**113年第六次電腦軟體共同供應契約採購-雲端服務**

**(1130206)** **雲端服務檢核表**

雲端微服務(SaaS)辧公室生產力工具(含郵件、行事曆、雲端硬碟、即時通等)共通性資通安全基本要求

以下為「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表(112.9.25版)」中，要求【普】、【中】及【高】類型之資料或系統類型應建議辦理之各項控制措施。

請投件廠商依本檢核表就所提之雲端服務產品實際情形勾選為【普級】或【中】、【高】資料或系統類型，併於廠商說明欄填覆相關對應措施，**本表格內容後續將公告於資訊服務採購網中。**

服務名稱：Google Workspace

⬜符合【普級】資料或系統類型(所有「高、中、普」標記●項目，皆須符合並進行說明，標記「高、中」標記●項目，則為選填)

**☑️**符合【中】、【高】資料或系統類型(所有項目皆須符合並進行說明)

填寫說明：

1. 圖示表示：● 建議辦理，◎ 經訂購機關評估個案有必要辦理時，▲ 依訂購機關機關資通安全責任等級辦理。
2. 普、中、高皆標示◎項目(橘色項目)，為所有廠商選填項目，提供機關個別評估時參考。

| **項目** | **子項** | **資料或系統類型** | | | **請廠商自我檢視並填寫相關說明**  填寫日期：中華民國 113年 月 日 |
| --- | --- | --- | --- | --- | --- |
| **高** | **中** | **普** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 提供服務商 | 須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準 | ● | ● | ● | **☑符合要求：**  雲端服務應具備以下三項資訊安全管理制度及雲端服務個人資訊保護相關國際或國家標準驗證(通過驗證之證明文件須顯示出雲端服務在驗證範圍內，雲端服務原廠得以合作之公有雲業者通過驗證證書代之)：   1. 資訊安全管理系統國際標準(ISO/IEC 27001)或國家標準(CNS 27001)，二者擇一。 Google Workspace 符合 ISO/IEC 27001 標準，參考資料連結： <https://cloud.google.com/security/compliance/iso-27001?hl=zh-tw> 2. 雲端服務資訊安全管理國際標準，如ISO/IEC 27017或雲端安全聯盟CSA Star(等級不限)等，二者擇一 Google Workspace 符合 ISO/IEC 27017 標準，參考資料連結： <https://cloud.google.com/security/compliance/iso-27017?hl=zh-tw> 3. 雲端服務個人資訊保護管理國際標準(ISO/IEC 27018)。  Google Workspace 符合 ISO/IEC 27018 標準，參考資料連結： <https://cloud.google.com/security/compliance/iso-27018?hl=zh-tw> |
| 須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準  (提供服務項目涉及個資時機關應納入要求) | ◎ | ◎ | ◎ | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫或提供，有證書提供者將於資訊服務採購網中揭露) Google Workspace 在接受獨立第三方的稽核之後，已獲得值得信賴的 ISO/IEC 27701 PII 處理者認證，參考資料連結：https://cloud.google.com/security/compliance/iso-27701?hl=zh-tw |
| 不得為大陸地區廠商或第三地區含陸資成分廠商 | ● | ● | ● | **☑符合要求：**   1. 雲端服務原廠不得為「中國大陸（含港、澳）地區廠商」或「經濟部投資審議委員會列為陸資來台投資事業名錄之廠商」者。 2. 經數位發展部資通安全署、國家安全會議及其他資安、國安等機關通知有資安疑慮，例如投件廠商、投件代理商所提供產品之原廠屬「第三地區含陸資成分廠商」。 Google是總部位於美國加州山景城的跨國科技公司，為Alphabet的子公司 |
| 傳輸機密性與完整性 | 廠商提供機關資料傳輸措施 | ● | ● | ● | **☑符合要求**  請詳閱雲端服務安全性檢測個案編號CS-001：雲端服務均須具備「傳輸層安全通訊協定(Transport Layer Security-TLS)」的安全通訊協定v1.2以上。 Google Workspace 支援傳輸層安全標準 (TLS) 1.0、1.1、1.2 和 1.3 版。參考資料連結：<https://support.google.com/a/answer/100181?hl=zh-Hant> |
| 事件日誌保存與可歸責性 | 應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求 | ● | ● | ● | **依雲端服務共契採購契約要求**，雲端服務與履約標的相關之日誌保存項目如下：   1. 應用程式日誌(AP log)**(必要)** Google Workspace 提供以下審查日誌類型： [管理員活動審查日誌](https://cloud.google.com/logging/docs/audit?hl=zh-cn#admin-activity)：包含應用程式設置、日曆、聊天室設定等日誌 [數據訪問審核日誌](https://cloud.google.com/logging/docs/audit?hl=zh-cn#data-access)：包含用於讀取資源分配或元數據的API調用，以及用戶創建、修改或讀取用戶提供的資源數據的API調用。數據訪問審核日誌不會記錄所有公共共享資源（即所有用戶或所有經過身份驗證的用戶都可以使用）或不需要登錄Google Cloud、Google Workspace、Cloud Identity或雲硬盤企業版本帳戶即可訪問的資源上執行的數據訪問操作。 <https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#log-types> 2. 登入日誌(logon log)**(必要)** Google Workspace 提供登入稽核日誌功能，參考資料連結：https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#2 3. 網站日誌(web log)**(必要)** Google Workspace 提供以下審查日誌類型： [管理員活動審查日誌](https://cloud.google.com/logging/docs/audit?hl=zh-cn#admin-activity)：包含應用程式設置、日曆、聊天室設定等日誌 [數據訪問審核日誌](https://cloud.google.com/logging/docs/audit?hl=zh-cn#data-access)：包含用於讀取資源分配或元數據的API調用，以及用戶創建、修改或讀取用戶提供的資源數據的API調用。數據訪問審核日誌不會記錄所有公共共享資源（即所有用戶或所有經過身份驗證的用戶都可以使用）或不需要登錄Google Cloud、Google Workspace、Cloud Identity或雲硬盤企業版本帳戶即可訪問的資源上執行的數據訪問操作。 4. 作業系統日誌(OS event log)：若無法提供請提出說明(例如:因服務底層採用Serverless等架構，無直接管理作業系統，故無法提供作業系統日誌。) Google Workspace 的使用者無法直接管理作業系統，故無法提供作業系統日誌   上述日誌項目保存期限：自資料產生起保存**至少6個月**(含契約終止或解除或期滿後)。  Google Workspace 日誌項目資料保留至少 6 個月，參考資料連結： <https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#log-types> |
| 供應商及產品安全要求 | 針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險  1.供應商安全：符合以下任一條件。  (1)廠商有公開漏洞回報應變機制  (2)廠商有第三方檢測團隊執行檢測  2.產品安全：符合以下任一條件。  (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告  (2)提供經商用弱點檢測軟體未含**中、高**等級風險之掃描報告  (3)取得第三方認可實驗室認證，如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證 | ● | ● | ● | **☑符合要求：**   1. 供應商(雲端服務原廠)安全   ⬜漏洞回報應變機制：  (請廠商依據左列說明漏洞回報與應變之機制)  **☑**有第三方檢測團隊執行檢測：請提供第三方檢測團隊資訊 Google 會定期接受多個獨立第三方機構的稽核，驗證安全性、隱私權和法律遵循方面的控管措施。Workspace 已通過標準最嚴格的認證，可協助您排除違規受罰的風險：<https://workspace.google.com/intl/zh-TW/security/>   1. 產品安全 2. 請詳閱雲端服務安全性檢測個案編號CS-002( OWASP TOP10 最新版應用程式弱點掃描) 3. 請詳閱雲端服務安全性檢測個案編號CS-003(系統弱點掃描) 4. ⬜ 本雲端服務提供App，並取得行動應用App基本資安標章。App名稱：請填本雲端服務提供之App名稱   ⬜ Android：請填版本號 ⬜ iOS：請填版本號 |
| 廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification, CMMC) | ◎ | ◎ | - | (為訂購機關依個案評估有必要辦理時參考，廠商自行選擇是否填寫) |
| 防惡意軟體 | 靜態分析 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務具備防惡意軟體之靜態分析機制)  Gmail 能防範來自不受信任寄件者的可疑附件和指令碼，同時也針對您網域中不常見的附件類型提供防護措施。不常見的附件類型常會成為惡意軟體的散佈媒介。  參考資料連結：<https://support.google.com/a/answer/9157861?hl=zh-Hant> |
| 動態沙箱分析 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務具備防惡意軟體之動態沙箱分析機制) |
| 防惡意連結 | 靜態分析 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務具備防惡意連結之靜態分析機制)  Google Workspace 提供進階安全性設定，識別短網址背後的連結、掃描連結的圖片有無惡意內容，並在您點選指向不受信任網域的連結時顯示警告訊息。參考資料連結：  <https://support.google.com/a/answer/9157861?hl=zh-Hant> |
| 動態沙箱分析 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務具備防惡意連結之動態沙箱分析機制) |
| 防釣魚郵件 | 釣魚郵件過濾 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務具備釣魚郵件過濾機制)  Google Workspace 能防範假冒網域名稱或員工姓名的行為、避免有心人士冒用您的網域寄出電子郵件，並可偵測來自任何網域的未經驗證電子郵件 (寄件者名稱旁會顯示問號)。您可以針對私人群組或所有群組啟用假冒防護功能。參考資料連結：  <https://support.google.com/a/answer/9157861?hl=zh-Hant> |
| 身分偽冒辨識(anti-spoofing) | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務具備身分偽冒辨識機制)  Google Workspace 能防範假冒網域名稱或員工姓名的行為、避免有心人士冒用您的網域寄出電子郵件，並可偵測來自任何網域的未經驗證電子郵件 (寄件者名稱旁會顯示問號)。您可以針對私人群組或所有群組啟用假冒防護功能。參考資料連結：  <https://support.google.com/a/answer/9157861?hl=zh-Hant> |
| 資料與個資  安全 | 資料分類與標籤 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務之資料分類與標籤做法)  Google Workspace 雲端硬碟能自動為新檔案套用預設分類標籤，管理員可以使用預設分類功能，自動將標籤套用至雲端硬碟檔案，以滿足貴機構的資料安全性需求。參考資料連結：<https://support.google.com/a/answer/11280938?hl=zh-Hant>  Gmail 能將電子郵件分類整理  <https://support.google.com/a/users/answer/9282734?hl=zh-Hant#sections> |
| 資料加密與存取控制 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列分別說明雲端服務資料加密與存取控制之做法)  Google Workspace 透過零信任控管機制，強制對應用程式和資料實施情境存取限制。透過情境感知存取權功能，您可以根據使用者身分、位置、裝置安全性狀態和 IP 位址等屬性，為應用程式建立精細的存取權控管安全性政策。參考資料連結：  <https://support.google.com/a/answer/9275380?hl=zh-Hant> |
| 資料外洩防護 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務如何防止資料外洩做法)  資料遺失防護 (DLP) 政策可以用來偵測電子郵件和 Google 雲端硬碟檔案中的機密資訊 (例如信用卡號碼)。您可以透過政策設定系統在偵測到電子郵件和雲端硬碟檔案中含有敏感內容時該如何處理，比如禁止使用者轉寄這些電子郵件，或是禁止使用者共用這些雲端硬碟檔案。  <https://support.google.com/a/topic/7556687?hl=zh-Hant&ref_topic=7558840> |
| 未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區 | ● | ● | ● | **☑符合要求：**  雲端服務資料儲存所在地於本國境內者，未經機關審查同意不得隨意變更至本國境外。  Google Workspace 僅能設定資料地區政策，可選擇資料地區如下：無偏好設定、美國、歐洲 |
| 資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。 | ● | ● | ● | **☑符合要求：**  雲端服務資料存取、備份及備援之實體機房所在地不得位於中國大陸（含港、澳），且不得跨該等境內傳輸相關資料。  Google Workspace 僅能設定資料地區政策，可選擇資料地區如下：無偏好設定、美國、歐洲 |
| 廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列分別說明雲端服務於虛擬主機平台內之虛擬主機映像檔強化儲存與使用安全做法)  Google Workspace 為 SaaS 服務，並未提供虛擬主機服務 |
| 身分驗證與  存取控制 | 多因子認證 | ● | ● | ● | (符合【普】【中】、【高】者必填，請廠商依據左列說明雲端服務之多因子認證做法)  Google Workspace 提供兩步驟驗證功能：<https://support.google.com/a/answer/9176657?hl=zh-Hant> |
| 零信任：身分鑑別/設備鑑別/信任推斷 | ● | ● | ◎ | (符合【中】、【高】者必填，請廠商依據左列說明雲端服務之零信任：身分鑑別/設備鑑別/信任推斷做法)  Google Workspace 內建零信任功能  身分與端點管理：  [兩步驟驗證](https://support.google.com/a/answer/9176657?hl=zh-TW)、[密碼金鑰](https://support.google.com/a/answer/13529161?hl=zh-TW)和[安全金鑰](https://support.google.com/a/answer/2537800?hl=zh-TW#zippy=,view-add-or-remove-security-keys)  [單一登入 (SSO)](https://support.google.com/a/answer/60224?hl=zh-TW)、[OAuth 2.0](https://support.google.com/a/answer/2538798?hl=zh-TW) 和 [SAML](https://support.google.com/a/answer/6087519?hl=zh-TW) 支援功能  即時的[風險控管重新驗證機制](https://support.google.com/a/answer/6002699?hl=zh-TW)  自動的[垃圾郵件、網路釣魚和惡意軟體防護機制](https://support.google.com/a/answer/9157861?hl=zh-TW)  [端點管理](https://support.google.com/a/answer/1734200?hl=zh-TW)：涵蓋行動裝置和電腦裝置  存取權與資料保護  應用程式[情境感知存取權](https://support.google.com/a/answer/9275380?hl=zh-TW)  [資料遺失防護](https://support.google.com/a/answer/9646351?hl=zh-TW&visit_id=638103591229363954-918673174&ref_topic=9646660&rd=1)控制項  雲端硬碟中的[信任規則](https://support.google.com/a/answer/10621317?hl=zh-TW)和 [AI 分類](https://support.google.com/a/answer/12676216?hl=zh-TW)  加密[傳輸中資料和靜態資料](https://workspace.google.com/intl/zh-TW/learn-more/security/security-whitepaper/page-4.html#encrypting-data-in-transit-and-at-rest)  持續監控與法規遵循  [安全性資訊主頁](https://support.google.com/a/answer/7492330?hl=zh-TW)、[快訊](https://support.google.com/a/answer/9105393?hl=zh-TW)和分析  [安全調查工具](https://support.google.com/a/answer/7575955?hl=zh-TW&ref_topic=7563358&sjid=11886085889403086716-EU)  存取權[透明化](https://support.google.com/a/answer/9230474?hl=zh-TW)、[管理](https://support.google.com/a/topic/10404276?hl=zh-TW)與[核准機制](https://support.google.com/a/topic/12962898?hl=zh-TW)  [用戶端加密](https://support.google.com/a/answer/10741897?hl=zh-TW)  [資料地區](https://support.google.com/a/answer/7630496?hl=zh-TW)、[本地資料儲存](https://support.google.com/a/answer/14339894?hl=zh-TW)和[資料保留](https://support.google.com/vault/answer/2990828?hl=zh-TW)  參考資料連結：  <https://workspace.google.com/intl/zh-TW/security/> |