期宣導資訊安全政策

(一)為因應突發狀況及資訊資料回復，已著手規劃資訊斷線備援演練及備援資產盤點。並透過演練來進一步了解目前欠缺的措施、設備、人員熟練等等應變能力，透過後續的補強規劃，來強化企業整體的應變能力與危機處理。

(二)機房內主要伺服器設備與電力管理等，均定期配合廠商定期維護，保障防災、消防規劃、不斷電系統等保障維運環境。

(三)使用防火牆機制，將各內部需使用網路與服務的單位群組，進行分類與應用服務管制，加上時段管理與透過申請機制，來強化網路管理與彈性應用。

(四)郵件服務搭配 SPAM 機制，並掛載防毒模組與進階防禦模組，以利進行進階惡意程式比對。可進階防禦魚叉式攻擊、匯款詐騙、APT 攻擊郵件、勒索病毒以及新型態攻擊等事件。

(五)資料檔案與系統面等備份，均安排排程自動化的定期備份與異地存放。

(六)使用伺服器虛擬化技術，透過系統備份機制，可在突發狀況發生時，將系統的歷程備份版本，進行快速系統掛載與服務恢復。

(七)公司內所有的 Windows 電腦均有防毒軟體的佈建，並定期配合作業系統更新，能有效避免系統漏洞與提升系統安全，保障企業在整體應用上、網路上、管理上的可靠性與安全性。

(八)公司內各系統的使用，同仁員工密碼原則上均不能少於 8 碼，並搭配特殊符號、數字、大小寫英文等，同時不能與歷程密碼相同。

(九)定期宣導資訊安全政策與提供改善措施等規劃，避免內部同仁透過上網行為、郵件內容、USB 的隨插即用與個人持有設備等使用操作，造成公司內部風險提升與間接異常破壞。

資安風險	資安管控因應措施
1. 使用者不當於辦公室內私裝電腦及網路通訊等相關設備 2. 使用者無繼續使用資通系統時，未立即停用或移除使用者帳號 3. 機密資訊未於儲存或傳輸時應進行加密 4. 使用者使用電子郵件時未提高警覺，讀取來歷不明之郵件	1. 防火牆政策規則確保公司內外部網路安全連線、惡意軟體、駭客入侵等網路安全保護 2. 公司電腦安裝防毒軟體，確保電腦避免中毒，提升電腦安全性保護 3. 郵件防護系統：垃圾郵件防護、病毒郵件防護，郵件威脅與攻擊防護，以確保企業郵件的安全 4. 資訊安全加強宣導與教育訓練，推廣人員資訊安全之意識與強化對相關責任之認知