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

本公司資訊安全管理與個資管理的最高層級組織為「資訊安全暨個資保護委員會」，由總經理擔任召集人，委員由一級主管擔任，下轄「資訊安全推動運作小組」、「個資保護執行小組」、「緊急應變處理小組」、「稽核小組」等，並由資訊安全長監督、管理各小組之日常實務運作。

2.資通安全政策

(1)致力維護本公司與客戶相關資訊資產之機密性、完整性與可用性。

(2)提昇人員的資訊安全技能與認知，建立本公司可信賴的形象。

(3)建構完善的資訊安全管理制度，達成國際等級的資訊安全管理水平。

(4)持續採用先進技術，提供全方位、高安全性的資訊安全監控及管理機制。

3.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；本公司對於資訊安全管理非常重視，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，本公司已建立資訊安全政策和相關標準作業程序，並實施資安風險處理、全員資訊安全教育訓練、資安內部稽核等作業，除確認整體資訊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的檢討與因應。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。

4.具體管理方案及投入資通安全管理之資源

「資訊安全暨個資保護委員會」每年實施兩次管理審查，確保本公司資訊安全與個資保護相關作業的落實。

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訊安全意識，透過積極建置相關資訊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，說明如下：

(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訊安全管理進行稽查，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)加強宣導員工資訊安全概念，提高員工防範外部單位惡意擊之意識，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。