Alludo 廠商安全性要求

目錄

簡介

本文件概述 Alludo Group (統稱「Alludo」) 旗下公司的資訊安全性、業務持續性及隱私權相關作法，以及評估 Alludo 廠商之安全性與持續性措施的計畫。本文件提及之流程、程序、要求及義務統稱為「Alludo 標準」。

本「**廠商安全性要求文件**」係向提供商品與服務的廠商 (統稱「廠商」) 說明，Alludo 要求其在提供服務時對於安全性、業務持續性及隱私權負責之期望。廠商必須遵循業界最佳實務與其企業安全性原則，以實現以下要求；針對廠商面臨的任何問題 (包括資料遺失或設備損壞)，無論肇因為何，Alludo 概不負責。

如本文件與書面協議之間出現任何不一致之處，將以書面協議之條款為優先。廠商亦必須遵循任何當地、國家或地區之法規要求。如本文件與適用法規之間發生衝突，廠商應通知 Alludo 並提供替代控制措施建議，以維持同等之安全性、持續性或隱私權標準。

廠商安全性要求概觀

Alludo 必須負責保護其限制與機密資訊，以避免未經授權之存取或揭露。對此，Alludo 實作 Alludo 標準：內部資訊安全性、業務持續性及隱私權標準，以確保該限制與機密資訊受到保護，並確保 Alludo 提供之服務持續可用。為確保 Alludo 符合與資訊安全和業務持續性相關的內部標準和法規要求，Alludo 要求其廠商遵守本文件概述之 Alludo 標準。

因此，若廠商委託或轉包其在與 Alludo 協議下的任何部分之義務，或任用其他廠商直接或間接向 Alludo 提供服務，則廠商應要求其委任的廠商實作並管理符合 Alludo 標準的資訊保護計畫與方案。Alludo 致力於以合理方式與其廠商合作，以協助廠商達到與 Alludo 標準相關之法規遵循要求。該 Alludo 標準對於特定廠商之適用範圍，依該廠商向 Alludo 提供之服務與產品類型而有所不同。

身分識別與存取控制

廠商應確保達成以下要求：

1. 存取控制與使用者管理：

1.1. 落實書面規定的存取控制原則，並至少每年審查一次。
1.2. 定義並書面規定使用者角色、權限及存取權。
1.3. 落實使用者入職和離職的標準程序，包括保留相關核准的記錄。
1.4. IT 基礎架構元件之存取權是根據最低權限原則授予，並透過身分識別管理工具 (例如，Active Directory、OKTA 或類似工具) 加以管理。
1.5. 個人對系統、網路資源及其他 IT 資源的存取需經過正式核准，並透過專屬的使用者 ID 及個人密碼加以控制。
1.6. 維持職責分工，同時建立/修改使用者 ID 與分配權限。

2. 密碼與驗證原則：

2.1. 使用者必須在初次登入時變更其密碼。
2.2. 密碼必須符合業界標準要求，包括長度、有效期限、複雜度、密碼歷史記錄、失敗嘗試次數、帳戶鎖定持續時間、密碼使用期限及首次登入變更。
2.3. 在啟動密碼重設前，應使用安全機制來傳送使用者密碼和驗證使用者身分。
2.4. 不支援 IdP 驗證或需要獨立建置的系統，其配置必須強制執行強式驗證，強度不得低於中央密碼與存取控制原則中定義之組態。
2.5. 所有系統和應用程式應設定為透過核准的身分和存取管理機制使用安全登入程序。

2.6. 系統與應用程式必須設定為閒置工作階段逾時，以防止未經授權之存取。

3. 特殊權限存取管理：

3.1. 資源的特殊權限存取僅限於已定義的使用者角色，並由授權人員核准。
3.2. 特殊權限使用者帳戶應設定為使用多重因素驗證。
3.3. 不再需要的特殊權限應立即撤銷。
3.4. 管理認證的使用僅限於疑難排解等有限情況，而使用者則使用最低權限認證執行日常操作。
3.5. 使用多重因素驗證保護關鍵 IT 基礎架構、系統、網路裝置及應用程式 (例如，遠端存取、關鍵伺服器、網路裝置) 之存取。

4. 存取權審查與監控：

4.1. 定期審查存取權限，並立即處理發現的例外狀況。
4.2. 對所有使用者 ID (包括網域、應用程式、網路裝置、IT 系統、中介軟體、資料庫等) 進行核對的時間不超過每年一次，並對發現的任何差異立即採取修正措施。

5. 第三方與廠商管理：

5.1. 第三方廠商對網路與系統的存取權限，須根據「必要範圍」和「正式核准」原則嚴格控管。
5.2. 變更廠商提供之預設認證後，才可將系統、應用程式、網路裝置或其他 IT 基礎架構裝置投入生產。

6. 特殊存取考量：

6.1. 除非有正式的理由並經資深管理團隊核准，否則不得使用通用與共用 ID，並透過相關機制追蹤使用情況和追溯個人行動。
6.2. 所有非主控台的管理存取均使用業界認可的加密演算法加密，非主控台的管理存取禁止使用不安全之通訊協定 (例如，telnet/ftp)。

資產管理

廠商應確保達成以下要求：

7. 資產管理與清查：

7.1. 維護全面資產詳細目錄，並擷取資產擁有者資訊、聯絡資料及位置等基本詳細資料。
7.2. 定期更新與審查資訊技術資產 (包括硬體、作業系統、應用程式及資料庫) 之記錄，以確保準確性。
7.3. 建立與維護資產管理程序與組態控制項，以管理關鍵資產之可用性，以及重要網路與資訊系統之組態。

8. 資訊分類與標記：

8.1. 維護資訊分類原則，其中包含支援程序與指南。所有資產均根據既定指示貼上標籤，資訊則根據已定義的分類等級進行分類和保護。

9. 資產處理：

9.1. 維護資產管理正確處理指南，並告知所有適用員工與承包商。

9.2. 落實書面規定的程序，以保護資訊資產、識別應處置之資產，並確保安全處置此類資產。

9.3. 建立相關程序，以確保所分配的資產在雇用、合約或協議終止或解除後，迅速歸還相關資產管理團隊。

10. 行動裝置與卸除式媒體管理：

10.1. 針對儲存、傳輸或處理業務資訊之行動裝置 (包括 BYOD)，實施相關控制原則與程序。需採取充分的保護措施後，才可允許行動裝置存取業務資訊與資源。

10.2. 使用卸除式大量儲存裝置時必須加密，以確保資料安全。

11. 軟體法規遵循：

11.1. 禁止使用未經授權或未經核准之軟體。落實相關程序，以識別任何違規事項，並採取必要動作進行處理。

IT 作業

廠商應確保達成以下要求：

12. 關鍵系統作業：

12.1. 建立並維護以下關鍵網路和資訊系統的操作程序：

12.1.1. IT 資產存取權限的正式核准程序。

12.1.2. 所有技術 (例如，VPN、Windows 登入) 的強大驗證機制。

12.1.3. 定期審核特殊權限。

12.1.4. 根據業務持續性要求，識別關鍵技術的網路位置。

13. 變更管理：

13.1. 針對 IT 系統、應用程式、資料庫及網路元件實作全面的變更管理程序，以確保：

13.1.1. 所有變更的記錄、審查、測試及正式核准。

13.1.2. 針對可能造成破壞的修改，制定復原方案。

14. 其他：

14.1. 處理敏感與機密資訊之系統與網路元件必須接受檔案完整性監控檢查。

14.2. 將所有系統與網路元件設定為使用經授權之網路時間協定 (NTP) 來源，以利準確同步處理時間。

14.3. 針對所有關鍵系統、應用程式、網路裝置及使用者電腦，建立定期主動式與預防性維護程序。
14.4. 定期或按照業界標準審查防火牆與路由器規則集，並立即移除非必要或未經授權之規則。
14.5. 實作相關控制措施，以維護整體 IT 環境之資訊與軟體的完整性。

人力資源安全性

廠商應確保達成以下要求：

15. 背景調查：
15.1. 建立與維護執行背景調查的原則與程序。
15.2. 根據員工與承包商的職務與職責，在法律允許範圍下，於入職前對其進行適當的背景調查。
16. 人員變更管理：
16.1. 實作相關程序以管理人員或其角色與職責變更，包括針對新進人員進行相關原則與程序教育。
16.2. 在人員變更後，立即撤銷不再需要或不允許的存取權、識別證、設備及其他資源。
17. 原則強制執行：
17.1. 針對違反安全性原則之員工，實作並貫徹明確的紀律處分程序。
17.2. 透過適當的合約措施，確保違反安全性原則的責任。其中包括在員工雇傭合約與第三方承包商服務協議中納入相關條款。

安全性與隱私權訓練

廠商應確保達成以下要求：

18.所有員工與承包商都必須接受安全性與隱私權訓練。此訓練必須在初次雇用時完成，之後每年完成一次或更少。
19.具有重要 IT 安全性職責之員工與承包商，需每年接受針對其特定安全性角色與職務的專業訓練。
20.管理階層可以使用工具和系統，以監控並追蹤員工和承包商的訓練進度。
21.組織的訓練與認知計畫須定期審查與更新。此程序應考量不斷演變之業務需求、立法層面之變化，以及從過去之安全性事件學到的經驗教訓。

資訊安全性與治理

廠商應確保達成以下要求：

22. 安全性架構與治理：

22.1. 廠商必須針對資訊與網路安全治理實作經認可之安全性標準架構 (例如，NIST CSF、RMF、800-53、ISO 27001、CIS)。此架構應包括：
  22.1.1. 全面的資訊與網路安全原則和程序，需經年度審查、正式核准和全組織溝通。
  22.1.2. 與業務目標一致的妥善定義資訊安全性策略。
  22.1.3. 專門處理資訊與網路安全風險之健全治理與風險管理程序。
  22.1.4. 符合與資訊和網路安全相關之法律與法規要求的法規遵循機制。
22.2. 如未遵循經認可之安全性架構，則廠商必須提交報告表示其環境已經過稽核。
  22.2.1. 廠商與 Alludo 應共同議定針對已發現問題的補救方案，包括預期的時程。

23. 領導團隊與組織結構：

23.1. 定義資訊與網路安全的適當角色與職責並在整個組織內實施。

24. 風險管理與評估：

24.1. 針對以下事項，建立經資深管理團隊核准的正式風險管理架構：
  24.1.1. 識別內部與外部威脅。
  24.1.2. 評估範圍內之資訊/資料的敏感度。
  24.1.3. 評估潛在的業務影響。
  24.1.4. 評估威脅、漏洞及相關風險。
    24.1.4.1. 優先處理所有發現的風險和威脅，並及時採取動作以相應減輕風險。
    24.1.4.2. 實作相關程序和/或工具，以識別造成組織關鍵業務目標中斷之事件。
    24.1.4.3. 如廠商無法補救或降低可能影響提供之服務的任何重大風險，則必須立即通知 Alludo。

25. 法規遵循與績效監控：

25.1. 落實相關程序，以識別、記錄及追蹤組織的所有適用法律、法規及合約要求。
25.2. 進行定期評估，以驗證是否符合法律、法規及合約義務。維護此類評估之記錄，並及時彌補發現的落差。
25.3. 至少每年審查相關原則、程序及指南一次，並根據法律、法規及合約要求進行更新。
25.4. 定義、正式書面制定、定期評估及向資深管理團隊報告 IT、資訊安全性及資料隱私權等重要部門的關鍵績效指標。

網路安全性

廠商應確保達成以下要求：

26. 網路設計與安全性架構：

26.1. 廠商網路採用「深度防禦」原則，並結合網路分段等適當控制措施，以有效減少資訊與網路安全漏洞。
26.2. 實作強大之架構設計，採用有效之身分識別管理與健全之作業系統組態。

26.3. 每年審查一次網路設計與實作，以確保持續有效性與安全性。
26.4. 網路組態遵循所有適用法律和法規要求。

27. 存取控制與驗證：

27.1. 外部網路連線必須書面記錄、經由防火牆路由、驗證，並於建立前接受核准。
27.2. 無線網路存取必須驗證、授權、分段及加密。採用相關系統，以偵測與回應惡意無線存取點或未經授權之連線。
27.3. 廠商網路的遠端存取，必須獲得核准，以安全方式執行，並採用多因素驗證。
27.4. 實施相關控制措施，以防止或有效減少未經授權之廠商網路存取。

28. 安全操作與管理：

28.1. 管理工作站和網路裝置之間所有管理相關網路流量，均使用業界標準加密與驗證通訊協定。
28.2. 非主控台管理員的存取只能透過業界認可的加密通道進行。
28.3. 在網路裝置部署至生產環境前，停用或移除訪客帳戶，以及變更所有預設密碼與廠商提供之密碼。

29. 網路強化與威脅預防：

29.1. 停用未使用之服務、應用程式及連接埠，以減少攻擊面。
29.2. 針對關鍵網路區段部署入侵偵測和/或預防措施。
29.3. 保護關鍵系統，避免遭受阻斷服務 (DoS) 與分散式阻斷服務 (DDoS) 攻擊。

加密

廠商應確保達成以下要求：

30. 實施全面加密原則與支援程序，以確保遵循所有相關法律、法規及業務要求。此原則應遵循業界最佳實務，根據適用法律與標準確保加密安全性。

31. 加密標準與實作：

31.1. 僅允許採用安全、業界認可的加密演算法與金鑰強度，以確保所有系統和程序都有充足的資料保護。
31.2. 實施加密解決方案以保護機密資訊，並限制敏感資料的存取，包括對傳輸中資料和靜態資料進行加密。
31.3. 加密所有密碼儲存和傳輸，以隨時維護使用者認證的機密性。
31.4. 傳輸中的 Alludo 資料必須加密 (採用最低 TLS 1.2 或更新的標準)。
31.5. 靜態的 Alludo 資料必須加密 (採用最低 AES 256 位元或更新的標準)。

資料安全性

廠商應確保達成以下要求：

32. 復原：

32.1. **資料備份與復原**：

32.1.1. Alludo 資料必須定期執行備份。

32.1.2. Alludo 資料備份必須保留 1 年。

32.1.3. Alludo 資料備份必須加密。

32.2. **災難復原**：

32.2.1. 災難復原方案必須每年測試。

33. 備份原則與程序：

33.1. 備份原則與支援程序必須清楚書面記錄。

33.2. 備份還原流程必須書面記錄，並以定義的頻率進行測試。

33.3. 備份還原測試的證據必須保留。

33.4. 關鍵資料備份檔案的副本必須妥善保存。

34. 備份監控：

34.1. 備份管理員必須監控備份失敗的記錄檔 (如有)。

34.2. 備份失敗時，必須執行修正措施並以書面記錄。

35. 資料位置：

35.1. 廠商負責確保遵循資料所儲存之國家/地區的適用資料保護與隱私權法律。

35.2. 遵循資料跨國傳輸的限制 (GDPR 等)。

35.3. 廠商必須實作適當之技術和組織安全性措施，以根據資料所儲存之國家/地區的法律與標準保護資料。

35.4. Alludo 得保留稽核廠商資料處理實務的權利，以確保其遵循議定的安全性措施與當地法規。

36. 資料刪除：

36.1. 落實合約終止時安全刪除資料之程序，以確保遵循當地資料保留法律。

37. 全磁碟加密：

37.1. 工作站與伺服器必須設定全磁碟加密。

38. 資料分類：

38.1. 必須落實書面的資料分類原則。

38.2. 資料必須根據其關鍵性與敏感度進行分類。

38.3. 必須識別並實作與資料敏感度相對應的安全性控制措施。

資訊通訊

廠商應確保達成以下要求：

39. Web 安全性：

39.1. 實作 Web 內容篩選軟體，以封鎖對託管惡意內容之網站的存取。

39.2. 所有 Web 系統與應用程式都必須透過安全且經過驗證之機制存取。

39.3. 應用程式與 Web 入口網站必須透過加密通道進行用戶端與伺服器的通訊。

40. 電子郵件安全性：

40.1. 落實安全性控制措施，以防止電子郵件系統遭到濫用。

40.2. 所有電子郵件通訊聲必須透過加密通道傳輸。

40.3. 電子郵件閘道應具備：

40.3.1. 防網路釣魚篩選器。

40.3.2. 啟用電子郵件之安全性通訊協定 (即 DMARC、DKIM 及 SPF)。

40.3.3. 其他必要組態，以防止電子郵件產生之威脅。

軟體開發

廠商應確保達成以下要求：

41. 軟體開發生命週期：

41.1. 必須採用既有之軟體與系統開發架構。

41.2. 必須按照安全軟體開發最佳實務 (例如，OWASP) 開發系統與應用程式。

41.3. 軟體程式碼必須：

41.3.1. 防止未經授權的修改

41.3.2. 安全儲存

41.3.3. 遵守品質保證程序

41.4. 執行強制性的程式碼審查。

42. 測試與開發：

42.1. 應用程式必須接受完整之安全性與功能測試後，才可部署至生產環境。

42.2. 生產與非生產環境必須適當分隔。

42.3. 生產與非生產開發必須維持職責分工。

42.4. 測試環境中不應存在生產資料。

應用程式安全性

廠商應確保達成以下要求：

43. 應用程式安全性：

43.1. 所有全新開發的應用程式及經歷重大變更的現有應用程式，均應執行應用程式安全性評估，以識別已知的安全性漏洞。

43.2. 找出的所有 CVSS 分數高於 4 的安全性漏洞，都必須在應用程式部署至生產環境前完成修復。

43.3. 實作程式碼審查程序，以識別和補救可能造成安全性漏洞之程式碼。

44. Web 應用程式保護：

44.1. 透過健全之 Web 應用程式防火牆保護公開的 Web 應用程式，以防止外部威脅。

修補程式管理

廠商應確保達成以下要求：

45. 依據修補程式所處理的漏洞的關鍵性，將最新的安全性修補程式及時套用至系統、網路、應用程式及資料庫等。專屬系統的修補程式可直接從各 OEM 取得。

46. 所有修補程式都會在部署到生產系統之前進行測試，並在進行任何修補活動後，驗證經修補之服務是否可正確運作。

47. 如果系統無法修補，則會採取適當的緩解措施，定期評估這些緩解措施的有效性，並保留相關證據。

惡意軟體防護

廠商應確保達成以下要求：

48. 所有 IT 系統都持續受到惡意軟體防護解決方案的保護，即時檢查傳入的資料，以防止服務中斷或安全漏洞。此外，還會執行適當的使用者認知程序。防惡意軟體系統可偵測不同威脅，包括但不限於病毒、間諜軟體、蠕蟲、未經授權之行動程式碼、鍵盤側錄程式、殭屍網路及木馬程式。

49. 惡意軟體特徵碼會定期更新，以確保系統隨時具備最新的威脅定義。

50. 惡意軟體防護軟體經過設定，可執行排程掃描和按需掃描，並隔離或刪除任何經確認之惡意檔案或軟體。

51. 使用者無權或無法停用惡意軟體防護。

漏洞管理

廠商應確保達成以下要求：

52. 漏洞管理程序：

52.1. 制定用於全面漏洞管理的原則、流程及程序。

52.2. 透過程序接收、分析並回應來自內部與外部來源的漏洞資訊。

53. 漏洞評估與補救：

53.1. 針對廠商之 IT 基礎架構與應用程式 (包括災難復原站點) 進行季度漏洞評估。
53.2. 在定義時程內針對找出的 CVSS 分數高於 4 的漏洞進行補救。

54. 滲透測試：
54.1. 針對用於 Alludo 服務之廠商 IT 基礎架構與應用程式，進行年度獨立滲透測試。
54.2. 試的目的是找出易遭利用的漏洞，並防止因網路攻擊而造成的安全漏洞。
54.3. Alludo 會依合理要求授予相關滲透/漏洞測試報告之存取權。

記錄與監控

廠商應確保達成以下要求：

55. 關鍵系統 (包括應用程式) 應設定為記錄關鍵事件 (包括特殊權限存取與使用者活動之事件)，並保留此類記錄至少 1 年或依照適用法規要求保留。
56. 關鍵事件之記錄 (如適用) 至少包含下列內容：
56.1. 系統啟動與關閉。
56.2. 關鍵服務與程序之啟動與停止狀態。
56.3. 組態參數之變更 (例如，系統開機組態之變更)。
56.4. 成功登入與登入失敗嘗試次數。
56.5. 使用者帳戶之建立、修改及刪除。
56.6. 已存取之系統/資源。
56.7. 資源存取者與存取位置的識別與定位。
56.8. 日期與時間戳記。
57. 稽核記錄會從多個來源與感應器收集和建立關聯性，並安全地儲存與防止篡改，以便重建此類事件。
58. 建立監控記錄事件 (建議為即時) 之程序，以偵測任何未經授權之活動與攻擊目標，並確保關鍵事件記錄經過審查。

事件管理

廠商應確保達成以下要求：

59. 明確定義角色與程序，以確保針對資訊安全性與隱私權事件採取迅速、有效且井然有序的回應。
60. 訓練員工與承包商認識何謂安全事件，以及如何通報任何潛在或已證實的事件。
61. 負責分析與回應事件的人員均具備相關資格，並定期接受有效事件回應實務的訓練。
62. 所有通報事件均建立存放庫，詳細記錄為減輕事件影響而採取的行動，以及從事件中汲取的教訓。
63. 組織知悉任何影響其安全的事件時，應立即通知 Alludo，最遲不得超過偵測到事件後的 24 小時。

實體和環境安全性

廠商應確保達成以下要求：

64. 實作符合業界標準的實體安全與環境控制原則與程序。
65. 保護容納 IT 系統、應用程式及人員之關鍵設施 (例如，資料中心、營運站點)，以防止意外、攻擊和未經授權的存取。
66. 採用電子門禁、身分識別驗證、保全人員、訪客管理及全天候閉路電視監控等安全性措施，以防止未經授權進入。
67. 保留閉路電視影像至少 30 天，或依法律規定保留更久。
68. 設施的進出權限僅限於經授權且基於特定目的之人員，並須定期審查。
69. 訪客須全程陪同，進出時間需記錄，並隨時配戴訪客識別證。離開前須回收門禁卡或鑰匙。
70. 使用不斷電系統 (UPS) 或發電機，確保關鍵設施持續運作，防止斷電影響。
71. 定期維護 UPS、發電機、煙霧偵測器、滅火系統及門禁系統，並保存記錄。
72. 設施應採用防火材質建造，且配備火災警報器、煙霧偵測器、溫度與淹水感測器及滅火器，以防範自然災害。
73. 制定紙本與電子格式資料的安全處置機制，如紙張使用橫切碎紙機，電子媒體則採用清理、消磁或銷毀等方法。
74. 實施桌面淨空政策，確保安全處理便利貼、書面文件及卸除式媒體。
75. 至少每年評估實體與環境控制措施一次，以確保成效。

隱私權與資料保護

如果廠商或其轉包處理商代表 Alludo 或 Alludo 的客戶處理個人資料，廠商應確保達成下列要求：

76. 資料隱私權法規遵循與治理：

76.1. 遵循所有適用資料保護法。
76.2. 建立隱私權管理架構，其中包括：
76.3. 隱私權政策、聲明、通知及程序 (每年審查一次)。
76.4. 隱私權治理與風險管理程序。
76.5. 遵循法律與法規要求。
76.6. 維護最新之 Alludo 個人資料處理活動的記錄。
76.7. 定義與實作適當之資料隱私權角色與職責：
76.8. 指定資深資料隱私權專員 (或同等職位)。
76.9. 建立專業資料隱私權部門。
76.10. 成立相關委員會協調資料隱私權法規遵循活動。

77. 資料保護與安全性措施

77.1. 實作業界標準安全措施 (例如，ISO/IEC 27001:2013 與 SOC2 等)，以保護 Alludo 資訊。

77.2. 針對敏感個人資料採取額外安全措施 (例如，加密、匿名化)。

77.3. 強制執行存取控制措施：

77.4. 根據「必要範圍」和「最低權限」原則限制存取。

77.5. 在終止或角色變更時立即移除存取權限。

77.6. 定期審查存取權限。

77.7. 確保所有處理個人資料的人員都能遵守保密承諾。

78. 資料主體權利管理：

78.1. 協助 Alludo 履行其在資料主體權利方面的義務。

78.2. 於收到資料主體要求後的 2 天內通知 Alludo。

78.3. 除非法律另有規定，否則僅依 Alludo 指示回應要求。

79. 事件應變：

79.1. 於涉及 Alludo 資料之個人資料外洩的 24 小時內通知 Alludo。

轉包措施

廠商應確保達成以下要求：

80.針對所有涉及管理、處理或儲存 Alludo 資料之轉包處理商，進行年度第三方風險評估。這些評估應涵蓋轉包處理商的安全控制措施、資料保護措施、相關法規的遵循情況，以及整體風險狀態。廠商必須按要求提供這些評估的文件、迅速解決識別出的風險，並及時通報任何轉包處理商的變更或重大發現。本公司保留審查評估結果及在必要時要求採取額外安全措施的權利。

業務持續性管理

廠商應確保達成以下要求：

81.建立業務持續性管理 (BCM) 原則，並搭配詳細方案與程序。這些文件應概述組織的業務持續性目標，並接受年度審查與核准。

82.研擬與實作 BCM 測試架構，以評估現有業務持續性策略之成效。

83.業務影響分析 (BIA) 至少每年進行一次，或在重大組織變更之後進行。

84.建立危機管理方案，包括防範疫情之具體規定。此方案應確保在緊急情況下做出適當回應，並著重於保護員工、訪客、環境、資產，以及維持關鍵業務運作。

85.每年測試業務持續性管理系統 (BCMS) 的有效性，並完整保存每次測試的詳細記錄。

<文件結尾>