資通安全補充約定

一、名詞定義

（一）資訊軟硬體：指運用資訊科技處理資料建立、運算、儲存、傳送和保護之系統及軟硬體設備。

（二）資訊服務：指提供與資訊軟硬體有關之服務，包括雲端服務、整體規劃、系統整合、系統稽核、系統管理、網路管理、軟體開發、軟體驗證、軟體維護、硬體維護、硬體操作、機房設施管理、備援服務、網路服務、顧問諮詢、資料庫建置、資料處理、資料登錄或訓練推廣等服務。

（三）資訊系統：指所有處理業務資料、業務流程、為民服務之網頁應用軟體、行動應用軟體、資訊平臺、網站等軟體系統。

（四）行動應用軟體：指由使用者自行下載安裝於智慧型行動裝置之軟體。

二、廠商提供或使用之資訊軟硬體或資訊服務，如因特殊事由，部分無法符合本約定時，廠商應事先具體提出無法符合項目、原因、資通安全風險及替代改善措施，經機關同意接受後，始得排除適用；前開得排除適用範圍，不包括法令規定要求之必要事項。

三、廠商提供之資訊軟硬體及資訊服務，應符合下列法令規定：

（一）資通安全管理法及其相關子法(網址：https://law.moj.gov.tw/)。

（二）行政院所訂頒之各項資通安全規範及標準(網址：https://www.nccst.nat.gov.tw/)。

（三）臺北市政府訂頒之臺北市政府資通安全管理規定(網址：https://www.laws.taipei.gov.tw/Law)。

四、資訊系統應符合下列基本設計要求，並應列為驗收要項：

（一）資訊系統傳輸應採用 HTTPS(透過 SSL 或 TLS 等加密協定)協定以確保機敏資料以密文方式傳輸。

（二）資訊系統中除了公開區域外，任何執行功能及存取資源動作前，應檢查使用者已通過身分驗證且其具備權限可執行該功能或存取資料。

（三）資訊系統重要交易行為，於執行前應再次確認獲得授權，要求使用者再次進行身分驗證。

（四）資訊系統身分驗證或重要交易行為身分驗證，機關得要求配合機關使用者驗證及管理機制，或採用多重因素身分驗證以強化安全性。

（五）資訊系統不得以任何方式側錄、保存使用者密碼。

（六）資訊系統若具有與其他外部系統或資料庫等連線的需求，不可將連線之身分驗證資訊(帳號、密碼等)寫於程式原始碼中。

（七）身分驗證資訊若以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。

（八）資訊系統對於境外軟體存取、使用者登入、重要資料異動及存取等事件應進行日誌記錄，日誌檔應定時自動備份，並避免未經授權存取及刪除。

五、資訊系統在提供或使用前應完成下列資安測試或檢測：

（一）資訊系統應完成靜態應用程式安全測試（Static Application Security Testing，SAST），進行原始碼檢查，確認不存在 OWASP（The Open Web Application Security Project，開放網站應用程式安全專案）歸納公布之最新版十大網路資安風險（OWASP Top 10）或其他中高等級以上風險後，始得進行後續軟體安裝及其他整合或黑箱測試程序。但

廠商所提供或使用資訊系統，如係無法取得原始碼之既有軟體產品，得依第二點規定提出排除適用申請。

（二）廠商所提供或使用之資訊系統如係網頁型應用程式或網站，應至少通過下列資通安全測試，始得開放使用：

1.動態應用系統安全測試（Dynamic Application Security Testing，DAST），以自動化工具進行黑箱測試（Black-Box Testing），模擬駭客的攻擊行為，測試系統有沒有漏洞，不得存在 OWASP（The Open Web Application Security Project，開放網站應用程式安全專案）歸納公布之最新版十大網路資安風險（OWASP Top 10）或其他中高等級以上風險。

2.壓力測試（Stress Testing），在機關有線區域網路環境，單一應用程式伺服器同時上線人數至少【○人】（由機關於招標時視需要及業務性質載明，未載明者以 200 人計），壓力測試時間不少於【○小時】（由機關於招標時視需要及業務性質載明，未載明者以 10 小時計），應符合下列標準：

(1)登入：平均反應時間小於【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 4 秒計），連結成功率【○%】（由機關於招標時視需要及業務性質載明，未載明者以 99%計）以上；反應時間超過【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 6 秒計）之數量，不超過【○%】（由機關於招標時視需要及業務性質載明，未載明者以 1%計）。

(2)網頁瀏覽（存取）：平均反應時間小於【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 4 秒計），連結成功率【○%】（由機關於招標時視需要及業務性質載明，未載明者以 99%計）以上；反應時間超過【○秒】（由機關於招標時視需要及業務性質載明，未

載明者以 6 秒計）之數量，不超過【○%】（由機關於招標時視需要及業務性質載明，未載明者以 1%計）。

(3)查詢：平均反應時間小於【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 4 秒計），連結成功率【○%】（由機關於招標時視需要及業務性質載明，未載明者以 99%計）以上；反應時間超過【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 6 秒計）之數量，不超過【○%】（由機關於招標時視需要及業務性質載明，未載明者以 1%計）。

(4)交易：平均反應時間小於【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 4 秒計），連結成功率【○%】（由機關於招標時視需要及業務性質載明，未載明者以 99%計）以上；反應時間超過【○秒】（由機關於招標時視需要及業務性質載明，未載明者以 6 秒計）之數量，不超過【○%】（由機關於招標時視需要及業務性質載明，未載明者以 1%計）

（三）廠商所提供或使用之資訊系統如係行動應用軟體，應於上架至軟體市集、或以其他方式正式提供使用者下載安裝前，通過「行動應用 App 基本資安制度推動委員會」認可之「行動應用 App 基本資安檢測實驗室」行動應用軟體安全檢測，並取得「行動應用 App 基本資安檢測合格證明書」。於上線後次年起，該行動應用軟體生命週期內每年至少通過複檢一次。但廠商所提供或使用之行動應用軟體，如係非本國廠商開發之軟體產品，或有其他特殊情形，進行前開軟體安全檢測確有困難時，得依第二點規定提出排除適用申請。

六、資訊系統所使用之網址及開發人員資料，應符合下列規定：

（一）廠商所提供或使用之資訊系統如係網頁型應用程式或網站，使用之網址由機關要求或同意後訂之，不得以 IP 位址為網

址，並以使用「.taipei.gov.tw」、「.gov.taipei」為其上層域名為原則。但有特殊情形，經機關要求或同意者，不在此限。

（二）廠商所提供或使用之資訊系統如係行動應用軟體，如需上架至軟體市集，開發者原則應為「臺北市政府」。經機關要求或同意，得以其他廠商(機構)為開發者(不含個人)，且該廠商(機構)，應為國內外合法之廠商(機構)，並能提供聯繫方式及資訊。

七、其他

（一）實際提供資訊軟硬體或資訊服務之分包廠商不得為經濟部投資審議委員會網站公告之陸資資訊服務業者，亦不得使用前開陸資企業出品之產品。

（二）契約如包含資訊系統開發或資訊服務，原則應全部於我國境內進行及完成，如部分或全部於我國境外辦理者，應事先通知機關並同意後，始得為之。前開境外地區不得為中國大陸、香港、澳門或其他經機關評估具資安風險地區。

（三）下列人員不得為契約專案團隊成員或派駐人員或參與軟體開發、測試：

1.任職於中國大陸、香港、澳門或外國公營機構或政府機關者。

2.任職於經濟部投資審議委員會網站公告之陸資資訊服務業者。

3.具中國大陸國籍者。

八、資通安全檢測及稽核

（一）契約資訊軟硬體及資訊服務部分合計金額如達新臺幣一千萬元以上者，廠商應接受並配合機關或其所委託之第三方進行

資通安全檢測；其範圍包括廠商以及實際提供或使用資訊軟硬體及資訊服務之分包廠商。資通安全檢測項目由機關視專案性質訂之。

（二）廠商提供或使用資訊軟硬體或資訊服務，如發生資通安全事件，或有其他重大違反資通安全規定之虞，機關或其所委託之第三方得對廠商進行資通安全稽核；資通安全稽核範圍應包括廠商以及實際提供或使用資訊軟硬體及資訊服務之分包廠商。資通安全稽核項目，由機關視實際事件狀況訂之。

（三）資通安全檢測或稽核如發現缺失，廠商應依機關要求於期限內完成改正。

九、罰則

（一）本約定所定違約金如下，每點新臺幣_____元（由機關於招標時載明，未載明者每點以新臺幣 1,000 元計）。

（二）依第三點約定，廠商違反資通安全法令規定，如法規另訂罰則時，依其罰則；未訂罰則時，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（三）廠商提供或使用之行動應用軟體違反第三點第二款、第三款約定，未經軟體安全檢測合格，即上架至軟體市集，或以其他方式正式提供使用者下載安裝，或提供契約使用，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（四）廠商違反第五點第一款約定，資訊系統未完成靜態應用程式安全測試，進行後續軟體安裝及其他整合或黑箱測試程序，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未

改正者，按次連續計罰。

（五）廠商違反第五點第二款約定，網頁型應用程式或網站未完成資通安全測試，即開放使用者，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（六）廠商違反第五點第三款約定，行動應用軟體未完成軟體安全檢測，即上架至軟體市集、或以其他方式正式提供使用者下載安裝，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（七）廠商違反第六點第一款約定，網頁型應用程式或網址，未經機關同意而使用，並對外發佈使用者，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（八）廠商違反第六點第二款約定，未經機關同意而未以臺北市政府作為其上架至軟體市集之行動應用軟體開發者，或未依機關要求以其他廠商(機構)為開發者，並使用或提供下載安裝者，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（九）廠商違反第七點第一款約定，分包廠商為經濟部投資審議委員會網站公告之陸資資訊服務業者或使用陸資企業出品產品，計罰□【○點】□【○元】□【契約價金○%】（由機關於招標時擇一載明），並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

（十）廠商違反第七點第二款約定，非經機關同意於境外地區進行

或完成資訊系統開發或資訊服務，計罰□【○點】□【○元】□【契約價金○%】(由機關於招標時擇一載明)，並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

(十一)廠商違反第七點第三款約定，使禁用人員為專案團隊成員、派駐人員或參與軟體開發、測試，每一人計罰□【○點】□【○元】□【契約價金○%】(由機關於招標時擇一載明)，並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

(十二)廠商違反第八點第一款、第二款約定，不接受並配合機關或其所委託之第三方進行資通安全檢測或稽核，計罰□【○點】□【○元】□【契約價金○%】(由機關於招標時擇一載明)，並應於要求期限內完成改正，限期改正仍未改正者，按次連續計罰。

廠商有前項各款情形致產生負面輿論或民意機構批評，減損機關聲譽，情節重大者，得加倍計罰。

廠商有第一項各款情形致造成機關三級以上資通安全事件，情節重大者，機關得終止或解除契約。