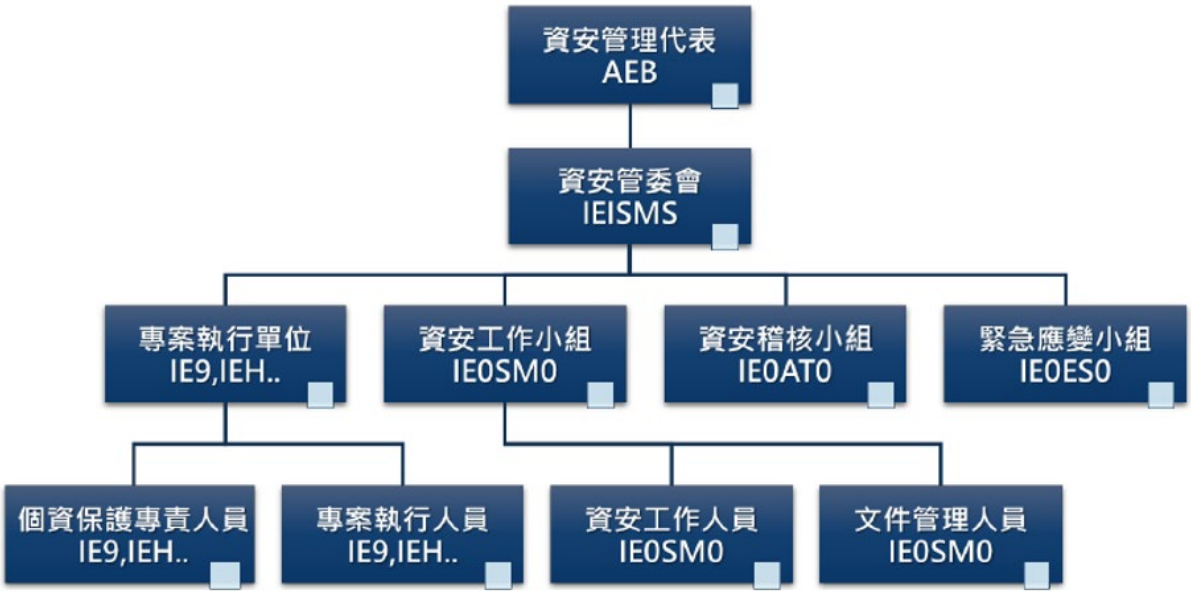
宏碁資訊服務股份有限公司

資訊安全管理

1.資通安全風險管理架構

本公司資通安全管理與個人資料管理的最高層級為資通安全管理暨個人資料保護代表(簡稱資安管理代表)由本公司總經理指派擔任,下轄資通安全管理暨個人資料保護委員會(簡稱資安管委會),其下設立資通安全管理暨個人資料保護工作小組(簡稱資安工作小組)、資通安全管理暨個人資料保護稽核小組(簡稱資安稽核小組)、資通安全管理暨個人資料保護緊急應變小組(簡稱緊急應變小組)及專案執行單位等,並由資訊安全主管監督、管理各小組之日常實務運作。



2.資通安全管理暨個人資料保護政策

(1)考量相關法律規章及營運要求,評估資通訊作業安全需求,建立相關資通安全管理規範及工作指導書,以確保資訊資產之機密性、完整性及可用性。

(2)建立本公司資通安全組織並訂定分工權責,俾利推行資通安全作業。

(3)依資通安全管理規範及工作指導書規定執行各項應辦事項。

(4)建立資通安全事件、個人資料安全事件通報應變機制,以確保事件妥善回應、控制及處理。

(5)定期執行資通安全稽核作業,以確保資通安全管理落實執行。

3.資通安全管理暨個人資料保護目標：

(1)資通安全管理目標：在合於法令、法規與合約要求條件下，確保資通訊資產及個人資料之機密性、完整性與可用性，提供持續可用之服務。

(2)個人資料保護目標：基於法令規定、合約要求及個人資料處理原則，提供可信賴的資通安全管理與個人資料保護作業環境，維護資訊系統及資料之合法利用，確保本公司業務持續正常運作，達成公司資通安全管理暨個人資料保護目標。

4.資通安全風險評估分析及其因應措施

本公司以顧問諮詢、產品加值整合、應用系統開發建置、軟體維運服務等方式，提供政府及企業客戶雲端運用、企業應用系統開發、產品加值運用、軟體採購諮詢與管理等服務之解決方案；本公司對於資通安全管理非常重視，為控制資安風險，避免發生資安事件而導致服務品質與企業信譽之危害，本公司已建立資通安全政策和相關標準作業程序，並實施資安風險處理、全員資通安全教育訓練、資安內部稽核等作業，除確認整體資通安全之落實度與風險之可控度之外，也針對各種新興資安風險進行及時檢討與因應。此外，本公司也建置各種資安技術控管方案，包括網路防火牆、網頁應用程式防火牆、防毒系統等，可確保本公司將資安風險控制於可接受的範圍內，且能維持本公司所提供專業服務的高品質及穩定度，使服務水準與客戶權益得到保障。

5.具體管理方案及投入資通安全管理之資源

本公司透過下列各項相關管理規範落實公司資通安全管理暨個人資料保護：

(1) 資安事件通報應變管理規範

(2) 資安制度文件管理規範

(3) 資安組織與管理審查管理規範

(4) 人員安全與教育訓練管理規範

(5) 資訊資產管理規範

(6) 風險評鑑管理規範

(7) 機敏(個人)資料保護管理規範

(8) 存取控制及加解密管理規範

(9) 網路及通訊安全管理規範

(10) 實體及環境安全管理規範

(11) 運作安全管理規範

(12) 應用系統獲得、開發與維護管理規範

(13) 業務持續運作管理規範

(14) 供應(委外)廠商安全管理規範

(15) 持續改善作業管理規範

(16) 資通安全目標量測管理規範

另對應資通安全管理暨個人資料保護事項投入之資源方案如下：

(1) 專責組織：本公司已設置資通安全專責單位。

(2) 專責人力：設置資安專責主管及 1 名資安專責人員，負責公司資通安全規劃、技術導入與相關的稽核事項，以維護及持續強化資通安全。

(3) 資安認證：通過 ISO27001 資訊安全管理及 ISO27701 個人資料保護管理外部驗證，相關稽核無重大缺失。

(4) 教育訓練：於 114 年 5 月針對全體員工進行線上資通安全教育訓練 3 小時，參與人次 287 人；以及 114 年 12 月執行社交工程釣魚郵件測試。

(5) 資安公告：本公司不定期發佈資安公告，來傳達資安防護重要規定與注意事項。

(6) 管審會議：「資訊安全暨個資保護委員會」每年實施一次管理審查會議，審查資安執行績效與改善事項，討論可能影響之內部和外部風險議題、確認資通安全執行如稽核反饋、制度之改善機會與建議方案、運行之風險以及各項需求資源的投入等。

(7) 資安保險：本公司參與宏碁集團共同投保資安保險，以提升資安風險之保障，確保公司營運安全與資料保護。

(8) 資安治理會議：每季一次由集團資安治理委員會召開資安會議，宣達資安治理策略、追蹤各項資安作業執行進度及了解資安現狀。

本公司基於提升資料保護及設備使用安全，強化公司同仁間之資通安全意識，透過積極建置相關資通安全管理措施並進行風險評估，進而間接保障股東權益，所採取之具體管理方案及主要因應措施如下：

(1) 於公司內部控制制度之電腦資訊循環中訂有資通安全檢查之控制作業，作為同仁遵行依據，同時不定期檢討內控制度之有效性，進一步強化及落實。

(2) 稽核人員每年對公司資通安全管理進行稽查，以了解資安運作狀況，評估對各項風險控制及異常事項之改善是否確實，以降低及避免相關資安風險。

(3) 加強宣導員工資通安全概念，提高員工防範外部單位惡意攻擊之意識，同時亦減少作業習慣所導致之風險，為公司日常營運管理之運作提供安全保障，另本公司

資通安全相關規範已公告於內部網站。

(4) 為確保資料之保護及機密性，相關系統登入及存取均須經適當之核決及授權，以防範機密資料外流風險，所有電腦與資通訊設備，依所制定之編碼原則，進行分類分級；個人電腦作業系統將固定進行檢查確認維持最新的安全性更新，違者限制該電腦連網，並禁止自行安裝無版權、非法取得及由網路下載之不明軟體。

(5) 為確保公司同仁帳號密碼使用安全及強化連線認證管理機制，已導入新一代帳號密碼使用監管機制並強制啟用多元身分認證管理。

(6) 為確保公司同仁設備使用安全，已導入使用設備端點行為監控系統，並偕同上述的帳號密碼使用監管機制進行集中化維運管理。

6.資訊安全國際標準驗證

本公司已通過下列資訊安全相關國際標準之驗證，並持續維持證書之有效性，目前證書有效期為 112 年 8 月 17 日至 115 年 8 月 16 日。

(1) ISO 27001:2022 資訊安全管理驗證

(2) ISO 27701:2019 個人資料保護管理驗證