適用性聲明書					
文件編號	Takming-ISMS-D-036	機密等級	限制使用	版次	1.2

適用性聲明

章節	敘述	適用性		適用或不適用理由	不適用理由/參考文件
		適用	不適用		
A.5	資訊安全政策				
A.5.1	資訊安全之管理指導方針 依營運要求及相關法律與法規，提供資訊安全之管理指導方針及支持。				
A.5.1.1	資訊安全政策 資訊安全政策應由管理階層定義並核准,且對所有員工及相關外部各方公布及傳達。				
A.5.1.2	資訊安全政策之審查 資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。				
A.6	資訊安全組織				
A.6.1	內部組織 建立管理框架，以於組織內啟動及控制資訊安全之實作及運作。				
A.6.1.1	資訊安全之角色及責任 應定義及配置所有資訊安全責任。				
A.6.1.2	職務區隔 衝突之職務及責任範圍應予以區隔，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。				
A.6.1.3	與權責機關之連繫 應維持與相關權責機關之適切聯繫。				
A.6.1.4	與特殊關注方之連繫				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	應維持與各特殊關注方或其他各種專家安全論壇及專業協會之適切聯繫。				
A.6.1.5	專案管理之資訊安全 不論專案之型式，應在專案管理中因應資訊安全。				
A.6.2	行動裝置及遠距工作 確保遠距工作及使用行動裝置之安全。				
A.6.2.1	行動裝置政策 應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。				
A.6.2.2	遠距工作 應實作政策及支援之安全措施，以保護存取、處理或儲存於遠距工作場所之資訊。				
A.7	人力資源安全				
A.7.1	聘用前 確保員工及承包者瞭解其將承擔之責任，且其適任其角色。				
A.7.1.1	篩選 對所有可能被聘用者所進行之背景調查，應依照相關法律、法規及倫理，並應相稱於營運要求及其將存取之資訊保密等級及組織所察覺之風險聘用。				
A.7.1.2	聘用條款及條件 施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。				
A.7.2	聘用期間 確保員工及承包者認知並履行其資訊安全責任。				
A.7.2.1	管理階層責任 管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.7.2.2	資訊安全認知、教育及訓練 施行單位內所有員工及相關之承包者，均應接受與其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。				
A.7.2.3	懲處過程 應具備正式及已傳達之懲處過程，以對違反資訊安全之員工採取行動。				
A.7.3	聘用之終止及變更 將保護組織利益，納入聘用變更或終止聘用過程之一部份。				
A.7.3.1	聘用責任之終止或變更 應對員工及承包者定義、傳達於聘用終止或變更後，資訊安全責任及義務仍保持有效，並執行之。				
A.8	資產管理				
A.8.1	資產責任 識別組織之資產並定義適切之保護責任。				
A.8.1.1	資產清冊 應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。				
A.8.1.2	資產擁有權 清冊中所維持之資產應有擁有者。				
A.8.1.3	資產之可被接受的使用 對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。				
A.8.1.4	資產之歸還 所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	組織資產。				
A.8.2	資訊分級 確保資訊依其對組織之重要性，受到適切等級的保護。				
A.8.2.1	資訊之分級 資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。				
A.8.2.2	資訊之標示 應依施行單位所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。				
A.8.2.3	資產之處置 應依施行單位所採用之資訊分級方案，發展及實作處置資產之程序。				
A.8.3	媒體處置 防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。				
A.8.3.1	可移除式媒體之管理 應依施行單位所採用之資訊分級方案，實作管理可移除式媒體之程序。				
A.8.3.2	媒體之汰除 當不再需要媒體時，應使用正式程序加以安全汰除。				
A.8.3.3	實體媒體傳送 應保護含有資訊之媒體於傳送時，不受未經授權的存取、誤用或毀損。				
A.9	存取控制				
A.9.1	存取控制之營運要求事項 限制對資訊及資訊處理設施之存取。				
A.9.1.1	存取控制政策 存取控制政策應依據營運及資訊安全要求事項，建立、文件化及審查之。				
A.9.1.2	對網路及網路服務之存取				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	應僅提供予使用者存取其已被特定授權使用之網路及網路服務。				
A.9.2	使用者存取管理 確保經授權使用者對系統及服務之存取，並防止未經授權之存取。				
A.9.2.1	使用者註冊及註銷 應實作正式之使用者註冊及註銷過程，俾能指派存取權限。				
A.9.2.2	使用者存取權限之配置 應實作正式之使用者存取權限配置程序，以對所有型式之使用者對所有系統及服務，指派或撤銷存取權限。				
A.9.2.3	具特殊存取權限之管理 應限制及控制具特殊存取權限之配置及使用。				
A.9.2.4	使用者之秘密鑑別資訊的管理 應以正式之管理過程控制秘密鑑別資訊的配置。				
A.9.2.5	使用者存取權限之審查 施行單位應定期審查使用者存取權限。				
A.9.2.6	存取權限之移除或調整 所有員工及外部使用者對資訊及資訊處理設施之存取權限，一旦其聘用、契約或協議終止時，均應予以移除；或於其聘用、契約或協議變更時均須調整之。				
A.9.3	使用者責任 令使用者對保全其鑑別資訊負責。				
A.9.3.1	秘密鑑別資訊之使用 於使用秘密鑑別資訊時，應要求使用者遵循施行單位之實務規定。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.9.4	系統及應用存取控制 防止系統及應用遭未經授權之存取。				
A.9.4.1	資訊存取限制 應根據存取控制政策，限制對資訊及應用系統功能之存取。				
A.9.4.2	保全登入程序 當存取控制政策要求時，應以保全登入程序，控制對系統及應用之存取。				
A.9.4.3	通行碼管理系統 通行碼管理系統應為互動式，並應確保嚴謹通行碼。				
A.9.4.4	具特殊權限公用程式之使用 應限制及嚴密控制可能篡越系統及應用控制措施之公用程式的使用。				
A.9.4.5	對程式源碼之存取控制 應限制對程式原始碼之存取。				
A.10	密瑪學				
A.10.1	密碼 確保適當及有效使用密碼學，以保護資訊之機密性、鑑別性及/或完整性。				
A.10.1.1	使用密碼式控制措施(加密控制措施)之政策 應發展及實作政策，關於資訊保護之密碼式控制措施的使用。				
A.10.1.2	金鑰管理 應加以發展及實作政策，關於貫穿其整個生命週期之密碼金鑰的使用、保護及生命期。				
A.11	實體及環境安全				
A.11.1	保全區域 防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.11.1.1	實體安全周界 應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。				
A.11.1.2	實體進入控制措施 保全區域應藉由適切之進入控制措施加以保護，以確保僅允許經授權人員進出。				
A.11.1.3	保全之辦公室、房間及設施 應設計資訊處理設施所在區域之實體安全並施行之。				
A.11.1.4	防範外部及環境威脅 應設計並施行實體保護，以防範天然災害、惡意攻擊或事故。				
A.11.1.5	於保全區域內工作 應設計及施行資訊處理設施所在區域內工作之程序。				
A.11.1.6	交付及裝卸區 對諸如交付及裝卸區及其他未經授權人員可進入作業場所之進出點，應加以控制；若可能，應與資訊處理設施隔離，以避免未經授權之存取。				
A.11.2	設備 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。				
A.11.2.1	設備安置及保護 應安置並保護設備，以降低來自環境之威脅及危害造成的風險，以及未經授權存取之機會。				
A.11.2.2	支援之公用服務事業 應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。				
A.11.2.3	佈纜安全				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。				
A.11.2.4	設備維護 應正確維護設備，以確保其持續之可用性及完整性。				
A.11.2.5	財產之攜出 未經事前授權，不得將設備、資訊或軟體帶出場域外。				
A.11.2.6	場所外設備及資產的安全 安全應適用於場域外資產，並將於施行單位場所外工作之不同風險納入考量。				
A.11.2.7	設備汰除或再使用之保全 含有儲存媒體之所有設備組件，於汰除前或再使用前應加以查證，以確保任何敏感性資料及有版權之軟體已被移除或安全地覆寫。				
A.11.2.8	無人看管之使用者設備 使用者應確保無人看管之設備具備適切保護。				
A.11.2.9	桌面淨空及螢幕淨空政策 對紙本及可移除式儲存媒體應採用桌面淨空政策，且對資訊處理設施應採用螢幕淨空政策。				
A.12	運作安全				
A.12.1	運作程序及責任 確保資訊處理設施之正確及安全操作。				
A.12.1.1	文件化運作程序 運作程序應加以文件化，並使所有需要之使用者均可取得。				
A.12.1.2	變更管理 應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.12.1.3	容量管理 各項資源之使用應受監視及調整，並對未來容量要求預作規劃，以確保所要求之系統效能。				
A.12.1.4	開發、測試及運作環境之區隔 應區隔開發、測試及運作之環境，以降低對運作環境未經授權存取或變更的風險。				
A.12.2	防範惡意軟體 確保資訊及資訊處理設施，以防範惡意軟體。				
A.12.2.1	防範惡意軟體之控制措施 應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。				
A.12.3	備份 防範資料漏失。				
A.12.3.1	資訊備份 應依議定之備份政策，定期取得資訊、軟體及系統的影像檔備份複本，並測試之。				
A.12.4	存錄及監視 記錄事件並產生證據。				
A.12.4.1	事件存錄 應產生、保存並定期審查記錄使用者活動、異常、錯誤及資訊安全事件之事件日誌。				
A.12.4.2	日誌資訊之保護 應防範存錄設施及日誌資訊遭竄改及未經授權存取。				
A.12.4.3	管理者及操作者日誌				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。				
A.12.4.4	鐘訊同步 組織或安全領域內所有相關資訊處理系統之鐘訊，應與單一參考時間源同步。				
A.12.5	運作中軟體之控制 確保運作中系統之完整性。				
A.12.5.1	運作中系統之軟體安裝 應實作各項程序，以控制對運作中系統之軟體安裝。				
A.12.6	技術脆弱性管理 防範對技術脆弱性之利用。				
A.12.6.1	技術脆弱性管理 應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。				
A.12.6.2	對軟體安裝之限制 應建立並實作使用者安裝軟體之管控規則。				
A.12.7	資訊系統稽核考量 使稽核活動對運作中系統之衝擊降至最低。				
A.12.7.1	資訊系統稽核控制措施 應仔細規劃並議定，涉及運作中系統之稽核要求事項及活動，以使營運過程中斷降至最低。				
A.13	通訊安全				
A.13.1	網路安全管理 確保對網路及其支援之資訊處理設施中資訊之保護。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.13.1.1	網路控制措施 應實施網路控制措施，維護網路安全。				
A.13.1.2	網路服務之安全 應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外所提供。				
A.13.1.3	網路之區隔 應區隔各群組之資訊服務、使用者及資訊系統使用的網路。				
A.13.2	資訊傳送 維護組織內及與任何外部個體所傳送資訊之安全。				
A.13.2.1	資訊傳送政策及程序 應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。				
A.13.2.2	資訊傳送協議 協議應闡明組織與外部各方間營運資訊之安全傳送。				
A.13.2.3	電子傳訊 應適切保護電子傳訊時所涉及之資訊。				
A.13.2.4	機密性或保密協議 應識別、定期審查及文件化，以反映施行單位對資訊保護之需要的機密性或保密協議之要求事項。				
A.14	系統獲取、開發及維護				
A.14.1	資訊系統之安全要求事項 確保資訊安全係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。				
A.14.1.1	資訊安全要求事項分析及規格				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	資訊安全相關要求，應納入新資訊系統或既有資訊系統之強化的要求事項中。				
A.14.1.2	保全公共網路之應用服務 應防範於公共網路上傳送的應用服務中涉及之資訊，免於詐欺活動、契約爭議及未經授權揭露與修改。				
A.14.1.3	保護應用服務交易 應保護應用服務交易中涉及之資訊，以防止不完整傳輸、誤選路由(mis-routing)、未經授權之訊息修改、未經授權之揭露、未經授權之訊息複製或重演。				
A.14.2	於開發及支援過程中之安全 確保於資訊系統之開發生命週期內，設計及實作資訊安全。				
A.14.2.1	保全開發政策 應建立軟體及系統開發之規則，並應用至施行單位內之開發。				
A.14.2.2	系統變更控制程序 應藉由使用正式之變更控制程序，以控制開發生命周期內之系統變更。				
A.14.2.3	運作平台變更後，應用之技術審查 當運作平台變更時，應審查及測試營運之關鍵應用，以確保對組織運作或安全無不利衝擊。				
A.14.2.4	軟體套件變更之限制 應不鼓勵修改軟體套件，且僅限於必要變更，並應嚴格控制所有變更。				
A.14.2.5	保全系統工程原則 保全系統之工程原則，應予建立、文件化、維持及應用於所有資訊系統實作工作。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.14.2.6	安全發展環境 對涵蓋整個系統開發生命周期之系統開發及整合工作，施行單位應建立並適切地保護安全開發環境。				
A.14.2.7	委外開發 組織應監督及監視委外系統開發活動。				
A.14.2.8	系統安全測試 於開發中，應實施安全功能之測試。				
A.14.2.9	系統驗收測試 應建立新資訊系統、系統升級及新版本之驗收測試計畫及準則。				
A.14.3	測試資料 確保測試用資料之保護。				
A.14.3.1	測試資料之保護 應小心選擇、保護及控制測試資料。				
A.15	供應者關係				
A.15.1	供應者關係中之資訊安全 確保對供應者可取得之組織資產的保護。				
A.15.1.1	供應者關係之資訊安全政策 應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。				
A.15.1.2	於供應者協議中闡明安全性 應與每個可能存取、處理、儲存或傳達資訊，或提供IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。				
A.15.1.3	資訊及通訊技術供應鏈				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。				
A.15.2	供應者服務交付管理 維持資訊安全及服務交付之議定等級與供應者協議一致。				
A.15.2.1	供應者服務之監視及審查 組織應定期監視、審查及稽核供應者服務交付。				
A.15.2.2	管理供應者服務之變更 應管理供應者所提供服務之變更，包括維持及改善既有的資訊安全政策、程序及控制措施，並考量所涉及之營運資訊、系統及過程的關鍵性，以及風險之重新評鑑。				
A.16	資訊安全事故管理				
A.16.1	資訊安全事故及改善之管理 確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。				
A.16.1.1	責任及程序 應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。				
A.16.1.2	通報資訊安全事件 應循適切之管理管道，儘速通報資訊安全事件。				
A.16.1.3	通報資訊安全弱點 應要求使用資訊系統及服務之員工及承包者，注意並通報任何系統或服務中所觀察到或可疑之資訊安全弱點。				
A.16.1.4	資訊安全事件評估及決策 應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.16.1.5	對資訊安全事故之回應 應依文件化程序，回應資訊安全事故。				
A.16.1.6	由資訊安全事故中學習 應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性或衝擊。				
A.16.1.7	證據之收集 組織應定義及應用程序，以識別、收集、取得及保存可用作證據之資訊。				
A.17	營運持續管理之資訊安全層面				
A.17.1	資訊安全持續 資訊安全持續應嵌入組織之營運持續管理系統中。				
A.17.1.1	規劃資訊安全持續 施行單位應決定對其資訊安全之要求事項，以及於不利情況下〔例：危機或災難期間〉，對資訊安全之持續性要求事項。				
A.17.1.2	實作資訊安全持續 施行單位應建立、文件化、實作及維持過程、程序及控制措施，以確保在不利情況期間所要求之資訊安全持續等級。				
A.17.1.3	查證、審查及評估資訊安全持續 組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。				
A.17.2	多重備援 確保資訊處理設施之可用性。				
A.17.2.1	資訊設備之可用性 應對資訊處理設施實作充分之多重備援，以符合可用性要求。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

A.18	遵循性				
A.18.1	對法律及契約要求事項之遵循 避免違反有關資訊安全之法律、法令、法規或契約義務，以及任何安全要求事項。				
A.18.1.1	適用之法規及契約的要求事項之識別 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。				
A.18.1.2	智慧財產權 應實作適切程序，以確保遵循智慧財產權及專屬軟體產品使用之相關法律、法令及契約的要求事項。				
A.18.1.3	紀錄之保護 應依法令、法規、契約及營運要求保護紀錄，免於遺失、毀損、偽造、未經授權存取及未經授權發布。				
A.18.1.4	個人可識別資訊之隱私及保護 應依適用之相關法令、法規中之要求，以確保符合個人可識別資訊之隱私及保護。				
A.18.1.5	密碼式控制措(加密控制措施)的監管 應使用密碼式控制措施(加密控制措施)，以遵循所有相關協議、法律及法規。				
A.18.2	資訊安全審查 確保依組織政策及程序，實作及運作資訊安全。				
A.18.2.1	資訊安全之獨立審查 應依規劃之期間或當發生重大變更時，獨立審查組織對管理資訊安全之作法及其實作〔亦即資訊安全之各項控制目標、控制措施、政策、過程及程序〕。				
A.18.2.2	安全政策及標準之遵循性				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後

	管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。				
A.18.2.3	技術遵循性審查 應定期審查資訊系統對組織之資訊安全政策及標準的遵循性。				

適用或不適用的理由(1)政策要求(2)風險評估的結果或降低風險所採取之措施(3)運作需求或程序規範(4)不適用理由如後