【附件4】**廠商產品或服務資通安全自我檢核表（非資通產品或服務者免填）**

參與創新照護產品及服務名錄所提供之商品或服務應符合相當資通安全水準，請廠商確實填寫以下檢核項目：

|  |  |
| --- | --- |
| **檢核項目** | **自我檢核結果** |
| **設置內部營運之資通安全管理制度及對客戶資料之保護機制**  說明：   1. 廠商考量其所面對之內外部議題，建立符合自身目標之資通安全政策，並以文件化管理，內容包含資通安全目標，並能識別資通安全風險予以對應。 2. 廠商營運時所接觸之客戶資料，應有對維持該等資料完整性、機密性及正確性之方法，例如採行密碼控制措施、進行設備維護、避免未經授權之資產攜出，或其他存放裝置或資料之保護措施。 | □符合  □不符合或不適用；  原因：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| **設置資通安全權責人員與教育訓練**  說明：   1. 廠商應由高階管理者擔任資通安全總負責人，該管理者應有權責協調分配資通安全政策之制定、修正與執行。 2. 廠商應就組織內部之所有資通安全責任明訂與分配，並應注意將相互衝突之職務或責任領域加以區隔，降低組織資產遭未經授權或非故意之修改或誤用。 3. 廠商應透過教育訓練提升所屬人員之資通安全認知，並規劃、落實及記錄教育訓練之內容與頻率等。 | □符合  □不符合或不適用；  原因：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| **設置資通安全作業與保護方法**  說明：   1. 廠商應盤點其資通系統，確立系統作業流程與責任劃分之管控方法，以確保資通處理設施能被正確、安全地操作。 2. 相關管控方法例如防範惡意程式方法、備份資料避免資料遺失、存取與監控以記錄事件或留存證據、確保作業系統完整性、防範技術脆弱性等。 | □符合  □不符合或不適用；  原因：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| **設置網路安全管理**  說明：   1. 廠商應採取必要措施，保護於網路公開之應用服務，並避免詐騙行為、契約爭議，及未經授權之存取與修改。 2. 相關網路安全管理措施包含網路控制措施；將得以識別網路服務之安全機制、服務水準及管理要求納入網路服務協議中（無論此等服務是內部或委外提供）；網路區隔措施等。 | □符合  □不符合或不適用；  原因：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| **設置系統存取控制管理**  說明：   1. 廠商應採取系統存取控制管理措施，以防止系統或資通遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害等，並確保其機密性、完整性及可用性。 2. 相關控制措施可包含：帳號註冊或註冊等權限管理、於系統中佈建使用者身分配置程序、限制與管理特權存取權限、使用者密碼資通管理，另須定期檢視使用者權限，並隨著雇用（內部員工）或合約關係（客戶或第三方）的轉變來移除或調整存取權限等。 | □符合  □不符合或不適用；  原因：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |
| **資通安全檢核（產品為資通系統/網站服務者適用）**  說明：   1. 為確保產品或服務之資通安全性，廠商依照採購合約所交付之軟硬體及電子文件，應先行檢查是否內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel），並於上線前清除相關測試資料。 2. 本年度是否發生資安事件，如有發生，廠商業已完成損害控制、復原作業及根因調查。 3. 廠商業已定期或不定期對擬上架產品或服務進行弱點掃描、滲透測試等相關資通安全必要檢測，確認該產品並無中度以上之資通安全風險。 | □符合  □不符合或不適用；  原因：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。 |

廠商確認與保證上述自我檢核表之填寫內容為真實、完整、正確及無誤導，如有與事實不符者，廠商願負一切法律責任。