# 資通安全責任及保密規範

廠商及複委外之廠商應遵守以下相關規定

一、 應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本公司資通安全管理及保密相關規定。

二、 履約人員國籍不得為中國籍，且所使用之資通設備、服務、軟體及元件不得為中國所有（大陸品牌）。

三、 執行本專案之相關程序、人員、設備及環境，應具備完善之資通安全管理措施或通過第三方驗證。

□應通過第三方驗證（ISO 27001有效之版本）。

■辦理本專案之相關程序、人員、設備及環境須具備完善之資通安全管理措施。

四、 於本專案應指定專案管理人員，專案成員應具備該領域之專業證照，以保證履約交付內容之品質，並配置「資通安全專業人員」，以及提供資通安全專業人員擁有之資通安全專業證照（數位發展部資通安全署公告之資通安全專業證照清單之一）或具有類似業務經驗證明。

五、 □ 本專案不得複委託（分包）；

■ 本專案得複委託，複委託之受託者應具備與本專案廠商相同之完善資通安全管理措施或通過第三方驗證，且不得以經濟部投資審議委員會網站公告之陸資資訊服務業者為分包廠商。廠商執行業務上若有複委託之需求，應取得本公司之同意及該複委託廠商對於機敏資料保密之書面承諾，並以書面通知本公司複委託廠商之名稱、地址及機敏資料處理之進行適當之監督。

六、 □ 本專案業務涉及國家機密，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

七、 □ 應提供本專案資通系統（客製化）之安全性檢測證明，其檢測工具不得為自由軟體，且需提供檢測工具名稱、版本及原始報告，以及確認檢測時之弱點資料庫已更新至最新版本（檢測報告必須載明檢測日期及檢測工具名稱、版本，以及弱點資料庫更新日期）。

檢測項目如下：

□ 系統主機弱點掃描

□ 網頁弱點掃描

□ 滲透測試

□ 原始碼檢測

承前項：□本專案資通系統為本公司核心資通系統或本專案金額達新臺幣一千萬元（含）以上，應由第三方進行安全性檢測及提供檢測報告，第三方機構應為現行「電腦軟體共同供應契約」之資通安全服務暨資訊服務廠商，且檢測項目須與廠商「電腦軟體共同供應契約」合格項目相符，所提供之檢測報告規格、要求亦須符合「電腦軟體共同供應契約」要求。

八、 本專案資通系統開發與維護如使用第三方軟體或元件，應提供第三方元件清單（包含版本及是否可以持續更新等資訊），並說明其來源與授權證明。

九、 □ 應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合本公司對系統品質及資通安全要求。

十、 □ 本專案標的涉關鍵基礎設施(或本公司指定之設施)，廠商及分包廠商之履約人員於進場或參與工作前，應提出 3 個月內核發之「警察刑事紀錄證明」（外國人應提出該國籍政府核發之類似文件，並經公證或認證。但申請入國簽證時，已備行為良好之證明文件者除外）；其證明內容應記載無犯罪紀錄，並經公司審核同意，始得進場或參與工作。屬臨時性進場者（例如送貨司機及其隨車人員）得免提送上開證明文件，但應接受本公司或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督管理。

十一、於執行本專案及保固服務期間，若知悉或發生資通安全事件時（含本專案範圍及廠商內部管理範圍），應於 1 小時內通知本公司及採行補救措施。

十二、本專案（含保固）終止或解除時，廠商應確返還、移交、刪除或銷毀履行契約而持有之資料，並提供切結書與說明資料之刪除或銷毀方式。

十三、於本專案（含保固）期間，本公司得視需求或發生可能影響本專案之資通安全事件時，對廠商及分包廠商實施現場實地資安稽核，稽核範圍為本專案相關之程序、人員、設備及環境，廠商不得拒絕。稽核結果若不符合本專案約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本公司通知後應於期限內完成改善，未依限完成者，依契約違約條款辦理。

十四、廠商及其指定之代理人、專案經理、專案顧問、員工等，於本專案進行期間因進行調查、搜集依合約所產生或所接觸之資料，非經本公司同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知悉之上述資料，廠商須負保密責任。

十五、資料保密期限，不受本專案工作完成（結案）及廠商不同工作地點及時間之限制，廠商持有或獲知資料，未經本公司書面同意或授權，不得洩漏或公開於第三者。

十六、廠商違反本保密之規定，致造成本公司或第三者之損害或賠償，廠商同意無條件負擔全部責任，包括因此所致本公司或第三人涉訟，所須支付之一切費用及賠償。於第三人對本公司提出請求訴訟，經本公司以書面通知廠商提供相關資料，廠商應合作提供絕無異議。

十七、廠商參與專案之人員於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切本公司未標示得對外公開之商業秘密，以及本公司依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於本公司指定之處所內使用之。非經本公司事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至本公司或本公司所指定處所以外之處所。

十八、上述個人知悉或取得本公司商業秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。上述個人同意因執行本專案所接觸之商業秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員，並要求其恪守保密義務。

十九、上述個人在下述情況下解除其所應負之保密義務：原負保密義務之資訊，由本公司提供以前，已合法持有或已知且無保密必要者。原負保密義務之資訊，依法令業已解密、依契約本公司業已不負保密責任、或已為公眾所知之資訊。

二十、原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

二十一、上述個人若違反本保密之規定，本公司得請求上述個人及其任職之廠商賠償本公司因此所受之損害及追究上述個人洩密之刑責，如因而致第三人受有損害者，上述個人及其任職之廠商亦應負賠償責任。

二十二、上述個人所負之保密義務，於保密有效期間內，不因離職或其他原因不參與本案而失其效力。

廠商名稱：

廠商章及負責人章：

中 華 民 國 113 年 月 日