90 日安全性計畫：截至 2020 年 7 月 1 日的關鍵更新

2020 年 4 月 1 日，我們**承諾**提供多項安全性與隱私權方面的強化功能。當天我們宣佈的 90 日計畫，再度強調將 Zoom 核心精神中永存的 7 大承諾落實在安全性與隱私權方面。以下是各項承諾的狀態更新：

第 1 項：從 4 月 1 日起凍結功能，並轉移我們所有工程資源以專注於處理最大的信任、安全和隱私權問題。

狀態：針對與隱私權、安全或安全性無關的所有功能，我們已採取 90 日功能凍結。我們發佈了 **Zoom 5.0**，特色在於採用 AES 256 GCM 加密、安全性圖示及「檢舉使用者」功能，並且變更會議的預設設定（預設為開啟密碼及等候室）、緊縮 Zoom Chat 控管等等。另外，我們**收購了 Keybase**，開始建立適用於所有使用者（包括免費及付費使用者）的端對端加密項目，並開始依地區提供**客製化資料路由**。

第 2 項：與第三方專家和代表使用者進行全面審查，深入瞭解並確保我們所有新使用案例的安全性和隱私權。

狀態：我們與第三方專家小組合作進行審查，並強化我們的產品、實務作法和政策，包括我們的 CISO 諮詢委員會、Lea Kissner、Alex Stamos、Luta Security、Bishop Fox、Trail of Bits、NCC Group、Praetorian、Crowdstrike、Center for Democracy and Technology，以及隱私權、安全性及包容性領域的其他組織。

第 3 項：準備透明度報告，詳盡說明與資料、記錄或內容請求有關的資訊。

狀態：我們已在定義透明度報告架構與方法上取得重大進展，該報告詳盡說明與 Zoom 收到的資料、記錄或內容請求有關的資訊。我們期盼在今年稍晚的首次報告中，提供會計年度第 2 季的資料。同時，我們最近也發佈**政府請求指南**並更新我們的隱私權政策，主要修訂方向是使內容更易於理解。前述文件可在 zoom.com/zh-tw/privacy-and-legal 找到。

第 4 項：強化我們目前的錯誤賞金計畫。

狀態：我們已研擬集中錯誤存放庫及相關的工作流程。這個存放庫接受 HackerOne、Bugcrowd 和 security@zoom.us (後者不需要 NDA) 所提供的透過 Praetorian 進行分類的弱點報告。我們透過每日會議建立持續的審查程序，並改善與安全研究人員和第三方評估人員的協調。我們也聘用弱點與錯誤賞金主管、增額多位應用程式安全工程師，同時正在招募更多安全性工程師，這些人員均將專職處理弱點事宜。

第 5 項：與業界領先的 CISO 合作，成立 CISO 委員會，促進有關安全性和隱私權最佳做法的持續對話。

狀態：我們已成立 CISO 委員會，由本公司全球副資訊長 Gary Sorrentino 領導，成員包括 36 位來自 SentinelOne、Arizona State University、HSBC 及 Sanofi 等不同產業的 CISO。本委員會過去三個月已集會四次商討重要事項，例如：區域資料中心選擇、加密、會議驗證及金鑰安全性功能。

第 6 項：進行一系列同步白箱滲透測試，以進一步發現並解決問題。

狀態：Zoom 邀集 Trail of Bits、NCC Group 與 Bishop Fox 等多家公司共同審查我們的平台。審查範圍包括 Zoom 的生產環境、核心網頁應用程式與企業網路，以及常見用戶端適用的公開 API。

第 7 項：每週三舉行每週一次的網路研討會，向我們的社群提供隱私權和安全性更新。

狀態：從 4 月 1 日起，我們每週三都會舉辦網路研討會，總共已舉辦了 13 場，邀請多位高階主管及顧問接受與會者的現場提問。

其他關鍵更新：

- 我們從 4 月 1 日起有多位關鍵領導人員上任或轉調，包括：
  - **Velchamy Sankarlingam**，產品與工程總裁
  - **Jason Lee**，資訊安全長
  - **Damien Hooper-Campbell**，多元化長
  - **H.R.McMaster**，加入 Zoom 董事會
  - **Josh Kallmer**，公共政策與政府關係全球主管
  - 弱點與錯誤賞金主管，自 7 月 13 日起
  - Andy Grant，防禦安全主管，自 7 月 13 日起
- **Zoom Phone 加入 Zoom 政府解決方案**，此調整已獲得美國聯邦風險與授權管理計畫 (FedRAMP) 授權
- 我們仍致力於擴編美國工程團隊，以支援亞利桑那州鳳凰城和賓州匹茲堡**新辦公室**激增的使用量。