**附件六：廠商資通安全責任事項**

1. 辦理受託業務之相關程序及環境，應填寫「委外廠商資通安全管理措施說明表」佐證具備完善之資通安全管理措施，或通過第三方驗證(TAF認證機構)，如受託業務涉及提供雲端服務者，應提供ISO 27001標準認證。
2. 應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員，負責推動、協調及督導資通安全管理事項。
3. 經本會同意，委外廠商始得將受託業務分包予第三人，委外廠商須要求並監督該第三人應具備與委外廠商同等之資通安全維護措施及標準，並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。
4. 辦理客製化資通系統之開發，若涉及利用非自行開發之系統或資源者，應標示非自行開發之內容與其來源及提供授權證明。
5. 辦理受託業務，違反資通安全相關法令或知悉資通安全事件發生時，應立即通知本會承辦單位及採行必要之補救措施，並應配合本會之資通安全事件通報及相關處理作業。委外廠商未為通知或未配合本會相關處理作業者，應就本會因此所生之一切損害負賠償責任。
6. 委託關係終止或解除時，委外廠商就履行委託契約而持有之資料應返還、移交予本會，並刪除或銷毀之。
7. 委外廠商同意本會得定期或於知悉發生可能影響本案之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。
8. 委外廠商受託業務涉及資通訊軟體、硬體或服務等相關事務者，執行本案之團隊成員不得為大陸籍人士，並不得提供及使用大陸廠牌資通產品或服務。
9. 受託業務涉及國家機密時，執行業務之相關人員應接受適任性查核，並受國家機密保護法規定之管制。

委外廠商應確保執行該業務之所屬人員及可能接觸該國家機密之其他人員，無下列事項：

1. 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。
2. 曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。
3. 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。
4. 招標公告、招標文件或契約所載其他與國家機密保護相關之具體項目。
5. 委外廠商執行受託業務之人員進出本會範圍應受限制。委外廠商駐點人員使用之資通設備，應依本會「資通服務廠商派駐人員資通安全同意表」之要求遵守相關安全管控措施。
6. 委外廠商駐點人員若要更換或撤離，應填寫「資通服務廠商派駐人員撤離資料表」。