

[中文譯本僅供參酌。若中、英文版本間有任何歧異，應以英文為準。]

## 可接受的使用政策

可接受的使用政策 (下稱「AUP」) 描述與禁止使用和/或存取 Dell 基礎結構、網路、雲端產品、系統、服務、網站、帳戶和產品 (下稱「Dell 資源」) 相關之規定。在本 AUP 中，「使用者」係指 Dell 客戶或透過 Dell 客戶存取 Dell 資源之使用者。使用者使用或存取 Dell 資源，即代表同意遵守此 AUP 的最新版本。如果使用者違反本 AUP，或者授權或協助其他人員違反本 AUP，(除 Dell 擁有的其他權利之外) Dell 得自行裁量暫停或終止使用者存取或使用 Dell 資源。

### 違反規定的情形

使用者不得以 Dell 認為存在以下情形之方式或目的上傳內容或使用 Dell 資源：

1. 違反任何適用之法律或法規 (下稱「法律」)，包括但不限於數位千禧年著作權法，或與兒童色情和/或非法賭博相關之法律；
2. 屬於侮辱性、欺騙性、色情、猥褻、誹謗、重傷、冒犯、宣揚暴力內容或其他不當內容；
3. 侵犯或侵害他人權利，包括侵犯或盜用他人的任何智慧財產權；
4. 宣揚或鼓吹非法活動；
5. 跟蹤、騷擾或傷害任何人 (包括未成年人)；
6. 冒充任何人員或實體，或者歪曲使用者與某人或某實體的關係；
7. 修改、變更或竄改 (包括試圖自我修復) Dell 資源中包含的任何軟體；
8. 在非受法律許可之情形下，對 Dell 資源進行反向工程、解譯或反編譯；
9. 以旨在避免支付費用或者超過使用限制或配額之方式存取或使用 Dell 資源；
10. 對 Dell 資源造成妨礙或導致其中斷；
11. 使用任何能夠處理大量資料的自動化手段 (包括傀儡程式、編目程式、指令碼或其他方式) 存取 Dell 資源；
12. 透過駭客攻擊、密碼破解或其他手段，嘗試未經授權即存取 Dell 資源的任何部分；
13. 干擾 Dell 資源的安全性或完整性，包括以下情形：
  - a. 未經許可即存取或使用 Dell 資源，包括嘗試探查、掃描或測試 Dell 資源的漏洞，或嘗試違反 Dell 資源使用的任何安全或驗證措施；
  - b. 未經許可即監控 Dell 資源的資料或流量；
  - c. 偽造封包或電子郵件標頭，或偽造消息中用於描述來源或傳送路線的任何部分；
  - d. 上傳任何包含病毒、蠕蟲、毀損檔案、特洛伊木馬、其他形式的有害程式碼，或任何其他可能有損於 Dell 資源的內容；或
  - e. 對 Dell 資源進行駭客攻擊、破壞 Dell 資源穩定性、對 Dell 資源進行未經授權的變更，或改變其他網站來虛假暗示其與 Dell 資源存在關聯；
14. 使用者連線至任何使用者、主機或網路，但是沒有權限與此類使用者、主機或網路進行通訊，例如以下情形：
  - a. 以任何方式監控或抓取 Dell 資源，並且可能干擾 Dell 資源效能或作業；
  - b. 執行拒絕服務的攻擊；
  - c. 干擾 Dell 資源作業，包括嘗試使 Dell 資源超負荷；或

- d. 開展網路服務營運，例如開放式 Proxy、開放式郵件轉送代理，或開放式遞迴網域名稱伺服器；
- 15. 分發、發佈、傳送或促進未經要求的群發電子郵件、促銷、廣告宣傳或招攬，包括商業廣告和資訊公告；  
或
- 16. 蒐集對違反本 AUP 之訊息的回覆。

以上列示之禁止行為範例並未涵蓋所有情形。Dell 得自行裁量並確定使用者內容或使用者對 Dell 資源之使用是否違反本 AUP。所有使用者內容，和/或透過使用者帳戶執行之操作，均由使用者自行負責。

### 違反規定的後果

使用者違反本 AUP 之行為將被視為嚴重違反 Dell 與使用者之間的合約。若使用者違反本 AUP，Dell 保留自行裁量並依與使用者簽訂之適用合約，適用其中規定的或 Dell 依法可採取的救濟措施的權利 (例如，暫停和/或終止使用者對 Dell 資源的存取權限)。

另外，Dell 保留對任何可能違反本 AUP 或濫用 Dell 資源之行為進行調查的權利。Dell 可以採取的措施包括但不限於以下措施：

1. 移除、禁止存取，或修改違反本 AUP 的任何資料或內容；和
2. 向執法部門、監管機構或其他適當的第三方報告任何可能的違法活動。必要時可能會揭露相應的使用者內容和資訊。

### 報告

若發現任何違反或涉嫌違反本 AUP 之行為，使用者必須立即向 Dell 報告。使用者應當依 Dell 的要求提供協助，以處理此類事件或違反規定的情形。任何報告均應透過以下電子郵件 ([Dell.Legal.Notices@dell.com](mailto:Dell.Legal.Notices@dell.com)) 傳送給 Dell。