資通安全執行情形

資訊安全政策

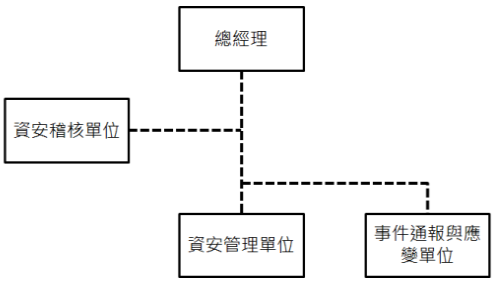
數泓視資訊安全為企業基本責任，為保障利害關係人之資訊資產不受侵害，本公司建置完善的資訊安全管理體系，確保資訊處理的正確性與可用性，並持續強化系統、設備和網絡之安全防護機制。

資訊安全管理辦法與目標

為強化資訊安全管理，本公司已制定「資通安全政策」，並依循政策持續修訂與更新，以確保資訊安全制度符合企業營運需求及法令遵循。

組織架構

本公司之資安專責組織由總經理擔任召集人，並配置資安主管、資安人員及稽核人員各一名，制定「資通安全政策」，建立全面性的資訊安全治理架構，並定期評估企業營運所面臨之資安風險，確保資安管理體系之適切性與有效運作。資安團隊統籌推動資訊安全工作，包括資安風險評鑑、資安訊息傳遞及定期召開內部資安會議，持續執行與優化各項資安政策，彙整治理方向與執行成果進行彙報，以確保資訊作業內部控制機制之有效性，並提升全體員工之資安意識。



（圖）資安中心組織

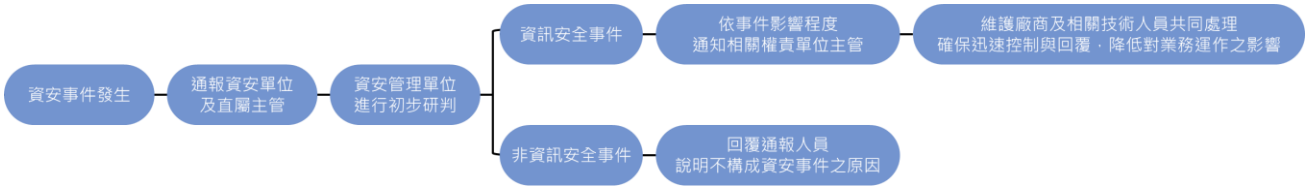
資訊安全處理流程

為確保資訊安全事件發生時能迅速應對，數泓訂定「內部重大資訊處理作業程序」，透過完善的資安處理流程，以提升事件通報效率並即時採取行動，降低事件對本公司業務與資產可能造成之衝擊與損害。

依據「資通安全政策」規定，本公司全體同仁一旦發現疑似資訊安全事件，即有即時通報之責任，接獲通報後，將依事件性質與影響程度，啟動相對應之通報與應變流程。資訊處亦會詳細記錄事件發生經過、初步判斷與應變處理紀錄，確保事件處理具備可追溯性與透明度。

此外，本公司建構完善之危機處理體系，涵蓋事前防護建置、事中即時應變與預警機制，以及事後復原追蹤與鑑識作業，確保每一項資訊安全事件均能有效處理。

透過完整的處理機制與制度化落實，本公司能有效識別、即時應對及妥善處理各類資訊安全事件，自通報、應變至後續改善皆有明確程序，確保事件影響降至最低，保障企業資訊安全與業務穩定運行。



114年資通安全執行情形如下：

(一)資訊安全管理機制：

管控項目	執行措施
防毒軟體	針對郵件病毒有過濾。
防火牆	針對有需求之設備內對外、外對內，才開放網路連線。
郵件過濾 SPAM	針對垃圾郵件以及病毒郵件阻擋過濾。
個人工作 PC/ERP 系統	每 90 天期提醒更換密碼。

(二)資訊安全教育訓練：

時間	主題	人數	總時數
114 年 1 月 13 日	資訊安全意識、必備知識與責任 E-Course	1	2
114 年 1 月 13 日	資安事件說明及預防措施 E-Course	1	2.5
114 年 1 月 13 日	上市上櫃公司資通安全管控指引說明 E-Course	1	1.5

總結報告：本公司 114 年未發生資安事件。

上述 114 年資通安全執行情形，已於 114 年 11 月 13 日向董事會報告。