附表 A：本制度規範安全管理措施

修正與公告日期：2021 年 12 月 30 日

附表 A 係針對本制度規範管理措施制定基本安全管理措施，組織應符合附表 A 所列各項管理措施，確保組織蒐集、處理及利用個人資料流程符合法令遵循，並已採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。

A8.7 資通安全	
A8.7.1 存取控制	管理目標：組織對個人資料的存取加以規範與保護，防止任何未經授權的存取與破壞。 管理措施： 1. 存取控制實施 組織應透過存取控制政策與存取實施機制（如存取控制清單）對個人資料之存取進行管控。 2. 帳號管理 組織應建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序，並應刪除或禁用已逾期之臨時或緊急帳號、閒置帳號。逾組織所訂定之時間時，系統應自動將使用者登出。 3. 職責分工 組織對於個人資料之存取應落實職責分工。 4. 最小權限 組織應落實最小權限的概念，僅允許使用者依組織任務與業務功能需要，完成指派任務授權的存取行為。 5. 遠端存取 組織應透過政策訂定選擇禁止或嚴格限制遠端存取個人資料，倘允許遠端存取，組織應確保傳輸過程經過適當加密，並應建立自動監控措施，以確保從遠端連線至資通系統之活動，均符合遠端存取政策。 6. 行動裝置存取 組織應透過政策訂定選擇禁止或嚴格限制，來自於可攜式或行動裝置對個人資料的存取。如果行動裝置經允許存取個人資料，組織應確保該裝置被適當保護，並定期檢視或確認該裝置以確認其安全狀態。 7. 資訊分享 組織應制定個人資料資訊分享機制，確保對個人資料存取之授權符合政策規定。

A8.7.2 技術檢視	管理目標：組織依據個人資料風險評鑑與業務所需，決定資訊系統需要被稽核與紀錄的事件，並建立監控機制。 管理措施： 1. 稽核事件 組織應監控影響個人資料機密性的事件，例如對個人資料的未授權存取。 2. 稽核紀錄的檢視、分析 組織應定期檢視與分析資通系統稽核紀錄，以發現個人資料的不當或不尋常活動的跡象、調查可疑的活動或可疑的違規、將發現報告給權責主管並採取適當措施。
A8.7.3 識別鑑別	管理目標：組織對於組織內部的系統使用者，應有特定的方式確認其所擁有的存取帳號與權限，以確保行為之明確可歸責性。 管理措施： 1. 使用者之識別與鑑別 組織內之使用者使用資通系統，組織應賦予其唯一的識別與驗證方式，避免使用共用帳號。 2. 身分驗證管理 使用預設密碼登入系統時，應於登入後要求立即變更。身分驗證相關資訊不以明文傳輸。
A8.7.4 媒體安全	管理目標：組織應確保儲存個人資料之媒體，其存取、保存、傳輸與汰除時之安全。 管理措施： 1. 媒體存取 組織應採用特定防護措施，對特定授權人員，限制其對數位與非數位媒體類型的存取。 2. 媒體標記 組織應建立媒體標記之方法且進行適當標記。 3. 媒體儲存 組織應建立並落實個人資料媒體儲存之安全作業規定。 4. 媒體傳輸

	個人資料儲存媒體運輸或傳輸到管控區域外時，應採用適當安全防護措施。 5. 媒體汰除 組織於媒體汰除時應透過適當程序加以安全汰除，確保無法被還原。
A8.7.5 實體與環境安全	管理目標：防止儲存個人資料場所不受人為因素非授權入侵與存取而導致個人資料之洩漏。 管理措施： 1. 實體存取控制 組織應識別儲存個人資料之安全周界，於存放個人資料場所採取適當安全措施，並針對場所之進出加以管控。 2. 實體存取監視 組織應定期檢視已實施安全措施之有效性，並建立個人資料儲存場所監視與環境控管安全機制。
A8.7.6 資訊傳輸	管理目標：防止個人資料傳輸時遭非授權揭露。 管理措施： 1. 邊界保護 組織於系統外部邊界與系統內部的關鍵內部邊界，應建立適當監視與控制通訊的介面防護。 2. 傳輸機密性 組織應採取適當措施確保個人資料傳輸的機密性。
A8.7.7 系統與資訊完整性	管理目標：確保個人資料資通系統安全控管措施之有效性。 管理措施： 1. 安全性檢測 組織應進行資通系統脆弱性識別、報告與修正作業。系統更新前應事先進行測試，瞭解該更新對資通系統可能產生之結果與衝擊。 2. 稽核事件 組織應規劃資通系統有稽核特定事件之功能，並決定應稽核之特定系統事件，對稽核紀錄之

	存取管理，僅限於有權限之使用者。 3. 惡意程式防護 組織應針對資通系統可能的出入端點、工作站、伺服器或可攜式媒體等設備，有效部署惡意程式防護機制。 4. 資通系統監看 組織應透過資通系統監視內向與外向通訊，發現資通有被入侵跡時，應依程序通報特定人員。
A8.7.8 系統發展生命週期階段	管理目標：確保組織系統發展之安全需求（含機密性、完整性、可用性）。 管理措施：組織於系統發展生命週期需求、設計開發、測試及部署與維運階段運用安全系統發展生命週期（SSDLC）概念之安全設計概念。
A8.7.9 系統發展生命週期委外階段	管理目標：確保組織系統發展之委外安全管理。 管理措施：組織資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、完整性、可用性）納入委外契約。
A8.7.10 獲得程序與系統文件	管理目標：確保資料流管控與文件管理之機制 管理措施：組織系統開發、測試及正式作業應為區隔，且應避免使用真實個人資料作為系統之測試資料，如有使用真實個人資料測試系統之必要，應透過相關程序申請並經許可始可採用，並管理相關系統文件。

A8.7.11 營運持續計畫	管理目標：確保組織業務運作正常，訂定最大可容忍中斷時間（MTPD）與最低可接受服務水準。 管理措施： 1. 系統備份 組織應訂定系統可容忍資料損失之時間要求，執行系統碼與資料備份，並定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 2. 系統備援 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。於原服務中斷時，於可容忍時間內，由備援設備取代提供服務，提供最低可接受服務水準。
A8.8 組織人員之管理與監督	
A8.8.1 選任監督	管理目標：確保組織人員適任其角色。 管理措施：組織聘用人員時，應進行適當篩選。
A8.8.2 保密契約	管理目標：確保組織人員瞭解其所承擔之責任。 管理措施：組織與人員簽訂雇傭或委任契約時，應一併簽訂個人資料相關保密契約，並確保於人員離職或職務變動後適當期間內仍負有保密義務。
A8.8.3 教育訓練	管理目標：確保組織人員獲得應有資通安全專業課程訓練或資通安全職能訓練，以利管理制度推動與運作。 管理措施：組織應制定教育訓練計畫，並訂定評量機制。