**資拓宏宇國際股份有限公司資通安全附加條款**

1. 目的

資拓宏宇國際股份有限公司(以下簡稱甲方)為確保其重要資訊、網路及資通訊服務之安全性，特訂定本附加條款，並將本附加條款納入與廠商(以下簡稱乙方)之簽署之○○○○○○合約(以下簡稱本案)中，以為甲、乙雙方信守。

1. 廠商資格與通則
	1. □乙方須為本案採購設備之製造商或其在台公司或分公司、或其授權在台之代理商或經銷商。如乙方為代理商或經銷商時，須於提出其產品之製造商或其從屬公司所授權代理或授權經銷之證明文件暨連帶保固證明正本，以證明其在中華民國台灣地區設有經正式授權之代理商或經銷商，並確保保固期內維護及技術支援無虞。
	2. 乙方應保證履約標的之生產、研發、製造或提供非屬行政院核定之危害國家資通安全產品之廠商及產品清單(含軟體、硬體及服務)，且乙方應保證至本合約期滿，如有保固期，則至保固期滿。購案如涉及資通訊設備之維護/維運作業，乙方應保證其非屬行政院所禁止之廠商，或受該等廠商投資之廠商。
	3. 乙方履約之相關程序及環境，應採取適當之資通安全相關維護措施，或出具通過第三方驗證之證明(包含以下勾選項目)，且證書為有效期間內。

□ISO 27001(資訊安全管理系統認證)

□ISO 27701(個人資料隱私管理系統認證)

□BS 10012(個人資訊管理系統認證)

□ISO 27017(雲服務資訊安全管理系統認證)

□ISO 27018(雲服務個資保護管理系統認證)

□ (可自行增加)等國際標準認證

* 1. 乙方應保證履約標的之生產、研發、製造或提供非屬主管機關核定之危害國家資通安全產品，且乙方應保證至本合約期滿，如有保固期，則至保固期滿。
	2. 本案如涉及資通訊設備之維護/維運作業，乙方應保證其非屬主管機關所禁止之廠商，或受該等廠商投資之廠商。
	3. 上述乙方提供之證明文件，如有偽造或不實，或在履約期間發現或違反本條規定者，甲方得立即解除或終止契約，如有損害並得請求賠償。
	4. 乙方應遵守履約之甲方業主[[1]](#footnote-1)所從事業務之中央目的事業主管機關相關規範與要求；若甲方業主屬公務機關或特定非公務機關，乙方應遵守《資通安全管理法》及其子法等一切相關規定，並配合甲方業主之稽核作業等相關要求。
1. 履約標的(請勾選)
2. **□套裝產品(包括軟體、硬體及服務，但不含任何客製)**
3. 乙方應保證所提供之套裝產品，未含有任何軟硬體木馬、後門程式、間諜程式或其他非正常產品應具有之元件或功能，乙方並應依甲方指示與要求提供佐證[[2]](#footnote-2)。
4. 乙方交付之套裝產品，應提供內含之軟體清單(包括軟體名稱、版本、序號等)。**□**若使用第三方組件(含開源軟體)，應交付第三方組件清單(包括但不限於：組件名稱、出處資訊、原始著作權利聲明、免責聲明、版本資訊)，且應保證已取得該第三方權利人授權甲方使用，該第三方組件之授權範圍及授權時間應符合甲方本案需求。
5. 套裝產品若內含管理工具或管理web頁面，應提供其使用之網路服務及服務埠清單，□並應具備限制特定設備或來源(如：IP位址與Port)連入服務之功能。
6. 乙方交付之套裝產品，合約期間暨後續保固期間應依下列條件辦理：
	1. 若有新發現之漏洞、原製造商公布重大更新或軟體有新版本，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版。
	2. 若因系統環境相容性原因，原廠不建議修補時，乙方須出具原廠之說明文件與補償性措施，並取得甲方同意。
7. □涉及公眾電信網路，須提供「符合ITU、3GPP 或NIST發布之資通安全規定」證明。
8. □屬於「台灣資通產業標準協會」已公布之物聯網產品驗證項目[[3]](#footnote-3)，須提供通過物聯網資安檢測或取得物聯網資安標章之證明。
9. **採購設備器材(共分2大類，請依設備類型勾選)**

### □資通訊設備[[4]](#footnote-4)(網通設備/專用伺服器主機/終端設備)

1. 乙方應保證所提供之設備暨內含之韌體/作業系統/軟體，未含有任何軟硬體木馬、後門程式、間諜程式或其他非正常產品應具有之元件或功能，並提供佐證。
2. 乙方應提供甲方採購設備之製造商、韌體/作業系統版本、修補程式版本、必要開啟之功能、必要開啟之網路服務及服務埠、必要帳號與其用途、取得修補方法之管道等資訊。
3. 乙方交付之設備，應提供內含之軟體清單(包括軟體名稱、版本、序號等)。**□**若使用第三方組件(含開源軟體)，應交付第三方組件清單(包括但不限於：組件名稱、出處資訊、原始著作權利聲明、免責聲明、版本資訊)，且應保證已取得該第三方權利人授權甲方使用，該第三方組件之授權範圍及授權時間應符合甲方本案需求。
4. 乙方交付之設備應提供以下功能:
5. 具備建立、修改、與刪除/停用帳號名稱、通行碼或憑證之功能(含預設帳號與通行碼)，且設備不應將帳號名稱、通行碼與憑證寫死在軟韌體中。
6. 具備身分認證機制或支援TACACS+/RADIUS等認證機制，以可滿足以下要求：
7. 依甲方之要求設定通行碼安全性 (含最小長度、複雜度、變更週期)功能。
8. 提供鎖定帳戶機制。
9. 提供通行碼重設機制。
10. 身分驗證相關資訊不以明文傳輸。
11. 本機不以明文儲存通行碼。
12. 具備管理者權限管理功能，並可建立、修改、與刪除/停用個別帳號權限。
13. 具備維運管道連線逾時管理功能，當連線達到閒置時間時，應予以中斷服務。
14. 具備限制特定設備或來源(如：IP位址與Port)連入服務之功能。
15. 無線通訊應具備安全的加密保護機制(如WiFi須使用WPA2以上、Zigbee與藍芽應提供AES 128 bit以上加密方式) 。
16. 維運服務應採用無弱點之加密連線協定(如TLS 1.2、TLS 1.3)。
17. 如具備自動校時功能，並可由甲方自行指定校時伺服器。
18. 具備更新設備軟韌體功能。
19. 如具備以下日誌功能，若因設備功能限制無法支援，須出具說明文件，並取得甲方同意。
	1. 具備稽核日誌功能，包含系統運作日誌、帳號登出入日誌、帳號操作指令日誌。
	2. 具備日誌留存與輪替(rotate)功能，設備本身日誌留存容量至少須可保存□\_\_\_\_\_\_GB或 □\_\_\_\_\_\_日曆天或□最新的\_\_\_\_\_\_筆紀錄。
	3. 具備日誌外拋功能，可依甲方指定之收容格式及傳送方式拋送日誌。
20. □具備可關閉任一服務與通訊埠之功能。
21. □具備可綁定維運管道(含out-of-band)於特定實體網路通訊埠之功能。
22. 乙方交付之設備應至少完成以下事項:
23. 移除或關閉不需使用之功能服務、系統元件或偵錯介面。
24. 移除或關閉不需使用之網路服務及服務埠。
25. 刪除或停用不必要之帳號。
26. 應採用安全穩定之軟、韌體版本。
27. □於交貨驗收前，交付之設備不得含有中等級以上弱點(CVSS[[5]](#footnote-5) v3評分 4.0 分以上之 CVE[[6]](#footnote-6))(範圍包括設備所有網路介面之所有網路通訊埠服務、設備之服務及管理網頁)，並提供佐證資料供甲方驗收。
28. 乙方交付之設備，合約期間暨後續保固期間應依下列條件辦理:
29. 禁止使用已EOS(End-Of-Service)之作業系統與應用程式，但因設備原廠要求而必須使用該等系統與應用程式始能達成甲方本案需求者，須經甲方同意後為之。
30. 若有新發現之漏洞、原製造商公布重大更新或韌體有新版本，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版。
31. 若因系統環境相容性原因，原廠不建議修補時，乙方須出具原廠之說明文件與補償性措施，並取得甲方同意。
32. □涉及公眾電信網路，須提供「符合ITU、3GPP 或NIST發布之資通安全規定」證明。
33. □屬於「台灣資通產業標準協會」已公布之物聯網產品驗證項目[[7]](#footnote-7)，須提供通過物聯網資安檢測或取得物聯網資安標章之證明。

### □伺服器主機[[8]](#footnote-8)

1. 乙方應保證所提供之設備暨內含之韌體/作業系統/軟體，未含有任何軟硬體木馬、後門程式、間諜程式或其他非正常產品應具有之元件或功能，並提供佐證。
2. 乙方應提供甲方採購設備之製造商、韌體/作業系統版本、修補程式版本、必要開啟之功能、必要開啟之網路服務及服務埠、必要帳號與其用途、取得修補方法之管道等資訊。
3. 乙方交付之設備應提供以下功能:
4. 具備建立、修改、與刪除/停用帳號名稱、通行碼或憑證之功能(含預設帳號與通行碼)，且設備不應將帳號名稱、通行碼與憑證固定保留(hard-coding)在軟韌體中。
5. 具備更新設備軟韌體功能。
6. 乙方交付之設備應至少完成以下事項:
7. 移除或關閉不需使用之功能服務、系統元件或偵錯介面。
8. 移除或關閉不需使用之網路服務及服務埠。
9. 刪除或停用不必要之帳號。
10. 應採用安全穩定之軟、韌體版本。
11. □於交貨驗收前，交付之設備不得含有中等級以上弱點(CVSS v3評分 4.0 分以上之 CVE)(範圍包括設備所有網路介面之所有網路通訊埠服務)，並提供佐證資料供甲方驗收。
12. 乙方交付之設備，合約期間暨後續保固期間應依下列條件辦理:
13. 禁止使用已EOS(End-Of-Service)之作業系統與應用程式，但因設備原廠要求而必須使用該等系統與應用程式始能達成甲方本案需求者，須經甲方同意後為之。
14. 若有新發現之漏洞、原製造商公布重大更新或韌體有新版本，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版。
15. 若因系統環境相容性原因，原廠不建議修補時，乙方須出具原廠之說明文件與補償性措施，並取得甲方同意。
16. **□委外軟硬體維護(包含於甲方業主環境)**
17. 乙方進行維護作業時，不論是在甲方或其業主之環境執行，乙方人員均應遵守甲方與甲方業主之要求(包括但不限於保密義務、個資保護、資訊安全、門禁管理等規定)辦理。
18. 乙方所維護之軟硬體，合約期間內應依下列規定辦理:
19. 若有新發現之漏洞、原製造商公布重大更新或韌體有新版本，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版。
20. 若因系統環境相容性原因，原製造商不建議修補時，乙方須出具原製造商之說明文件與補償性措施，並取得甲方同意。
21. 乙方及其人員應遵守甲方之委外廠商[遠端]連線維護作業遵循事項、實體安全及門禁管理辦法、機房管理辦法等相關規定，執行相關設備安裝、維護、調校等或其他作業，非經甲方許可，不得接觸甲方內部等級(含)以上之資料。
22. 乙方工作人員均應簽署個人「保密切結書」，並遞交甲方指定單位審核；□乙方應將乙方工作人員之詳細名冊送甲方指定單位備查，俾供現場核對前往施工之乙方人員身分，落實甲方資通安全管理。
23. 乙方工作人員應於現場（機房）主管指定安排之工作區（所指定之機房或辦公場內的位置）內作業，其進出及作業管理由各機房主管單位依安全檢查及機房門禁管理並留下紀錄。
24. 乙方工作人員非經甲方同意，不得自行攜入資通訊處理設備至甲方工作區域及機房，且不得私自接取甲方之網路。
25. 派駐甲方服務之人員，若因業務或管理之必要，長期借(租)用甲方終端設備，且使用甲方內部網路者，所使用之終端設備須依甲方資訊安全相關規定安裝安控軟體。若為乙方自備專屬電腦，亦應遵循甲方所有資安相關管控規定，例外情形應取得甲方同意，設備攜回前，應確實依甲方相關規定及程序，刪除儲存媒體中之資料，並應經甲方權責主管確認。
26. 乙方工作人員未經甲方權責主管核准不得進入甲方系統；維護服務需使用甲方資料時，須由甲方授權及監督，依申請內容、範圍及步驟執行，工作結束乙方應即清除產出之非必要資料；未經甲方核准，乙方不得攜出所存取資料。如儲存媒體損壞後由甲方以物理性破壞或其他資料無法還原之方式處理。
27. 乙方工作人員因本案需要申請登入設備之權限時，應依甲方之帳號權限申請與管理要求辦理，申請業務所需之最小權限，至少每六個月確認一次使用情況，不得再轉交其他人員使用。如乙方工作人員離職、職務異動或其他事由等，不再使用該帳號，應事前告知甲方異動其權限。
28. 乙方進行軟硬體安裝或維護時，設備間不得使用互跳(或間接)方式登入(如RDP、SSH、Rlogin、Telnet等)，應使用甲方指定之維運管道或管制規定辦理。
29. 乙方不應企圖試探系統或服務可疑的安全弱點。
30. 乙方作業過程中如違反甲方及/或甲方業主之資訊安全政策或相關規範、發現或懷疑系統遭受不當操作及使用(含稽核機制失效、系統嚴重錯誤)或其他資通安全事件，應於發現後□15□30分鐘內通報甲方，並協助甲方執行適當之應變措施。
31. 乙方工作人員因本案所做之所有異動(如系統升版、改接、更新Patch、測試作業及參數異動)，應事先提出申請，經甲方審核同意後，始可依甲方規定之系統變更作業程序進行作業。乙方工作人員應確實依申請內容、範圍及步驟執行，不得任意變更作業內容，作業期間應啟動日誌(log)紀錄，不得關閉，例外情形應取得甲方同意。
32. 乙方對甲方所做之軟硬體安裝、故障修復或定期維護服務皆須詳實記錄於維護紀錄中，內容應包含維護期間(記載時間至分鐘)、異動原因及異動內容，維護紀錄(如完工報告單、故障維修紀錄、保養紀錄單等)經甲方確認後提供乙份存於甲方。
33. 乙方因本案協助甲方進行緊急連線診斷時，除須事先申請經甲方許可之連線管道外，每次使用皆應經甲方事前核准。未經甲方事前書面同意，不得向第三人透露甲方的連線程序及通行碼(含雙因子認證使用之載具)，或轉接於第三人。
34. 乙方執行本案應配置充足且經適當之資格訓練、擁有資安專業證照或具有類似業務經驗之資安專業人員。
35. 乙方同意甲方得視需要就本案執行情形為適當之訪查、監督、確認及紀錄，並得向乙方索取相關資料，乙方不得規避、妨礙或拒絕，同時，乙方應針對風險事項於甲方指定時間內完成修補改善。
36. 乙方若有服務項目異動之狀況，應於■一個月□三個月□ 日曆天前通知甲方，並取得甲方同意。
37. **□委外開發系統(含軟體/程式/APP)**
38. 乙方應保證所交付之系統，未含有任何軟硬體木馬、後門程式、間諜程式或其他非正常產品應具有之元件或功能，亦不得具備已被資訊安全組織公布，易遭駭客攻擊之任何弱點，包括但不限於OWASP(Open Web Application Security Project)最新發布之前十大安全問題種類、資訊安全教育研究組織公布之CWE/SANS TOP 25最危險之程式錯誤、WEB軟體安全協會(WASC)公布之最新攻擊與弱點及未來發布之安全問題種類，並提供佐證及安全性檢測證明；若發現交付之系統含有弱點，乙方應負無償修補之責，並應於約定期限內，完成修補至符合甲方與其業主之要求。
39. □乙方應保證負責本案之系統開發人員須完成相關「安全程式碼撰寫」之教育訓練或認證。
40. 乙方應建立或使用甲方於本案之程式原始碼版本管理之安控措施及管理監督程序，非經甲方事前書面同意，乙方不得使用軟體原始碼代管服務平台(如：GitHub或其他可公開存取平台)進行本案委託開發系統之程式原始碼版本管理。
41. 乙方交付之系統不得使用已EOS(End-Of-Service)產品(包含作業系統、應用程式、第三方組件等)，若因設備原廠要求或其他原因而必須使用始能達成甲方本案需求者，乙方須於開發前告知甲方並經甲方同意後為之。
42. 乙方交付之系統，應至少完成以下事項:
43. 移除或關閉不需使用之功能服務、系統元件或偵錯介面。
44. 移除或關閉不需使用之網路服務及服務埠。
45. 刪除或停用不必要之帳號。
46. 應採用安全穩定之軟體版本。
47. □提供本案系統發展生命週期之相關文件，需求分析文件應包含安全性需求(含機密性、可用性、完整性)分析結果，並於設計文件載明實現的方法或技術，前述需求分析與設計內容應經甲方同意後實作相關控制措施，並提供測試結果。
48. 乙方交付之系統應提供以下功能:
49. 嚴格限制未經授權資料之存取，並依使用者角色權限及安全等級明確區分及授權，程式存取資料庫不可使用特權或全域帳號(含DBA權限的帳號)並最小化開放可存取之資料表欄位(如透過Stored Procedure(預儲程序)、Function(自定函數)、View(檢視表)實現抽象化存取)。存於系統之使用者通行碼應加密。若有特殊例外情形，應檢附必要性說明與強化安控措施，並取得甲方同意。
50. 修改預設帳號或通行碼之功能。
51. 應建立輸入驗證機制，限制並過濾可能作為系統命令執行、資料庫或LDAP查詢語法之輸入字元，且拒絕任何潛藏惡意字串之使用者輸入。
52. 如本案具備個資存取行為之系統，須提供個資存取軌跡紀錄留存及支援傳送軌跡紀錄至甲方指定系統之功能。
53. 如本案具備存取憑證產生與驗證之系統，應確保產生之存取憑證(Access Token)與驗證機制的安全性，避免洩漏存取憑證相關資訊(含存取憑證本身、產生演算法與產生因子等)，並應建立存取憑證(Access Token)之合法性驗證機制，若遇用戶端提出非由系統核發之存取憑證，應立即中止該連線。
54. 乙方交付甲方之系統應具備身分認證機制安全，應至少包含以下:
55. 通行碼長度應超過(含)■8碼□12碼或□依甲方、甲方業主之密碼政策辦理(以較嚴格者為凖)，且檢查通行碼複雜度及變更週期。
56. 提供帳戶鎖定機制。
57. 提供通行碼重設機制，並於確認使用者身分後，發送一次性及具有時效性符記。
58. 身分驗證相關資訊，應採加密或雜湊函式處理後儲存，不以明文或編碼形式儲存或傳送，並支援演算法最大長度金鑰。
59. 具備身分權限管控之系統，其登入頁面須具備防範自動化程式攻擊或密碼更換嘗試之機制，且所有程式頁面均須檢查是否通過身分認證及具備存取權限。
60. 如本案具備個資隱私或金融交易功能之系統應支援雙因子或多因子驗證機制，多因子驗證機制若採簡訊驗證等輸入字串形式，驗證碼應符合隨機性與一次性要求，且限定輸入錯誤與時效之失效機制。
61. 若具多種登入方式(如Ｗeb, APP, PC client等)，須具備相同認證強度。
62. 身分授權機制不得未檢查來自使用者之參數即直接引用，避免有提權之情形發生。
63. 存取憑證須確認經完整身分認證後，方能產生提供使用者，並於使用者提交存取憑證時，須驗證其為系統所產生，且存取憑證不應使用明碼(如：GET方式)進行傳遞。
64. 乙方交付之系統應遵守甲方系統與程式開發安全相關規定，於交貨驗收前，應確認下列項目，並提出安全檢測報告供甲方驗收:
65. 安全檢測報告中的安全檢測類型應包含:
	1. 所有程式原始碼弱點檢測。
	2. □若程式有提供 WEB 介面或 HTTP 服務，須包括網頁弱點檢測。
	3. 若含主機設備，須包括主機弱點檢測。
	4. □滲透測試(如本案涉及關鍵系統業務或為業主要求事項，建議勾選)。
	5. □委託金額達新臺幣一千萬元以上，或經甲方認定有必要者，應通過甲方或甲方所委託之第三方安全性檢測，檢測類型包含上述項目。
66. 報告內容至少包括：檢測環境說明(檢測工具、檢測工具版本、檢測相關設定)、受檢系統資訊、受檢檔案資訊、及檢測工具產出報告等。
67. 檢測工具所產出報告的內容至少包括：弱點項目、弱點描述、弱點項目判定結果，其中弱點項目判定結果應至少包括高、中、低風險等三種等級。
68. 檢測結果要求:
	1. 程式原始碼弱點檢測結果不得含有「高風險」以上之弱點。
	2. 主機弱點檢測、□網頁弱點檢測結果不得含有「中風險」以上之弱點。
	3. 滲透測試檢測結果不得含有「中風險」以上之弱點。
	4. 以上檢測結果之高、中風險弱點，乙方應負責完成修補，或經甲方同意後得採行其他補償性措施。
	5. 若程式有使用開源軟體(包含作業系統、應用程式、第三方組件等)，非經甲方書面同意，不得有「高風險」之保護性授權條款(如AGPL、GPL或其他[[9]](#footnote-9))。
69. 乙方交付之系統，若含具個資或金融交易功能之APP，須通過數位發展部數位產業署制定之MAS(Mobile Application Security)檢測規範，並提供佐證。
70. ■如本案有涉及或適用《資通安全管理法》之情形，應符合資通安全責任等級分級辦法之附表十、資通系統防護基準。(本案業主若為公務機關或特定非公務機關，應勾選本項)
71. 乙方須於系統交付時提供系統介面清單、必要安裝之元件及版本資訊、必要開啟之功能、必要開啟之網路服務port、預設帳號及通行碼、個資處理所有過程軌跡架構圖，及處理過程中產生之暫存檔案名稱(或規則)清單，包含檔案之目錄名稱。對於系統正常處理程序及例外狀況，應提供管控措施說明。
72. 乙方交付之系統，應提供內含之軟體清單(包括軟體名稱、版本、序號等)。若乙方使用第三方組件(含開源軟體)，應交付第三方組件清單(包括但不限於：組件名稱/開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、版本資訊)、執行檔及原始程式碼，且不得含有高等級以上弱點(CVSS v3評分 7.0 分以上之 CVE)，且應保證已取得該第三方權利人授權甲方使用，該第三方組件之授權範圍及授權時間應符合甲方本案需求，並不得使用保護性授權條款(如：AGPL、GPL或其他)；若遇授權爭議，乙方應依甲方指示辦理，並應自負完全責任。若因系統環境相容性原因，致無法修補時，乙方須出具說明文件與補償性措施，並取得甲方同意。
73. 乙方應保證其所交付之系統皆為自行開發，若涉及利用非乙方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，並提供授權證明。
74. 乙方交付之系統，合約期間暨後續保固期間應依下列條件辦理:
75. 本案系統上線後，若進行程式修改更版，應先於測試環境中測試驗證通過(含程式原始碼弱點檢測、開源軟體檢測)，並經甲方確認後，方得依甲方規定之系統變更作業程序進行程式更版。
76. 系統若有新發現之漏洞或弱點時，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版，通過甲方資安相關檢測。
77. 若因系統環境相容性原因，致無法修補時，乙方須出具說明文件與補償性措施，並取得甲方同意。
78. 乙方於甲方環境進行作業時，乙方人員均應遵守甲方資通安全規範。
79. 若乙方所供應之軟硬體設備或資料存取、儲存、備份及備援等作業，其實體所在地及資料傳輸涉及跨境議題，應以書面告知甲方，並說明至少包含傳輸資料及傳輸目的地之國家等相關資訊，且不得傳遞個人資料至法令法規禁止之國家(地區)。
80. 乙方及其人員應遵守《資通安全管理法》及相關子法、甲方門禁管理與現場(機房)作業管理規定，及數位發展部管轄之資通安全管理相關規定，不得派任或委託經主管機關通知具危害國家安全疑慮之人員進入甲方機房、料庫（場）及其他設施重地，進行相關設備安裝、維護、校準等作業，或進行涉及甲方網路系統資源、或相關資通系統軟體設計及開發或遠端系統連線之維運及測試作業。
81. 乙方開發過程中如違反資通安全相關法令、發現或懷疑系統遭受不當操作及使用(含日誌處理失效、系統嚴重錯誤)或其他資通安全事件，應立即通報甲方，並協助甲方執行適當之應變措施。
82. 乙方同意甲方得視需要就本案執行情形為適當之訪查、監督、確認及紀錄，並得向乙方索取相關資料，乙方不得規避、妨礙或拒絕，同時，乙方應針對風險事項於甲方指定時間內完成修補改善。
83. **□委外軟硬體建置/維運(於甲方環境)**
84. 乙方於甲方環境進行作業時，乙方人員均應遵守甲方之資通安全規範要求，乙方保證交付之履約標的，不得具備已被資訊安全組織公布，易遭駭客攻擊之任何弱點，包括但不限於OWASP(Open Web Application Security Project)最新發布之前十大安全問題種類、資訊安全教育研究組織公布之CWE/SANS TOP 25最危險之程式錯誤、WEB軟體安全協會(WASC)公布之最新攻擊與弱點及未來發布之安全問題種類；若發現履約標的含有弱點，乙方應負無償修補之責，並應於約定期限內，完成修補至符合甲方與其客戶之要求。
85. 乙方所建置/維運之軟硬體，於合約期間內之作業過程，應至少完成以下事項:
86. 建置驗收前，乙方須確認建置設備不得含有中等級以上弱點(CVSS v3評分 4.0 分以上之 CVE)，並提供佐證資料供甲方驗收。
87. 移除或關閉不需使用之功能服務、系統元件或偵錯介面。
88. 移除或關閉不需使用之網路服務及服務埠。
89. 刪除或停用不必要之帳號，並依據甲方要求最小化設定角色權限。
90. 應採用安全穩定之軟、韌體版本。
91. 啟動連線管控機制，如本機防火牆、應用軟體層控制設定。
92. 安裝甲方指定之防毒軟體，並更新至最新病毒碼。
93. 自動連網進行安全修補程式安裝、病毒更新或鐘訊同步等作業，應調整設定至甲方規定之區域進行，不得直接連接網際網路自行處理。
94. 限制經甲方核准之特定設備或來源(如：IP位址與Port)方得登入。
95. 開啟留存日誌項目，依甲方需求設定日誌紀錄項目、留存方式、留存時間及傳送日誌。
96. 上述6~10項，若因設備功能限制無法支援，須出具說明文件，並取得甲方同意。
97. 乙方所建置/維運之軟硬體，於合約期間內應依下列規定辦理:
98. 若進行程式修改更版，應先於測試環境中測試驗證通過(□含程式原始碼弱點及網頁檢測)，並經甲方確認後，方得依甲方規定之系統變更作業程序進行程式更版。
99. 前述更版若有使用第三方組件(含開源軟體)，應交付第三方組件清單(包括但不限於：組件名稱/開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、版本資訊)，且不得含有高等級以上弱點(CVSS v3評分 7.0 分以上之 CVE)，且應保證已取得該第三方權利人授權甲方使用，該第三方組件之授權範圍及授權時間應符合甲方本案需求。若因系統環境相容性原因，致無法修補時，乙方須出具說明文件與補償性措施，並取得甲方同意。
100. 若有新發現之漏洞、原製造商公布重大更新或韌體有新版本，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版。
101. 若因系統環境相容性原因，原製造商不建議修補時，乙方須出具原製造商之說明文件與補償性措施，並取得甲方同意。
102. □涉及公眾電信網路，須提供「符合ITU、3GPP 或NIST發布之資通安全規定」證明。
103. □屬於「台灣資通產業標準協會」已公布之物聯網產品驗證項目[[10]](#footnote-10)，須提供通過物聯網資安檢測或取得物聯網資安標章之證明。
104. 乙方及其人員應遵守甲方之委外廠商[遠端]連線維護作業遵循事項、實體安全及門禁管理辦法、機房管理辦法等相關規定，執行相關設備安裝、維護、調校等或其他作業，非經甲方許可，不得接觸甲方內部等級(含)以上之資料。
105. 乙方工作人員均應簽署個人「保密切結書」，並遞交甲方指定單位審核；□乙方應將乙方工作人員之詳細名冊送甲方指定單位備查，俾供現場核對前往施工之乙方人員身分，落實甲方資通安全管理。
106. 乙方工作人員應於現場（機房）主管指定安排之工作區（所指定之機房或辦公場內的位置）內作業，其進出及作業管理由各機房主管單位依安全檢查及機房門禁管理並留下紀錄。
107. 乙方工作人員非經甲方同意，不得自行攜入資通訊處理設備至甲方工作區域及機房，且不得私自接取甲方之網路。
108. 派駐甲方服務之人員，若因業務或管理之長期借(租)用甲方終端設備，且使用甲方內部網路者，所使用之終端設備須依甲方資訊安全相關規定安裝安控軟體。若為乙方自備專屬電腦，亦應遵循甲方所有資安相關管控規定，例外情形應取得甲方同意，設備攜回前，應確實依甲方相關規定及程序，刪除儲存媒體中之資料，並應經甲方現場主管確認。
109. 乙方工作人員未經甲方權責主管核准不得進入甲方系統；需使用甲方資料時，須由甲方授權及監督，依申請內容、範圍及步驟執行，工作結束乙方應即清除產出之非必要資料；未經甲方核准，乙方不得攜出所存取資料。如儲存媒體損壞後由甲方以物理性破壞或其他使資料無法還原之方式處理。
110. 乙方工作人員因本案需要申請登入設備之權限時，應依甲方之帳號權限申請與管理要求辦理，申請業務所需之最小權限，至少每六個月確認一次使用情況，不得再轉交其他人員使用。如乙方工作人員離職、職務異動或其他事由等，不再使用該帳號，應事前告知甲方異動其權限。
111. 乙方進行作業時，設備間不得使用互跳(間接)方式登入(如RDP、SSH、Rlogin、Telnet等)，應使用甲方指定之維運管道或管制規定辦理。
112. 乙方不應企圖試探系統或服務可疑的安全弱點。
113. 乙方作業過程中如違反甲方及/或甲方業主之資訊安全政策或相關規範、發現或懷疑系統遭受不當操作及使用(含稽核機制失效、系統嚴重錯誤)或其他資通安全事件，應於發現後□15□30分鐘內通報甲方，並協助甲方執行適當之應變措施。
114. 乙方工作人員因本案所做之所有異動(如系統升版、改接、更新Patch、測試作業及參數異動)，應事先提出申請，經甲方審核同意後，始可依甲方規定之系統變更作業程序進行作業。乙方工作人員應確實依申請內容、範圍及步驟執行，不得任意變更作業內容，作業期間應啟動日誌(log)紀錄，不得關閉，例外情形應取得甲方同意。
115. 乙方對甲方所做之軟硬體安裝、故障修復或定期維護服務皆須詳實記錄於維護紀錄中，內容應包含維護期間(記載時間至分鐘)、異動原因及異動內容，維護紀錄(如完工報告單、故障維修紀錄、保養紀錄單等)經甲方簽認後提供乙份存於甲方。
116. 乙方因本案協助甲方進行緊急連線診斷時除須事先設有經甲方許可之連線管道外，每次使用皆應經甲方事前核准。未經甲方事前書面同意，不得向第三人透露甲方的連線程序及通行碼(含雙因子認證使用之載具)，或轉接於第三人。
117. 乙方執行本案應配置充足且經適當之資格訓練、擁有資安專業證照或具有類似業務經驗之資安專業人員。
118. 乙方同意甲方得視需要就本案執行情形為適當之訪查、監督、確認及紀錄，並得向乙方索取相關資料，乙方不得規避、妨礙或拒絕，同時，乙方應針對風險事項於甲方指定時間內完成修補改善。
119. 乙方若有服務項目異動之狀況，應於■一個月□三個月□ 日曆天前前通知甲方，並取得甲方同意。
120. **□委外軟硬體建置/維運(於乙方或甲方業主環境)**
121. 乙方及其人員應遵守甲方或/及甲方業主之資訊安全政策，非經甲方事前許可，不得執行相關設備安裝、維護、調校等或其他作業，亦不得接觸甲方內部等級(含)以上之資料，並於作業完成後，應提供維護/工作紀錄予甲方備查。
122. 乙方保證交付之履約標的，不得具備已被資訊安全組織公布，易遭駭客攻擊之任何弱點，包括但不限於OWASP(Open Web Application Security Project)最新發布之前十大安全問題種類、資訊安全教育研究組織公布之CWE/SANS TOP 25最危險之程式錯誤、WEB軟體安全協會(WASC)公布之最新攻擊與弱點及未來發布之安全問題種類；若發現履約標的含有弱點，乙方應負無償修補之責，並應於約定期限內，完成修補至符合甲方與其客戶之要求。
123. 乙方所建置/維運之軟硬體，於合約期間內之作業過程，應至少完成以下事項:
124. 建置驗收前，乙方須確認建置設備不得含有中等級以上弱點(CVSS v3評分 4.0 分以上之 CVE)，並提供佐證資料供甲方驗收。
125. 移除或關閉不需使用之功能服務、系統元件或偵錯介面。
126. 移除或關閉不需使用之網路服務及服務埠。
127. 刪除或停用不必要之帳號，並依據甲方要求最小化設定角色權限。
128. 應採用安全穩定之軟、韌體版本。
129. 啟動連線管控機制，如本機防火牆、應用軟體層控制設定。
130. 設備應安裝商用防毒軟體，並更新至最新病毒碼。
131. 自動連網進行安全修補程式安裝、病毒更新或鐘訊同步等作業，應調整設定至甲方規定之區域進行，不得直接連接網際網路自行處理。
132. 限制經甲方核准之特定設備或來源(如：IP位址與Port)方得登入。
133. 開啟留存日誌項目，依甲方需求設定日誌紀錄項目、留存方式、留存時間及傳送日誌。
134. 上述6~10項，若因設備功能限制無法支援，須出具說明文件，並取得甲方同意。
135. 乙方所建置/維運之軟硬體，合約期間內應依下列規定辦理:
136. 若進行程式修改更版，應先於測試環境中測試驗證通過(含程式原始碼弱點及網頁檢測)，並經甲方確認後，方得依甲方規定之系統變更作業程序進行程式更版。
137. 前述更版若有使用第三方組件(含開源軟體)，應交付第三方組件清單(■包括但不限於：組件名稱/開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、版本資訊)，且不得含有高等級以上弱點(CVSS v3評分 7.0 分以上之 CVE)，且應保證已取得該第三方權利人授權甲方使用，該第三方組件之授權範圍及授權時間應符合甲方本案需求。若因系統環境相容性原因，致無法修補時，乙方須出具說明文件與補償性措施，並取得甲方同意。
138. 若有新發現之漏洞、原製造商公布重大更新或韌體有新版本，乙方應無償主動提供修補或升級方法，並經甲方同意後，於約定期限內完成修補或升版。
139. 若因系統環境相容性原因，原製造商不建議修補時，乙方須出具原製造商之說明文件與補償性措施，並取得甲方同意。
140. □涉及公眾電信網路，須提供「符合ITU、3GPP 或NIST發布之資通安全規定」證明。
141. □屬於「台灣資通產業標準協會」已公布之物聯網產品驗證項目[[11]](#footnote-11)，須提供通過物聯網資安檢測或取得物聯網資安標章之證明。
142. 乙方工作人員未經甲方權責主管核准不得進入甲方系統；需使用甲方資料時，須由甲方授權，依申請內容、範圍及步驟執行，並留存申請及執行紀錄。
143. 乙方工作人員因本案需要申請登入設備之權限時，應依甲方之帳號權限申請與管理要求辦理，申請業務所需之最小權限，至少每六個月確認一次使用情況，不得再轉交其他人員使用。如乙方工作人員離職、職務異動或其他事由等，不再使用該帳號，應事前告知甲方異動其權限。
144. 乙方進行作業時，設備間不得使用互跳(間接)方式登入(如RDP、SSH、Rlogin、Telnet等)，應使用甲方指定之維運管道或管制規定辦理。
145. 乙方就甲方軟硬體項目，於乙方環境進行建置、安裝、測試或維護作業時，乙方之相關建置維運作業環境及人員均應遵守甲方及甲方業主資通安全規範要求，必要時接受甲方及甲方業主之定期/不定期稽核，乙方應針對不符合事項於甲方指定時間內完成修補改善。
146. 乙方不應企圖試探系統或服務可疑的安全弱點。
147. 乙方作業過程中如違反甲方及/或甲方業主之資訊安全政策或相關規範、發現或懷疑系統遭受不當操作及使用(含稽核機制失效、系統嚴重錯誤)或其他資通安全事件，應於發現後□15□30分鐘內通報甲方，並協助甲方執行適當之應變措施。
148. 乙方工作人員因本案所做之所有異動(如系統升版、改接、更新Patch、測試作業及參數異動)，應事先提出申請，經甲方審核同意後，始可依甲方規定之系統變更作業程序進行作業。乙方工作人員應確實依申請內容、範圍及步驟執行，不得任意變更作業內容，作業期間應啟動日誌(log)紀錄，不得關閉，若有例外情形應事前取得甲方同意。
149. 乙方對甲方所做之軟硬體安裝、故障修復或定期維護服務皆須詳實記錄於維護紀錄中，內容應包含維護期間(記載時間至分鐘)、異動原因及異動內容，維護紀錄(如完工報告單、故障維修紀錄、保養紀錄單等)經甲方確認後提供乙份存於甲方。
150. 乙方因本案協助甲方進行緊急連線診斷時除須事先設有經甲方許可之連線管道外，每次使用皆應經甲方事前核准。未經甲方事前書面同意，不得向第三人透露甲方的連線程序及通行碼(含雙因子認證使用之載具)，或轉接於第三人。
151. 乙方執行本案應配置充足且經適當之資格訓練、擁有資安專業證照或具有類似業務經驗之資安專業人員。
152. 乙方同意甲方得視需要就本案執行情形為適當之訪查、監督、確認及紀錄，並得向乙方索取相關資料，乙方不得規避、妨礙或拒絕，同時，乙方應針對風險事項於甲方指定時間內完成修補改善。
153. 乙方若有服務項目異動之狀況，應於■一個月□三個月□ 日曆天前通知甲方，並取得甲方同意。
154. **□雲端服務**
155. 乙方應禁止使用大陸地區(含香港及澳門地區)廠商之雲端服務運算提供者。□但若符合甲方(含甲方業主)之規定[[12]](#footnote-12)，或取得其同意者，則不在此限。
156. 乙方提供雲端服務所使用之資通訊產品(含軟硬體及服務)不得為大陸廠牌，執行甲方受託業務之團隊成員(含分包廠商)亦不得有陸籍人士參與，就境外雲端服務之執行團隊成員，至少應具備相關國際標準之人員安全管控機制，並通過驗證。□但若符合甲方(含甲方業主)之規定[[13]](#footnote-13)，或取得其同意者，則不在此限。
157. 乙方應評估機敏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。□但若符合甲方(含甲方業主)之規定[[14]](#footnote-14)，或取得其同意者，則不在此限。
158. 針對所傳輸或儲存之甲方敏感資料或其客戶資料，乙方應建置適當之保護設備或技術，採取適當之控制措施（如：資料加密、多因子認證…等），並於甲方資料保存期限內，留存使用軌跡紀錄。採用加密演算法者，應能妥善保護加密金鑰（如使用硬體安全模組或其他安全方式）。
159. 甲方得就受託業務範圍辦理安全檢測(例如：弱點掃描、滲透測試…等作業)及更新Patch，以提升服務的安全性，並請乙方應依下列規定辦理：
160. 不得逕自封鎖甲方檢測使用之IP。
161. 若乙方提供之服務存有弱點或漏洞，乙方應負無償修補之責，並於雙方約定期限內，完成修補至符合甲方與其客戶之要求。
162. 若因環境相容性原因，無法修補弱點時，乙方出具補償性措施說明文件，並取得甲方同意。
163. 乙方就甲方受託業務範圍中，若涉及個資之蒐集、處理或利用者，乙方應遵循《個人資料保護法》及相關法令法規辦理，採取相對應安全維護措施，或依本附加條款第二條規定（出具有效期間內第三方驗證之證明，如：ISO 27701、BS 10012、ISO 27018）方式辦理，克盡善良管理人之注意義務。
164. 涉及個資蒐集、處理或利用之資料，除法律另有規定外，未經甲方同意，乙方不得以任何方式揭露或交付第三人(包含但不限於重製、傳輸、洩漏、告知、出借、移轉、對外發表、刊登或移作其他任何之用途使用)，或為自己或第三人之利益而使用。
165. 乙方應依甲方制訂之資訊安全事件通報程序，或由乙方監控並建立資訊安全事件通報程序。遇事件發生時，乙方相關單位及人員應依循前述通報程序辦理。
166. 乙方同意甲方得視需要就本案執行情形為適當之訪查、監督、確認及紀錄，並得向乙方索取相關資料，乙方不得規避、妨礙或拒絕，同時，乙方應針對風險事項於甲方指定時間內完成修補改善。
167. 乙方應於服務合約終止或轉移時，將使用之作業系統映像檔、儲存空間、快取空間、備份媒體、甲方資料或敏感資料等全數刪除或銷毀，並提供刪除或銷毀之紀錄予甲方備查。
168. **□人力及人員委任服務**
169. 乙方及其人員應視甲方要求參與資安教育訓練，並確實了解甲方或/及甲方業主之資訊安全政策，並遵循相關規定執行，且應簽署甲方及甲方業主指定之保密文件。
170. 乙方及其人員不論是在甲方或甲方業主之環境提供服務時，乙方人員均應遵守甲方與甲方業主之要求(包括但不限於保密義務、個資保護、資訊安全、門禁管理等規定)辦理。
171. 乙方及其人員如在甲方環境提供服務，應：
172. 依甲方指定安排之工作區內作業，非經甲方事前同意，不得自行出入機房或其他管制區域。如因作業需要而須出入機房或管制區域，應依甲方指示與規定辦理，並留下門禁管理紀錄。
173. 不得自行攜入資通訊處理設備至甲方工作區域及機房，且不得私自接取甲方之網路；未經甲方權責主管核准不得進入甲方系統。
174. 若乙方人員有使用甲方之公務設備、系統，應盡善良保管人維護責任，維護資訊安全，並應使用合法授權軟體或社交軟體，同時符合智慧財產權相關法律規定，並依甲方規定使用。
175. 乙方人員如需要申請登入設備、系統之權限時，應依甲方之帳號權限申請與管理要求辦理，申請業務所需之最小權限，至少每六個月確認一次使用情況，不得再轉交其他人員使用。乙方人員應善盡保管帳號密碼之責，不得轉借或洩漏乙方個人帳號之密碼予任何人。如乙方人員離職、職務異動或其他事由等，不再使用該帳號，應事前告知甲方異動其權限。
176. 乙方及其人員提供服務過程中，如違反甲方或其業主之資安政策、發現或懷疑系統遭受不當操作及使用(含日誌處理失效、系統嚴重錯誤)或其他資通安全事件，應立即通報甲方，並協助甲方執行適當之應變措施。
177. 乙方人員如有違反甲方或甲方業主之資安政策、個資保護規範或其他相關規定，經甲方確認屬實後，除依本附加條款第四條處罰外，違反人員將計罰一次書面警告，若乙方人員年度累計二次(含以上)書面警告者，甲方得要求乙方更換人員。
178. 乙方同意甲方得視需要就本案執行情形為適當之訪查、監督、確認及紀錄，並得向乙方索取相關資料，乙方不得規避、妨礙或拒絕，同時，乙方應針對風險事項於甲方指定時間內完成修補改善。
179. 乙方人員不再提供服後，不得擅自留存甲方所持有之重要文件或專案文件(包含但不限於專案規劃書、專案規格書、需求訪談報告、系統分析說明書等機密資料)至個人之資訊設備或雲端儲存空間；非經甲方事前書面同意，乙方不得將上述文件複製、修改、編輯、轉授權、授權或洩露予第三人，或為乙方本人或他人之利益而使用，亦不得繼續留存於乙方本人之其他資訊設備或雲端儲存空間。
180. 違反罰則及賠償
181. 乙方或其人員如有下列情事者，依下列規定辦理：
182. 如違反甲方資訊安全政策或相關規定，應■按次計罰新台幣(下同) 5000元之懲罰性違約金□以甲、乙雙方簽署之契約內容辦理，甲方並得要求乙方改派適當人選提供服務，且自查獲翌日起6個月內該違規人員不得進入甲方機房或管制區域。
183. 如違反甲方業主之資通安全規定或其他規範/要求，除前款規定外，乙方並應按次計罰[[15]](#footnote-15) 5000元之懲罰性違約金，若因此而致甲方被處罰，乙方應承擔責任。
184. 如有前二款情事之一，致甲方受有損害或須支出費用者，除前二款規定外，乙方並應與其人員對甲方負連帶賠償責任，甲方並得解除或終止契約。
185. 前項以外情形，乙方如因違反本附加條款其他規定，乙方應按違反次數每次計罰5000元之懲罰性違約金；如因而導致資安事件(含個資外洩、遭受入侵等)發生時，乙方應另按資安事件發生次數，每次支付5000元懲罰性違約金予甲方，並應賠償甲方因此所受之一切損失(包含但不限於所受損害、所失利益、營業損失、商譽損害、律師費用、訴訟、調解或仲裁費用、刊登媒體費用)，甲方並得解除或終止契約。
186. 乙方就本案應賠償及支付甲方之費用，甲方有權於結付乙方之結算金額中先予以扣抵，倘有不足，乙方應另行足額賠償及支付甲方。
187. 其他
188. 乙方依約應提供之所有文件、繪圖、圖表、規範或其他合約及保固期間之任何資料，應依照規定甲方指定程序及時程提供給「甲方」。除書面資料外，乙方亦應按甲方要求提供前述文件之電子媒體資料，交付甲方前應完成掃毒確認未遭惡意程式感染，以安全管道傳遞(如Secure email、檔案加密)。
189. 本契約屆期、終止或解除時，乙方及其工作人員應返還及移交其因履行本契約所持有之任何形式資料載體，或按甲方指示刪除及銷毀該等資料，且應向甲方提出切結書聲明其已確實全數返還移交或刪除銷毀。甲方於本契約有效期間內亦得隨時請求乙方依前述規定辦理。
190. 乙方非經甲方事前書面同意，不得將本契約所訂履約事項複委託或分包其他廠商履行，且該複委託之受託者或分包商廠商資格或其應具備之資通安全維護措施，應先經甲方審核同意。
191. 本附加條款所稱乙方人員，包含但不限於乙方之受僱人、受任人、代理人、合作廠商、轉包/分包商及該廠商人員，乙方應確實轉知本附加條款規定並促其遵守，該人員如有違反本附加條款規定者，概以乙方之違反行為論。
192. □關鍵基礎設施人員管制特別約定：
193. 本採購履約標的涉關鍵基礎設施，依甲方業主之要求，乙方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，並經甲方審核同意，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，但應接受甲方或其指定者全程陪同或監督管理。
194. 乙方人員執行工作，應接受甲方或其指定者全程陪同或監督管理。
195. 乙方應擔保其人員無犯罪紀錄，且乙方應依個人資料保護法規定取得乙方人員同意後，將其基本資料造冊(包含姓名、身分證字號、連絡電話、警察刑事紀錄證明等)並送交甲方審核；乙方人員如有更換時，乙方應依本款規定辦理並重新列冊送交甲方。
196. 本附加條款未載明事項，依甲、乙雙方簽署之契約辦理。本附加條款如有疑義，以甲方解釋為準。
1. 甲方業主泛指甲方於本案所提供服務之客戶、機關、公司行號、法人、組織或個人實體。 [↑](#footnote-ref-1)
2. 佐證資料如產製聲明書或其他類似文件。 [↑](#footnote-ref-2)
3. 台灣資通產業標準協會已公布之物聯網產品驗證項目(如數位機上盒、智慧音箱)，請參考網址: https://www.taics.org.tw/ValidationMenu08.aspx?validateType\_id=2 [↑](#footnote-ref-3)
4. 資通訊設備，涉及資通訊處理作業之實體設備，包含下列:

網通設備:電信設備、網路設備、資安設備、事務機、攝影機。

專用伺服器主機:採客製化OS且無法自行安裝軟體，或屬於Appliance並無法觸及OS設定之設備。

終端設備(具備OS) : 含作業系統(如:RTOS、Embedded Linux、Android、WinCE等)之終端設備，如:電腦設備、平板、電信終端(ATU-R)、IoT終端等。

若屬伺服器主機(如X86伺服器、刀鋒伺服器等)，請勾選二、採購設備器材下之「伺服器主機」類別。 [↑](#footnote-ref-4)
5. CVSS : Common Vulnerability Scoring System [↑](#footnote-ref-5)
6. CVE : Common Vulnerabilities and Exposures [↑](#footnote-ref-6)
7. 台灣資通產業標準協會已公布之物聯網產品驗證項目(如數位機上盒、智慧音箱)，請參考網址 : https://www.taics.org.tw/ValidationMenu08.aspx?validateType\_id=2 [↑](#footnote-ref-7)
8. 伺服器主機 : 具備管理資源與計算能力，可對網路上的用戶端電腦提供特定服務之設備，如X86伺服器、刀鋒伺服器等。若為專用伺服器主機，請勾選二、採購設備器材下之「資通訊設備」類別。 [↑](#footnote-ref-8)
9. 有關保護性授權條款係為使用這類開源軟體必須將所有衍生創作以相同方式開源，例如GPL-2.0、GPL-3.0、 AGPL、 CC BY-SA、 CeCILL v2.0或其他等。 [↑](#footnote-ref-9)
10. 台灣資通產業標準協會已公布之物聯網產品驗證項目(如數位機上盒、智慧音箱)，請參考網址 : https://www.taics.org.tw/ValidationMenu08.aspx?validateType\_id=2 [↑](#footnote-ref-10)
11. 台灣資通產業標準協會已公布之物聯網產品驗證項目(如數位機上盒、智慧音箱)，請參考網址 : https://www.taics.org.tw/ValidationMenu08.aspx?validateType\_id=2 [↑](#footnote-ref-11)
12. 甲方業主之契約有明確同意允許使用大陸地區(含香港及澳門地區)廠商之雲端服務。 [↑](#footnote-ref-12)
13. 甲方業主之契約有明確同意允許使用大陸廠牌之雲端服務所使用之資通訊產品。 [↑](#footnote-ref-13)
14. 甲方業主之契約有明確同意允許機敏資料於雲端服務之存取、備份及備援之實體所在地得位於大陸地區(含香港及澳門地區)。 [↑](#footnote-ref-14)
15. 違約金金額，由甲方請購單位依履約風險制定。 [↑](#footnote-ref-15)