.taipei 域名反濫用政策

若有任何潛在「.taipei」域名濫用的情形，可以透過以下電子郵件通報：service@nic.taipei。

(一)以下政策（“域名反濫用政策”）係根據註冊協議(Registry Agreement)規範 11 第 3 (a) 節以及管理局與註冊商協議(Registry-Registrar Agreement)第 3.5.2 節所制訂，於管理局通知註冊商後三十(30_)日生效。管理局營運.Taipei 期間，域名濫用行為不被允許。

管理局、註冊商、註冊域名持有者及一般使用網路之用戶，包括因濫用行為的性質所導致安全及穩定性的疑慮。管理局對於濫用.taipei 域名的定義，包括但不限於執行以下操作：

- 非法或詐欺行為。
- 垃圾郵件：利用電子信息系統發送未經請求的大量郵件。關於垃圾郵件的用語適用於類似濫用之行為，例如：即時訊息之垃圾郵件、網站及網路論壇的垃圾郵件。舉例來說，為了說明的目的，使用拒絕服務的電子郵件當作攻擊手段。
- 網路釣魚：使用設計偽造的網頁介面，竊取使用者機密的資料數據，例如使用者名稱、密碼或財務資料數據等。
- 網址轉接：使用者在不知情的狀況下，被導向詐欺的網站或服務，通常係 DNS 被劫持或中毒為典型特徵。
- 濫用發布惡意軟體：軟體的散播係非經使用者的允許，會滲透及破壞電腦系統。
- 實際發生的例子包括但不限於以下情形：電腦病毒、蠕蟲、鍵盤監控紀錄及木馬病毒程式。
- 快速流量主導：使用快速流量的技術來掩蓋網站及其它網路服務的位置，或避免檢測、消除記錄，或主導非法的活動。快速流量的技術經常使用 DNS 在改變主機或域名伺服器的網路位置。快速流量主導只有在管理局允許的情況下才可以進行。
- 殭屍網路的控制與指令：運作域名時，控制受感染的電腦系統、”殭屍”或直接拒絕服務作為攻擊的行為(DDoS 攻擊)。
- 散布與兒童有關的情色產品。
- 非法入侵其它電腦或網路系統：非法入侵屬於他人的電腦、帳戶或網路系統，或企圖進入他人的安全措施系統(通常被稱為駭客)。此外，任何行為均有可能被作為企圖侵入系統的活動（例如：通訊埠口掃描、秘密掃描或其他蒐集

訊息的活動)。

根據該註冊局第 3.6.5 節，管理局在其認為必要時，能夠在其自行決定下，有權拒絕、取消或轉讓任何註冊或交易，或對任何域名進行註冊局鎖定、註冊局保留或其他類似操作；(1) 以保護註冊局的完整性和穩定性；(2) 以遵守任何適用的法律、政府規定或要求、執法要求或任何爭議解決程式；(3) 為管理局及其附屬機構、子公司、高級職員、董事和員工規避任何民事或刑事法律責任；(4) 依照註冊協議的條款；或 (5) 改正管理局或任何註冊商有關域名註冊的錯誤。管理局也有權在解決爭議期間對域名進行鎖定、保留或類似操作。