Acer eDC 公有雲服務條款

本「服務條款」為宏碁雲架構服務股份有限公司（以下簡稱我們或 Acer eDC）提供公有雲服務（以下簡稱 eDC Cloud 或本服務）之客戶使用規範。當您開始使用 eDC Cloud 時，即表示同意遵守本服務條款之規範。

1 一般條款

1.1 eDC Cloud 包括運算、儲存及網路等服務資源，可供客戶於服務資源環境中設定所選服務、安裝應用程式及存放資料。eDC Cloud 係由客戶自行管理其服務資源或委由我們代為操作，而須進行服務之設定及管理（例如：備份、安全、備援、還原及監控）。

1.2 客戶在 eDC Cloud 的資料須自行備份或復原（例如：虛擬主機的快照與還原或檔案的備份），我們有提供相關的設定和管理功能及服務。

1.3 eDC Cloud 使用者介面為雲端服務入口網站 (CSP, https://cloud.aceredc.com)，得透過安全連線存取該網站，客戶應對其授權 CSP 使用帳號之存取及操作使用行為負責，客戶應自行負責儲存、維護及保護針對各項雲端服務而產生之一切存取帳號或密碼。

1.4 客戶會有專屬 VLAN 網段部署其服務，VLAN 網段指派 IP Address 供客戶存取其服務使用，並有防火牆配置來進行存取控制。

1.5 eDC Cloud 不包含使用服務中所應搭配的相關軟體，包括作業系統、資料庫、防毒、應用程式或自行安裝程式，客戶得依自身使用目的部署相關軟體到 eDC Cloud，惟須先取得適當之合法授權，使用軟體客戶應負責修補、設定及維護更新。

2 使用原則

2.1 客戶同意遵守本使用原則，並瞭解使用違反該原則之應用程式可能會自動暫停，或被 eDC 系統管理者中止使用權限。除非 eDC 認為有立即中止之必要，否則 eDC 將在中止服務前提供合理的通知。

2.2 客戶不得以下列方式使用 eDC Cloud：

- 法律、規定、行政規則或政府命令所禁止的方式；
- 侵害他人之權利或有侵害他人權利之虞的方式；
- 試圖在未經授權的情況下，存取或干擾任何服務、裝置、資料、帳戶或網路； 傳送垃圾郵件或散布惡意軟體；或以可能損害 eDC 服務或妨礙他人使用的方式。

3 服務變更

為能提供客戶更好的服務，我們對 eDC Cloud 會進行計畫性變更，包括但不限於服務功能、服務下線、基礎架構調整、韌體更新等，如變更會影響服務水準，eDC 將於三日前以電子郵件或於網站公告之方式通知客戶。

4 資訊安全

4.1 我們提供安全的基礎架構和服務，例如：虛擬化環境的實體主機、虛擬化平台(Hypervisor)、網路基礎設施、儲存設備、雲端服務入口網站與機房實體安全等，以及客戶虛擬主機映像與虛擬主機快照及其備份的存放媒體安全保護、營運所需的 CSP 客戶資訊之存取安全保護、使用雲端服務的客戶軌跡紀錄之安全保護。

4.2 客戶應負責針對客戶所提供或控管之服務實施及維護隱私權保護及安全措施，例如：虛擬化平台(Hypervisor)上的虛擬主機、使用軟體或安裝程式、存取帳號及密碼保護、防火牆政策和資料等，包括修補、設定、備份及維護更新等。

5 法律遵循

5.1 客戶在使用本服務時，必須遵守一切相關之法令規定，包括著作權法、個人資料保護法、隱私權及資料保護等相關法律。客戶應負責確認所儲存和處理之資訊及本服務之使用方式，非屬法令或政府機關所禁止之範圍。

5.2 除因提供本服務所應適用之法規命令外，eDC 並無義務遵守任何適用於客戶或其產業，而非資訊技術服務提供者一般適用之法律或規定。

5.3 eDC 提供本服務所適用之法規包括著作權法、電信法、第二類電信事業管理規則、電信事業資訊通訊安全管理作業要點、個人資料保護法、個人資料保護法施行細則。

6 資訊安全措施

6.1 eDC Cloud 資訊安全皆遵守 ISO 27001、ISO 27017、ISO 27018 與 CSA STAR 的規範，並定期由公正且獨立第三方進行安全稽核。在客戶資料上亦遵循個人資料保護法的規定。

6.2 雲端服務平台及雲端服務入口網站 (CSP)，有定期弱點掃描與定期備份，且持續修正與補強弱點。

6.3 雲端服務入口網站 (CSP)有提供存取控制，包含：帳號權限、密碼設定原則等供客戶自行管理及維護，以強化客戶環境安全。

6.4 我們有提供稽核日誌查詢本服務存取及操作行為，稽核日誌可透過 CSP 線上查詢或透過服務請求等方式取得。本公司亦會透過系統存取控制、防火牆連線控管等方式進行客戶稽核日誌的安全保護。

6.5 存取管理方面，雲端服務的管理後台會透過高安全性的管道維運，例如：維運人員均需透過跳板主機存取、動態密碼認證、公司網路與維運網路隔離等。相關的網路、系統、資安設備皆具備存取控制、定期帳號清查等措施，並佐以防火牆限制其連線行為。

6.6 我們會有嚴格的安全管制措施管理雲端服務機房，凡是內部存放有用來處理客戶資料之資訊系統的設施，均設有人員出入限制，只有經過授權的特定人員，方能出入此等設施。

6.7 我們採用各種業界標準系統，避免資料因停電或線路干擾而遺失。

6.8 eDC Cloud 基礎設施均設有 NTP 校正，確保時間同步。相關時間與時區以本服務所在地台灣為基準。

7 儲存位置

客戶資料均存放於中華民國境內，未經客戶同意，我們不會將客戶的資料移出或複製到本國以外的地方。

8 資料處理

客戶保留其資料之所有權，除依法院、司法機關或法規命令之要求外，我們將不會在未經客戶許可的情況下，使用或另行處理客戶資料、個人資料或其衍生資訊進行其他用途。

9 資料揭露

除有下列情形之一者外，在未經客戶同意的情況下，我方不得對第三人揭露客戶資料：

- 司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。
- 其他政府機關因執行公權力所需並有正當理由者。
- 與公眾生命、安全有關之機關（構）為緊急救助所需者。

若因上述原因而有相關資料揭露行為時，亦會遵循本公司相關內部管控程序並留存紀錄，以便日後雙方有所爭議時提供佐證。

10 資料加密

客戶資料儲存於 eDC Cloud，例如：虛擬主機之資料，我們提供資料加密的指引，讓客戶自行決定資料是否需加密。

11 刪除實體儲存設備資料

基礎設施的儲存設備故障或汰換，設備上的所有資料會被安全刪除或銷毀，以確保無法透過任何方式恢復數據資料。

12 資訊安全事件通報

若我們發現、偵測到任何安全性漏洞、資訊安全事件或客戶發現任何可疑活動（以下每項均稱為「安全性事件」），eDC 將採取下列措施：

(1) 通知客戶發生安全性事件；
(2) 調查安全性事件並將安全性事件之相關詳細資訊提供給客戶；
(3) 採取合理措施減輕效應並將安全性事件所引起之任何損害降至最低。

eDC 將於安全性事件發現後三天內或於合理期間內以電子郵件或於網站公告之方式通知客戶。

當客戶發現有可疑活動，包括安全疑慮、帳戶資訊遺失、個人資料外洩或遭受未獲權限之存取等情形者，可透過本公司「客戶服務管理部」提出服務請求，在客戶同意下，我們會協助客戶進行事件調查與處理。

13 資料保留及刪除

儲存於 eDC Cloud 之客戶資料，包含服務資源、CSP 客戶資料和操作稽核日誌等，得由客戶於合約期間內隨時存取，eDC 會在客戶之服務合約屆滿後，保留原服務資源、CSP 客戶資料和操作稽核日誌持續運行 30 天，以便客戶下載資料、自行刪除或完成續約。30 天保留期間結束之後，eDC 將刪除客戶資料及服務資源，刪除後無法復原。惟客戶要求服務合約屆滿後立即刪除者或合約另有約定外，則不在此限制。

儲存於本公司的營運所需客戶資訊，將依個人資料保護法規定留存。

14 聯絡資訊

若客戶有任何服務請求，包括安全性疑慮、技術支援、服務水準、軟體版權爭議等，得聯絡 eDC「客戶服務管理部」提交服務請求，我們會善盡商業上合理之努力回應服務請求，客戶服務管理部聯絡資訊如下：

電話：03-4072000
傳真：03-4072001
電子信箱：eDC_Service@aceredc.com

本服務條款最後更新時間：2021 年 3 月。