0000000000 公司

文件編號	ISMS-D-001-01	適用性聲明書	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

壹、 適用範圍 (Scope):

資訊安全管理涵蓋本公司0000000000000。依據適用性聲明書版次1.0。

貳、 適用條款與說明

項次		控制目標	控制措施		選用與否 Y/N	選用與不選用理由	參考文件與資料
A.5	資訊安全政策	A.5.1 資訊安全之管理指導方針目標：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	Y	為確保資訊安全管理系統順利運作，達成ISMS 政策性文件控制目標。	資訊安全管理政策
			A.5.1.2	資訊安全政策之審查	Y	為維持「ISMS 政策性文件」之適用性及有效性，須定期進行檢討及修訂。	資訊安全管理政策 資訊安全管理作業程序
A.6	資訊安全之組織	A.6.1 內部組織目標：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	Y	為使資訊安全管理系統能明確定義資訊安全相關職務與責任及跨單位工作協調，成立資訊安全組進行相關管理活動。	資訊安全組織管理作業程序
			A.6.1.2	職務區隔	Y	為有效落實ISMS政策性文件及相關管理規範，並降低人員蓄意或誤用對資訊系統所造成之風險，應將人員分工並作職責區隔。	資訊安全組織管理作業程序
			A.6.1.3	與權責機關之連繫	Y	為確保資訊安全要求事項或事件發生時能立即得到相關之建議、支援或緊急之處理，應與主管機關維持適當之聯繫。	資訊安全組織管理作業程序

			A.6.1.4	與特殊關注方之連繫	Y	為取得新技術或相關資訊安全知識，應與資訊通全專家(如對網路維運、相關主機或防火牆產品諮詢)共同提供資訊安全相關建議。	資訊安全組織管理作業程序
			A.6.1.5	專案管理之資訊安全	Y	為確保資訊安全管理系統之各項要求之符合性與有效性，應於各新建或更新系統或設備之專案管理作業內，要求納入資訊安全考量。	資訊系統獲取、開發及維護管理作業程序 通訊與作業管理作業程序
		A.6.2 行動裝置及遠距工作 目標：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	Y	為確保可攜式及移動式電腦媒體等行動裝置之使用皆有適當管控，應制訂相關管理政策。	通訊與作業管理作業程序
			A.6.2.2	遠距工作	Y	範圍內可經由遠距作業方式，查看系統及機房之狀況，故需要實施控制措施。	通訊與作業管理作業程序 存取控制管理作業程序
A.7	人力資源安全	A.7.1 聘用前 目標：確保員工及承包者瞭解其將承擔之責任，且適任其角色。	A.7.1.1	篩選	Y	為確保人員進用時符合內部規定或資格之要求，建立相關作業人員任用篩選標準。	資訊安全組織管理作業程序 人力資源安全管理作業程序
			A.7.1.2	聘用條款及條件	Y	為確保人員適用於工作，人員任用時須描述人員資格與條件。	人力資源安全管理作業程序
		A.7.2 聘用期間 目標：確保員工及承包者認知並履行其資訊安全	A.7.2.1	管理階層責任	Y	為落實資訊安全相關規定，員工或委外廠商於工作執掌中應包含明確之資訊安全管理責任。	人力資源安全管理作業程序

		責任。	A.7.2.2	資訊安全認知、教育及訓練	Y	為加強人員資訊安全認知以及相關技能，須進行相關教育訓練。	人力資源安全管理作業程序
			A.7.2.3	懲處過程	Y	違反資訊安全規定情節嚴重者依本公司相關規定議處，對於造成他人權益損害者，依相關法律處理。	人力資源安全管理作業程序
		A.7.3 聘用之終止及變更 目標：將保護組織利益納入聘用變更或終止聘用過程之一部分。	A.7.3.1	聘用責任之終止或變更	Y	為確保人員聘僱終止後的一段時間內，保密協定及任用條件仍為有效，應於雙方協定或契約中清楚定義。	人力資源安全管理作業程序
A.8	資產管理	A.8.1 資產責任 目標：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	Y	確認範圍內所需保護之資產，清查所有資訊資產並適當分類列冊。	資訊資產管理作業程序
			A.8.1.2	資產擁有權	Y	為確保所有資產皆有適當之安全維護，指派負責人員或部門保管。	資訊資產管理作業程序
			A.8.1.3	資產之可被接受使用	Y	為確保人員對資產使用應遵循的規範，制訂相關管理規定。	資訊資產管理作業程序
			A.8.1.4	資產之歸還	Y	為確保所有人員在聘僱或契約終止時歸還其使用之資產，應制訂清楚規範。	資訊資產管理作業程序

		A.8.2 資訊分級 目標：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	**Y**	為執行資產之保護措施，應制訂資產的分級原則，以區別資訊之機密等級。	資訊資產管理作業程序
			A.8.2.2	資訊之標示	**Y**	為確保各資產皆有分級原則以區別資訊之機密等級，應制訂資產標示程序。	資訊資產管理作業程序
			A.8.2.3	資產之處置	**Y**	為確保各資產皆有分級原則以區別資訊之機密等級，應制訂資產處理程序。	資訊資產管理作業程序
		A.8.3 媒體處置 目標：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	**Y**	為確保可攜式及移動式電腦媒體之使用皆有適當管控，應制訂相關管理規定。	資訊資產管理作業程序
			A.8.3.2	媒體之汰除	**Y**	為避免媒體因報廢不當將敏感資料外洩，應制訂管控方式。	資訊資產管理作業程序
			A.8.3.3	實體媒體傳送	**Y**	為確保輸送中的實體媒體安全，不受未經授權的存取破壞。	資訊資產管理作業程序
A.9	存取控制	A.9.1 存取控制之營運要求事項 目標：限制對資訊及資訊處理設	A.9.1.1	存取控制政策	**Y**	為確保系統、網路與實體存取之安全，應制訂一套符合需求之存取控制政策。	存取控制管理作業程序

		施之存取。	A.9.1.2	對網路及網路服務之存取	**Y**	為確保網路與網路服務之安全，應制訂一套符合需求之存取程序。	存取控制管理作業程序
		A.9.2 使用者存取管理 目標：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	**Y**	為確保使用者帳號之安全，應有正式授權及註銷之程序。	存取控制管理作業程序
			A.9.2.2	使用者存取權限之配置	**Y**	為確保資訊設備或系統存取之安全，應依據既定的存取控制政策及執行業務所需，提供應用系統的使用者(包括支援人員)存取資訊和應用系統功能的權限。	存取控制管理作業程序
			A.9.2.3	具特殊存取權限之管理	**Y**	為降低擁有特殊權限之管理者可能造成之非法存取，應透過正式授權管道授權。	存取控制管理作業程序
			A.9.2.4	使用者之秘密鑑別資訊的管理	**Y**	為確保登入作業系統存取之安全，須使用帳號通行碼進行使用者身分識別。	存取控制管理作業程序
			A.9.2.5	使用者存取權限之審查	**Y**	為確保使用者存取權限是否合宜，應定期執行存取權限審查。	存取控制管理作業程序
			A.9.2.6	存取權限之移除或調整	**Y**	人員在聘僱或契約終止或職務調整時，為確保資訊安全，應移除或調整其對資訊設備的存取權限。	存取控制管理作業程序

		A.9.3 使用者責任 目標：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	Y	為確保通行碼使用符合要求，使用者應確實遵守通行碼使用原則。	存取控制管理作業程序
		A.9.4 系統及應用存取控制 目標：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	Y	為確保資訊設備或系統存取之安全，應依據既定的存取控制政策及執行業務所需，提供應用系統的使用者(包括支援人員)存取資訊和應用系統功能的權限。	存取控制管理作業程序
			A.9.4.2	保全登入程序	Y	為降低不當存取之風險，對登入作業系統嚴加限制與控制。	存取控制管理作業程序
			A.9.4.3	通行碼管理系統	Y	為確保使用者通行碼之安全，應制訂管理方式。	存取控制管理作業程序
			A.9.4.4	具特殊權限公用程式之使用	Y	為確保應用程式之安全，應對其使用之公用程式及其權限嚴加限制與控制。	存取控制管理作業程序
			A.9.4.5	對程式源碼之存取控制	Y	對系統程式原始碼之存取須加以控管。	存取控制管理作業程序
A.10	密碼學	A.10.1 密碼式控制措施 目標：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之政策	Y	為確保委外開發，購置與自行發展之軟硬體符合需求，保護資料之機密與完整性或鑑別性。	存取控制管理作業程序 資訊系統獲取、開發及維護管理作業程序 通訊與作業管理作業程序
			A.10.1.2	金鑰管理	Y	為確保金鑰作業之安全管理。	通訊與作業管理作業程序

0000000000 公司

文件編號	ISMS-D-001-01	適用性聲明書	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

A.11	實體及環境安全	A.11.1 保全區域 目標：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。	A.11.1.1	實體安全周界	**Y**	為確保相關實體安全控制符合安全上的需求，應明確定義實體安全範圍。	實體與環境安全管理作業程序
			A.11.1.2	實體進入控制措施	**Y**	為確保只有授權人員方可進入實體安全區域，應制訂人員進出管制規定。	實體與環境安全管理作業程序
			A.11.1.3	保全之辦公室、房間及設施	**Y**	為確保辦公區域設施之安全，應有適當之管控措施。	實體與環境安全管理作業程序
			A.11.1.4	防範外部及環境威脅	**Y**	為確保安全工作區域遭受外在環境威脅如火災、水災等重大災害之影響，應設置適當之保護措施。	實體與環境安全管理作業程序
			A.11.1.5	於保全區域內工作	**Y**	為確保在安全區域內工作之人員有適當之控制措施，以避免惡意行為之發生。	實體與環境安全管理作業程序
			A.11.1.6	交付及裝卸區	**Y**	設置安全作業區域設施，確保應有進出、收發及裝卸之管控措施。	實體與環境安全管理作業程序
		A.11.2 設備 目標：防止資產之遺失、損害、遭竊或破解，並	A.11.2.1	設備安置及保護	**Y**	為避免設備因環境影響而造成損害，應考量合適地點並加以安置保護。	實體與環境安全管理作業程序

		防止組織運作中斷。	A.11.2.2	支援之公用服務事業	Y	為確保設備不受電源或其它設施失效而中斷，應對支援設施(如空調、電力、水源等)定期維護檢查。	實體與環境安全管理作業程序
			A.11.2.3	佈纜安全	Y	為避免線路遭受破壞或拔除，線路應標示及保護。	實體與環境安全管理作業程序
			A.11.2.4	設備維護	Y	為確保設備之持續可用性與完整性，應予正確地維護。	實體與環境安全管理作業程序
			A.11.2.5	資產之攜出	Y	為確保資產不被任意攜出，應訂定相關管控措施。	實體與環境安全管理作業程序
			A.11.2.6	場所外設備及資產之安全	Y	為確保場外設施之安全，應有適當之管控措施。	實體與環境安全管理作業程序
			A.11.2.7	設備汰除或再使用之保全	Y	為確保相關設備報廢或回收使用時，不洩漏資料，應訂定相關管控措施。	實體與環境安全管理作業程序
			A.11.2.8	無人看管之使用者設備	Y	範圍內之使用者設備，依程序指派人員管理沒有無人看管的使用者設備。	實體與環境安全管理作業程序
			A.11.2.9	桌面淨空及螢幕淨空政策	Y	為降低機敏性資料遭不當存取，應制訂電腦螢幕淨空及桌面淨空規範。	實體與環境安全管理作業程序

0000000000 公司

文件編號	ISMS-D-001-01	適用性聲明書	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

A.12	運作安全	A.12.1 運作程序及責任 目標：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	**Y**	為確保資訊處理及各項作業皆有書面程序提供遵循，應製作相關之程序，讓需要之人員皆可取得。	通訊與作業管理作業程序
			A.12.1.2	變更管理	**Y**	為避免作業系統及應用系統軟體因變更不當所造成之風險，應制訂相關變更管理規定。	通訊與作業管理作業程序
			A.12.1.3	容量管理	**Y**	為確保系統之執行效能，各系統應考量其設備及系統之容量規劃及資源管理。	通訊與作業管理作業程序
			A.12.1.4	開發、測試及運作環境之區隔	**Y**	為避免系統之開發測試活動可能會影響正式營運，應將開發測試作業與正式作業區隔。	通訊與作業管理作業程序
		A.12.2 防範惡意軟體 目標：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	**Y**	為避免資料、軟體遭受惡意軟體或行動碼之攻擊，應加以防範、警示或制訂必要之回復措施。	通訊與作業管理作業程序
		A.12.3 備份 目標：防範資料漏失。	A.12.3.1	資訊備份	**Y**	為確保所有重要的資訊或軟體在資料損毀時能立即復原，應定期執行備份與測試。	通訊與作業管理作業程序

		A.12.4 存錄及監視 目標：記錄事件並產生證據。	A.12.4.1	事件存錄	Y	為確保使用者存取、失誤或異常事件之紀錄(Log)於安全事件發生時可做為調查依據，相關系統之活動皆需留下事件紀錄，以供稽核。	通訊與作業管理作業程序
			A.12.4.2	日誌資訊之保護	Y	為降低系統或稽核日誌遭修改或不當存取風險，應對系統或稽核日誌加以保護。	通訊與作業管理作業程序
			A.12.4.3	管理者及操作者日誌	Y	為確保系統之管理能有效執行，系統管理者及操作活動應留下日誌。	通訊與作業管理作業程序
			A12.4.4	鐘訊同步	Y	為確保資訊系統的時間一致性，各系統應定期進行時間校正。	通訊與作業管理作業程序
		A.12.5 運作中軟體之控制 目標：確保運作中系統之完整性。	A.12.5.1	對運作中系統之軟體安裝	Y	為確保人員遵守智慧財產法令法規及系統之安全，應制訂適當之管制程序。	通訊與作業管理作業程序
		A.12.6 技術脆弱性管理 目標：防範對技術脆弱性之利用。	A.12.6.1	技術脆弱性管理	Y	為確保資訊技術弱點能適時找出並修補，應制訂相關管理方式。	通訊與作業管理作業程序
			A.12.6.2	對軟體安裝之限制	Y	為確保人員遵守智慧財產法令法規及系統之安全，應制訂適當之管制程序。	通訊與作業管理作業程序

		A.12.7 資訊系統稽核考量 目標：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	**Y**	為確保稽核時之安全，涉及作業系統與網路安全的檢查活動應獲同意。	通訊與作業管理作業程序
A.13	通訊安全	A.13.1 網路安全管理 目標：確保對網路及其支援之資訊處理設施中資訊之保護。	A.13.1.1	網路控制措施	**Y**	為確保透過網路傳送資料之機密及完整性，應加入登入管制或監控機制。	通訊與作業管理作業程序
			A.13.1.2	網路服務之安全	**Y**	為確保網路服務之安全，應制訂網路服務管理要求。	通訊與作業管理作業程序
			A.13.1.3	網路之區隔	**Y**	為確保網路之安全性，應採取適當區隔管理。	通訊與作業管理作業程序
		A.13.2 資訊傳送 目標：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	**Y**	為確保與外機關(構)之資料與軟體交換之安全，應制訂管控程序。	通訊與作業管理作業程序
			A.13.2.2	資訊傳送協議	**Y**	為確保與外機關(構)之資料交換之可追蹤性與不可否認性應有適當之協議。	通訊與作業管理作業程序
			A.13.2.3	電子傳訊	**Y**	為確保與外機關(構)之電子資料交換之安全，應制訂管控程序。	通訊與作業管理作業程序

			A.13.2.4	機密性或保密協議	Y	為確保委外與第三方廠商契約內，應約定服務水準、機密性或保密之資訊安全協議及制訂相關安全管制措施。	通訊與作業管理作業程序
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 目標：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	Y	新建置之資訊系統或現有資訊系統的提升作業中，對營運要求之功能，應分析其安全要求與安全規格。	資訊系統獲取、開發及維護管理作業程序
			A.14.1.2	保全公共網路之應用服務	Y	有公開的網站，提供對外服務。	資訊系統獲取、開發及維護管理作業程序
			A.14.1.3	保護應用服務交易	Y	新建置之資訊系統或現有資訊系統作業中，對保護應用服務交易之營運要求之功能。	資訊系統獲取、開發及維護管理作業程序
		A.14.2 於開發及支援過程中之安全 目標：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	Y	為建立資訊系統於獲取與維護時，依循相關資訊安全管理規定，以確保資訊系統開發與敏感資訊處理之安全性，保障開發流程之品質。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.2	系統變更控制程序	Y	為降低不當變更造成資訊系統毀損的情形，應對變更的執行採取適當的控制措施。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.3	運作平台變更後，應用之技術審查	Y	為確保作業系統變更時不影響應用系統，應在實施完成後進行適切的檢查。	資訊系統獲取、開發及維護管理作業程序

			A.14.2.4	軟體套件變更之限制	Y	為確保系統之安全，應防止修改套裝軟體的行為。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.5	保全系統工程原則	Y	為建立資訊系統於獲取與維護時，依循相關資訊安全管理規定，以確保資訊系統開發與敏感資訊處理之安全性，保障開發流程之品質。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.6	保全發展環境	Y	為建立資訊系統於獲取與維護時，依循相關資訊安全管理規定，以確保資訊系統開發與敏感資訊處理之安全性，保障開發流程之品質。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.7	委外開發	Y	要求委外廠商遵循系統開發與維護之安全要求。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.8	系統安全測試	Y	為確保資訊系統，依循相關資訊安全管理規定辦理並符合業務所需，以確保資訊系統之安全性。	資訊系統獲取、開發及維護管理作業程序
			A.14.2.9	系統驗收測試	Y	為確保資訊系統，依循相關資訊安全管理規定辦理並符合業務所需，以確保資訊系統之安全性。	資訊系統獲取、開發及維護管理作業程序
		A.14.3 測試資料目標：確保測試用資料之保護。	A.14.3.1	測試資料之保護	Y	為確保系統使用之測試資料安全，應對測試資料之使用有適切的管控。	資訊系統獲取、開發及維護管理作業程序

0000000000 公司

文件編號	ISMS-D-001-01	適用性聲明書	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

A.15	供應者關係	A.15.1 供應者關係中之資訊安全目標：確保對供應者可存取之組織資產的保護。	A.15.1.1	供應者關係之資訊安全政策	Y	為確保資訊服務委外作業之管理，符合資安相關規定及合約要求。	業務委外作業程序
			A.15.1.2	於供應者協議中闡明安全性	Y	為確保資訊服務委外作業之管理，符合資安相關規定及合約要求	業務委外作業程序
			A.15.1.3	資訊及通訊技術供應鏈	Y	為確保資訊服務委外作業，符合資安相關規定及合約要求	業務委外作業程序
		A.15.2 供應者服務交付管理 目標：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	Y	為確保委外與第三方廠商達成契約內約定之服務水準，應制訂相關安全管制措施。	業務委外作業程序
			A.15.2.2	管理供應者服務之變更	Y	為因應委外與第三方服務需變更或調整時可能之風險，應制訂相關條款。	業務委外作業程序
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 目標：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	Y	為降低影響資訊安全的事故造成之影響，應建立適當的處理程序。	資訊安全事故管理作業程序
			A.16.1.2	通報資訊安全事件	Y	為確保發生資訊安全事件時，能迅速依循適當的管理程序通報，應建立正式的通報以及事件反應程序。	資訊安全事故管理作業程序
			A.16.1.3	通報資訊安全弱點	Y	為降低資安事件發生的機率，應規範同仁和廠商在發現、懷疑系統或服務出現安全弱點或受到威脅時，必須立即通報。	資訊安全事故管理作業程序

			A.16.1.4	對資訊安全事件之評鑑及決策	**Y**	為確保發生資訊安全事件時，能迅速依循適當的管理程序通報，應建立正式的通報以及事件反應程序。	資訊安全事故管理作業程序
			A.16.1.5	對資訊安全事故之回應	**Y**	為確保發生資訊安全事件時，能迅速依循適當的管理程序通報，應建立正式的通報以及事件反應程序。	資訊安全事故管理作業程序
			A.16.1.6	由資訊安全事故中學習	**Y**	為降低資訊安全事件發生之機率及損失，應將事件類型與處理方式進行檢討。	資訊安全事故管理作業程序
			A.16.1.7	證據之收集	**Y**	為確保事件發生時有足夠之證據，應制訂證據保存之規定。	資訊安全事故管理作業程序
A.17	營運持續管理之資訊安全層面	A.17.1 資訊安全持續 目標：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	**Y**	為確保資訊系統能穩定的運作，應對重要系統進行營運持續運作規劃。	業務持續管理作業程序
			A.17.1.2	實作資訊安全持續	**Y**	為確保重要系統營運中斷能在一定時間內恢復營運，應發展營運持續相關計畫。	業務持續管理作業程序
			A.17.1.3	查證、審查並評估資訊安全持續	**Y**	為確保營運持續計畫有效，應定期測試及更新。	業務持續管理作業程序
		A.17.2 多重備援 目標：確保資訊處理設施之可用性。	A.17.2.1	資訊處理設施之可用性	**Y**	為確保營運資訊系統之可用性，符合營運之要求。	資訊系統獲取、開發及維護管理作業程序 通訊與作業管理作業程序

0000000000 公司

文件編號	ISMS-D-001-01	適用性聲明書	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

A.18	循遵性	A.18.1 對法律及契約要求事項之遵循 目標：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	**Y**	為避免違反相關法令法規，應鑑別出法令法規。	遵循性管理作業程序
			A.18.1.2	智慧財產權	**Y**	為確保人員遵守智慧財產法令法規之要求，應制訂適當之管制程序。	遵循性管理作業程序
			A.18.1.3	紀錄之保護	**Y**	為保護資訊安全管理制度文件、日誌、稽核報告及管理審查紀錄之安全。	遵循性管理作業程序 資訊安全管理作業程序
			A.18.1.4	個人可識別資訊之隱私及保護	**Y**	應制訂相關規範，以確保個人資料收集、處理皆依相關法令規定執行。	遵循性管理作業程序
			A.18.1.5	密碼式控制措施之監管	**Y**	避免違反合約或觸法，在傳遞機密性或敏感性資料時，以安全之控制措施進行。	遵循性管理作業程序
		A.18.2 資訊安全審查 目標：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	**Y**	為確保資訊安全管理系統推行之符合性與有效性，應由管理階層及獨立稽核人員進行審查。	遵循性管理作業程序 資訊安全管理作業程序
			A.18.2.2	安全政策及標準之遵循性	**Y**	為確保所有資訊安全程序都已確實地執行，應定期檢討或審查。	遵循性管理作業程序 資訊安全管理作業程序

			A.18.2.3	技術遵循性審查	**Y**	系統應定期執行技術性檢查(如駭客攻防演練或弱點掃描)，確保系統符合安全標準。	遵循性管理作業程序