Acer eDC 資訊安全政策

第一條 目的

本政策文件規範宏碁雲架構服務股份有限公司（以下簡稱本公司），在廣泛的資訊安全威脅下，以安全和一致的方式處理自有和客戶的資訊資產，免於各種可能造成其商業運轉的傷害。

第二條 目標

資訊安全目標是維持本公司機房維運服務、網路管理與安全服務、主機託管、雲端服務之持續有效運作，確保各項資訊資產之安全無虞。

第三條 政策要求

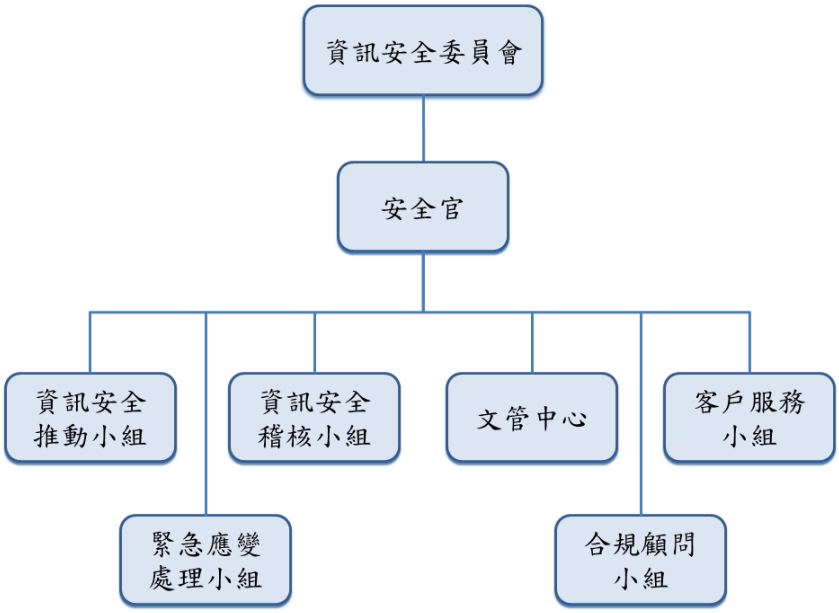
- 本政策應正式地讓使用者知悉與了解。
- 本政策之更新應註明發佈日期與版本。
- 本公司員工應遵守本政策。
- 接觸機敏性資料及系統的本公司員工，其進用時應進行背景調查。
- 違反本政策的行為應依本公司規定處理。
- 本政策之施行涵蓋實體與虛擬化環境，不論自有機房或雲端環境皆一體適用。

第四條 範圍

- 適用於本公司內部和外部使用者所存取的資訊資產，涵蓋其機密性、完整性和可用性。
- 適用於本公司所有的員工、承包商、顧問、臨時雇員、客戶、雲端租戶和其他的使用者。

第五條 資訊安全組織

- 本公司資訊安全組織如下圖所示：



第六條 資訊分級

- 本公司擁有的資訊及所管理的客戶資訊，應採用一個安全等級架構。
- 本公司所擁有或管理的全部資訊，不論其處理技術、來源、格式、存放地點、使用方式，資訊分級系統都一體適用。
- 所有可能接觸到機敏性資訊的使用者，都應遵循本公司之資訊分級政策。
- 資訊分級系統應支援「必要知道」的原則，亦即資訊只對在工作範圍內有必要知道的人公開。
- 資訊由產生到銷毀的整個過程都應受到保護，無論其儲存地點、取得方式、處理技術或用途，也不分其機敏性。
- 本公司對擁有的資訊資產都設定擁有人，詳載於正式文件。資訊資產內容至少包括資料庫、資料檔案、應用系統、維運文件、訓練教材、操作或支援程序、備用系統等。

- 機敏性的資訊揭露予顧問、承包商、和臨時雇員時，應事先請其簽署保密協議。並在對這些第三者揭露機敏性的資訊時，必須進行紀錄。

第七條 身份確認和存取控制

- 每一個電腦系統和通訊系統的用戶帳號，包含授予外部人員的用戶帳號，都是唯一且可歸責，並經申請與核准程序。
- 用戶帳號依權限高低分類並賦予適當的使用規則。
- 使用者對於以其用戶帳號所完成的機敏性作業，應負責且有紀錄備查。
- 人員離職或異動，應有清除用戶帳號、處理其電腦相關設備中所含資料的程序。
- 存取權限應有適當有效的管制、檢討程序。
- 應有程序或機制防範未經授權的存取或探尋系統安全弱點。
- 應訂定密碼管理辦法，確保密碼具備符合要求的強度。

第八條 通訊安全

- 網路連線須有申請及核准的程序，且須指定權責人員維護其組態。
- 網路應設定安全防線，相關過濾規則須確保本公司內部網路之安全且其管控不可規避，過濾規則也須有備份。其管理應由能力適當的人員負責，且緊急事件處理時須有負責人員能迅速存取管理。任何連線網際網路的行為都不能繞過其管控。
- 員工連線網際網路僅限公務用途，且應有安控機制降低被駭的風險。
- 內部網路上的資料內容為本公司的財產，應有管理機制以歸責且防止未授權存取。
- 電子郵件應用於溝通本公司業務相關活動，且為本公司之資產。電子郵件之存取及傳輸應考量其安全性，且原則上以傳輸非機敏性資料為主。

- 員工非經授權不得任意安裝網路通訊相關硬體設備於本公司網路上。
- 員工非經授權不得於臉書、Line 等社群網站揭露本公司公務相關資訊、包含網路及系統相關資訊、資安事故、行銷策略及統計資料等。
- 當本公司網路與外部網路有所連結時，應明確定義各自維護邊界。

第九條 營運安全

- 應定義稽核資料的保留期限，且須維護稽核資料的機密性、完整性和可用性。
- 稽核資料應僅限授權人員存取。
- 稽核日誌應能用於維運狀態或趨勢之分析、異常事件之調查或證據之保存。
- 存放在電腦系統中的重要資訊應定期備份，並依據滿足客戶需求或商業承諾之必要性。重要資訊是指於災害發生後可協助業務或維運活動回復運作者。
- 所有上線系統、應用程式和資料都應實施備份，並於突發事件發生後能有效存取以用於回復正常運作。
- 備份資料應測試確認其有效性。
- 應明確定義行動裝置與可攜式儲存媒體。
- 可能影響本公司維運之重要區域，非經核准禁止使用行動裝置與可攜式儲存媒體，若須使用亦應有相關的管制辦法。
- 行動裝置與本公司重要主機所在網路之連線應經核准，其網路存取亦應有適當規範。
- 行動裝置與可攜式儲存媒體若內含本公司機敏性資料，應有適當保護措施防範資料外洩，亦應有查核機制以確保資料安全。
- 行動裝置與可攜式儲存媒體若屬本公司資產，遞送、遺失、報廢時應有資料安全措施。
- 非本公司核發之行動裝置，包括私人之筆電、手機、平板等裝置，非經核准均不得與本公司內網連線。

- 個人電腦、維運相關系統主機應有惡意程式防範機制，且須確保防範機制之持續有效。
- 萬一發生惡意程式感染的徵兆，應有研判、分析、處理之作業程序進行必要處置，以將風險降低。
- 維運環境中若有新系統上線或既有系統異動時，應有機制確保其未受惡意程式之感染。
- 因工作需要須使用未經核准與公告的軟體，要經過申請及審查程序，且由「安全官」核准後才可安裝使用。
- 為了防止本公司人員使用未獲授權的軟體，導致惡意程式進行資料竊取、系統破壞或開啟後門，營運系統中所安裝或使用的軟體，應造冊彙整並經過核准與公告。

第十條 隱私政策與法規符合性

- 對於個人資料保護法所定義的個人資料，其蒐集、處理、利用均須符合法規的實務程序，以確保個人隱私。
- 本公司資訊安全管理作業、個人資料保護作業，都須符合法律規定與公司相關規範，其有違反者須依公司規定懲處。
- 資訊安全法規符合性之審查每年應至少進行一次。

第十一條　實體安全

- 本公司機房地點的選擇與環境的設計，應考慮火災、淹水、爆炸、暴民、遠離公眾存取和其他自然、人為災害等造成損害的可能，且建築物須避免標記或不引人注目。
- 本公司機房應安裝適當的安全裝備可偵測各種災害，且安全裝備須定期檢查。
- 本公司機房應有多重門禁控管措施。
- 本公司機房內不可放置易燃、危險或其他可能導致災害的物品或設備。
- 本公司機房應規畫有安全的卸貨地帶。

- 使用者不可在包含機敏性資訊或應用程式的禁區中單獨工作。
- 本公司機房所有進出人員應有詳細記錄。
- 本公司機房不允許未經授權的錄音/攝影/使用手機。
- 本公司託管客戶機房的門禁卡或鑰匙，應有適當的管控程序。
- 具備門禁管制的門需被長時間打開時，出入口應有員工或守衛監視。
- 警衛應明定其職責與異常事故處置方法，且須定期巡邏及偵測異常事故。警衛與守衛崗亭亦須配有適當的裝備以執行安全相關任務。
- 警衛應有進用規範及相關訓練。
- 應清楚公告不准攜入辦公環境的違禁物品。
- 應研訂、公告辦公環境安全守則供人員遵循，避免資訊洩漏、影響辦公品質、非授權操作設備或設備遺失、不當的動植物、昆蟲、食物的出現等。
- 為避免未授權的揭露，本公司發給之公務用行動裝置不可放在無人看管之處。攜出本公司時保管人亦須善盡保管責任。
- 本公司應訂定相關停車場管理措施，防範非授權車輛之進出、設備或資訊之遺失、車輛與交通相關意外事故。
- 進出本公司辦公室與機房須有授權，未授權者不得進入。
- 未獲本公司授權，不允許進入機房管理機敏性的上線系統。
- 本公司機房與辦公室區域應進行等級區分，做為依人員身分管制進出的依據。
- 進出辦公室及機房僅限已經授權的人，所有進出工具（如鑰匙、身分卡片等）都須嚴格執行安全程序，包括進出時間的限制、授權及定期檢討、人員異動之授權變更。
- 本公司機房之訪客需有經授權人員陪同。

第十二條　營運持續

- 因應各種災害導致業務中斷的風險，本公司應準備、定期測試及維護一份服務中斷回復計劃。

- 計劃包含復原時間目標（Recovery Time Objective，RTO）、復原點目標（Recovery Point Objective，RPO）、回復組織與職責、災害通報程序、主要系統回復程序、客戶通知程序等，包括詳細步驟和必要的支援資訊。
- 應訓練人員熟悉服務中斷回復計劃相關程序，測試時遭遇的問題、改進建議須向高層管理者報告。
- 服務中斷回復計劃應在正常工作時間以外或例假日都能隨時取得。

第十三條　資訊安全事件管理

- 資訊安全事件是指侵害、毀損、污染本公司機敏性電腦系統或資料，進而提高營運中斷、營運品質下降、法律訴訟與賠償等風險之事件。資訊安全事件也包含發現網路或系統的重大弱點或故障狀況。
- 本公司應準備、定期更新及測試資訊安全事件應變程序，包含解決問題的詳細步驟和支援資訊，確保資訊安全事件能及時、有效的處理。
- 應定義不同層級的資訊安全事件，以及處理各層級事件所須的程序。
- 資訊安全事件發生後須收集相關資訊，且安全地離線儲存，直到本公司不進行法律行動或使用該等資訊。事件處理過程亦須適當紀錄。
- 資訊安全事件相關資訊均屬機密，非經公司規範之許可程序，不得提供給系統合法使用者或外部人員。

第十四條　應用系統取得、發展及維護

- 系統取得或開發前應以資料安全性為核心進行業務風險評估，考慮內部、外部法規與標準要求，且資訊安全需求應書面化。
- 資訊安全設計應納入系統開發過程，涵蓋需求分析、系統開發、系統測試。輸入、輸出、內部處理須考量機敏性資料的安全及維持系統之正常運作。

- 應用系統之開發環境與正式環境須分離。
- 應用系統（含原始碼）之維護、版本控制、變更、存取、資料備份與回復等，應有相關的安全管制機制或程序。
- 委外開發合約應明確描述資訊安全要求，委外商須簽署保密協議。

第十五條　雲端與虛擬化安全

- 本公司雲端與虛擬化的安全要求，應遵從業界最佳標準實務，以及各項國際化標準，包含雲端安全聯盟 （CSA, Cloud Security Alliance）、國際標準化組織 （ISO, International Organization for Standardization）等。
- 對於雲端與虛擬化的網路、運算資源、資料儲存等環境，應建立實體化或虛擬化的區隔，以保護各雲端租戶的資訊與個人資料安全。
- 當雲端或虛擬化提供外部服務時，其服務內容或使用條款變更時，應以文件化的方式通知相關雲端租戶，並在合約或協議中闡明。
- 當雲端與虛擬化環境發生資訊安全事故或個人資料洩露時，應提供雲端租戶單一聯繫窗口，並在服務合約或協議中說明雙方的角色與責任，以及事故後續處置的權利、義務、資料共享原則。

第十六條　資訊安全規範制定與維護

- 資訊安全規範之施行，在實體環境或是雲端虛擬環境皆一體適用。
- 資訊安全規範之制定應依據本政策，並依工作實務上需要修訂。
- 資訊安全規範應載明員工之資訊安全角色及所負責任。
- 資訊安全規範應包含相關的審核、文件管理、公告及修訂等程序。
- 資訊安全規範應至少每年一次檢視產業環境、技術、本公司業務之變動，必要時須進行資訊安全規範之修訂，防範不符合法或其可行性、有效性之降低。