000000000000公司

控制措施有效性量測表

日期： xxx/xx/xx　　流水編號： xxx-xxxx

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
A.5 資訊安全政策	A.5.1 資訊安全之管理指導方針	A.5.1.1 資訊安全政策	檢查是否審查ISMS政策性文件至少1次。		年
		A.5.1.2 資訊安全政策之審查			
A.6 資訊安全之組織	A.6.1 內部組織	A.6.1.1 資訊安全之角色及責任	1.檢查資訊安全管理審查會議召開次數及其會議議題範圍： （1）ISMS資訊安全委員會會議至少召開1次。 2. 檢查是否審查機密性協議文件至少1次。 3. 檢查外部單位聯絡清單是否維持最新資料。 4. 檢查本年度之新專案之管理是否含括資訊安全之各項評估或要求。		年
		A.6.1.2 職務區隔			
		A.6.1.3 與權責機關之連繫			
		A.6.1.4 與特殊關注方之連繫			
		A.6.1.5 專案管理之資訊安全			
	A.6.2 行動裝置及遠距工作	A.6.2.1 行動裝置政策	1.檢查帳號權限申請，是否符合程序書規範，同時抽樣檢查符合性，不得有1件違反。 2.檢查XXX系統之log及帳號權限申請，是否符合程序書規範，同時抽樣檢查符合性，不得有1件違反。		年
		A.6.2.2 遠距工作			
A.7 人力資源安全	A.7.1 聘用前	A.7.1.1 篩選	檢查各單位人員招募是否依程序辦理，同時抽樣檢查符合性，不得有1件違反。		半年
		A.7.1.2 聘用條款及條件			
	A.7.2 聘用期間	A.7.2.1 管理階層責任	檢查資訊安全相關教育訓練上課時數		年
		A.7.2.2 資訊安全認知、教育及訓練			
		A.7.2.3 懲處過程			

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
	A.7.3 聘用之終止及變更	A.7.3.1 聘用責任之終止或變更	抽查離退人員，帳號是否確實刪除或停用，不得有1件違反。		半年
A.8 資產管理	A.8.1 資產責任	A.8.1.1 資產清冊	1.辦理風險評鑑時，抽查資產清冊，內容是否涵蓋新資產(包含服務類)，不得有1件違反。 2.檢查離退人員之作業，是否符合程序書規範，同時抽樣檢查符合性，不得有1件違反。		半年
		A.8.1.2 資產擁有權			
		A.8.1.3 資產之可被接受使用			
		A.8.1.4 資產之歸還			
	A.8.2 資訊分級	A.8.2.1 資訊之分級	抽查機敏性資產是否依機密等級標示，不得有2件以上違反。		年
		A.8.2.2 資訊之標示			
		A.8.2.3 資產之處置			
	A.8.3 媒體處置	A.8.3.1 可移除式媒體之管理	1.檢查儲存媒體汰除，均依規定進行消磁、低階格式化、利用工具清除資料或進行實體破壞，不得有1件違反。 2.傳送實體媒體(如磁帶/光碟等)是否依程序書規範保護，不得有1件違反。		年
		A.8.3.2 媒體之汰除			
		A.8.3.3 實體媒體傳送			
A.9 存取控制	A.9.1 存取控制之營運要求事項	A.9.1.1 存取控制政策	1.抽查重要設備/應用系統之存取權限是否定期審查，不得有1件違反。 2.檢查發生非授權人員非法存取網路成功件數，不得有1件成功。		年
		A.9.1.2 對網路及網路服務之存取			
	A.9.2 使用者存取管理	A.9.2.1 使用者註冊及註銷	1.檢查系統特權帳號是否均已申請，不得有1件違反。		半年
		A.9.2.2 使用者存取權限之配置			
		A.9.2.3 具特殊存取權限之管理			

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
		A.9.2.4 使用者之秘密鑑別資訊的管理	2.是否依程序，至少每半年執行一次帳號權限審查作業並向資訊安全委員會報告。		半年
		A.9.2.5 使用者存取權限之審查			
		A.9.2.6 存取權限之移除或調整			
	A.9.3 使用者責任	A.9.3.1 秘密鑑別資訊之使用	抽查設備及應用系統之通行碼，是否符合規定，不得有1件違反。		半年
	A.9.4 系統及應用存取控制	A.9.4.1 資訊存取限制	1.檢查作業系統是否限制登入失敗次數，不得有1件違反。 2.軟、硬體之新增異動是否事先提出申請，核可後始可變更，不得有1件以上違反。		年
		A.9.4.2 保全登入程序			
		A.9.4.3 通行碼管理系統			
		A.9.4.4 具特殊權限公用程式之使用			
		A.9.4.5 對程式源碼之存取控制			
A.10 密碼學	A.10.1 密碼式控制措施	A.10.1.1 使用密碼控制措施之政策	檢查密碼變更是否符合程序書規範，不得有1件違反。		半年
		A.10.1.2 金鑰管理	檢查金鑰管理員書面保管作業之是否符合程序書規範，不得有1件違反。		半年
A.11 實體及環境安全	A.11.1 保全區域	A.11.1.1 實體安全周界	1.抽查機房人員進出登記是否確實填寫，不得有1件以上違反。 2.抽查辦公區訪客人員進出登記是否確實填寫，不得有1件以上違反。 3.抽查門禁系統之帳號權限申請，是否符合程序書規範，同時抽樣檢查符合性，不得有1件違反。 4.抽查機房及辦公區之消防、空調、用水及用電之維護及可用性，是否符合程序書規範，同時抽樣檢查符合性，不得有1件違反。		半年
		A.11.1.2 實體進入控制措施			
		A.11.1.3 保全之辦公室、房間及設施			
		A.11.1.4 防範外部及環境威脅			
		A.11.1.5 於保全區域內工作			

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
		A.11.1.6 交付及裝卸區			
	A.11.2 設備	A.11.2.1 設備安置及保護	1.檢查機房設備須安置於機架上，不得有1件違反。 2.檢查資通設備汰除是否依規定清除儲存設備資料，不得有1件違反。 3.檢查資通設備是否依規定執行螢幕淨空，不得有1件違反。 4.檢查人員之辦公環境是否依規定執行桌面淨空，不得有1件違反。		半年
		A.11.2.2 支援之公用服務事業			
		A.11.2.3 佈纜安全			
		A.11.2.4 設備維護			
		A.11.2.5 資產之攜出			
		A.11.2.6 場所外設備及資產之安全			
		A.11.2.7 設備汰除或再使用之保全			
		A.11.2.8 無人看管之使用者設備			
		A.11.2.9 桌面淨空及螢幕淨空政策			
A.12 運作安全	A.12.1 運作程序及責任	A.12.1.1 文件化運作程序	1.軟、硬體異動是否事先提出申請核可後始可變更，不得有1件以上違反。 2.是否重要設備實施容量監控，不得有1部設備未納入。		年
		A.12.1.2 變更管理			
		A.12.1.3 容量管理			
		A.12.1.4 開發、測試及運作環境之區隔			
	A.12.2 防範惡意軟體	A.12.2.1 防範惡意軟體之控制措施	1.檢查發生中毒或遭植入木馬程式，造成內部網路無法正常運作之事件數，不得有1件以上。 2.檢查使用者設備是否安裝防毒軟體並持續更新，不得有1件違反。 3.檢查使用者之WINODWS設備是否自動更新系統修補並持續更新，不得有1件違反。		半年

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
	A.12.3 備份	A.12.3.1 資訊備份	抽查使用備份磁帶執行回復資料作業是否正常，無法正常執行作業件數不得多於1件。		年
	A.12.4 存錄及監視	A.12.4.1 事件存錄	1.抽查設備的時間是否均已同步，不得有1件違反。 2.抽查設備的事件存錄是否均依程序辦理，不得有1件違反。		半年
		A.12.4.2 日誌資訊之保護			
		A.12.4.3 管理者及操作者日誌			
		A.12.4.4 鐘訊同步			
	A.12.5 運作中軟體之控制	A.12.5.1 對運作中系統之軟體安裝	1.檢查使用者設備是否安裝未經授權之軟體，不得有1件違反。 2.檢查具有系統特權帳號之使用者設備是否安裝未經授權之軟體，不得有1件違反。		半年
	A.12.6 技術脆弱性管理	A.12.6.1 技術脆弱性管理	是否至少半年執行一次弱點掃描。		半年
		A.12.6.2 對軟體安裝之限制	檢查具有系統特權帳號之使用者設備是否安裝未經授權之軟體，不得有1件違反。		半年
	A.12.7 資訊系統稽核考量	A.12.7.1 資訊系統稽核控制措施	1.檢查執行弱點掃描或滲透測試是否事先取得書面的同意，不得有1件違反。 2.稽核工具的帳號權限審查是否符合規定，不得有1件違反。		半年
A.13 通訊安全	A.13.1 網路安全管理	A.13.1.1 網路控制措施	檢查是否每月分析網路異常使用，不得有1個月未執行。		半年
		A.13.1.2 網路服務之安全			
		A.13.1.3 網路之區隔			
	A.13.2 資訊傳送	A.13.2.1 資訊傳送政策及程序	異地傳送磁帶是否依程序書規範保護，不得		年
		A.13.2.2 資訊傳送協議			

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
		A.13.2.3 電子傳訊	有1件違反。		年
		A.13.2.4 機密性或保密協議			
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	A.14.1.1 資訊安全要求事項分析及規格	檢查專案需求書或專案計畫書中是否提列安全要求與規格，不得有1件違反。		年
		A.14.1.2 保全公共網路之應用服務			
		A.14.1.3 保護應用服務交易			
	A.14.2 於開發及支援過程中之安全	A.14.2.1 保全開發政策	軟、硬體異動是否事先提出申請，核可後始可變更，不得有1件以上違反。		年
		A.14.2.2 系統變更控制程序			
		A.14.2.3 運作平台變更後，應用之技術審查			
		A.14.2.4 軟體套件變更之限制			
		A.14.2.5 保全系統工程原則			
		A.14.2.6 保全發展環境			
		A.14.2.7 委外開發			
		A.14.2.8 系統安全測試			
		A.14.2.9 系統驗收測試			
	A.14.3 測試資料	A.14.3.1 測試資料之保護			
A.15 供應者關係	A.15.1 供應者關係中之資訊安全	A.15.1.1 供應者關係之資訊安全政策			

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
		A.15.1.2 於供應者協議中闡明安全性	1.軟、硬體及人力之委外作業是否依程序檢核作業並核可，不得有1件以上違反。 2.抽查委外廠商維護作業，有否未確實填寫紀錄(如：設備、機電、系統維護…等)，不得有1件違反。		年
		A.15.1.3 資訊及通訊技術供應鏈			
	A.15.2 供應者服務交付管理	A.15.2.1 供應者服務之監視及審查			
		A.15.2.2 管理供應者服務之變更			
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	A.16.1.1 責任及程序	1.抽查發生資安事件時未依規定通報之件數，不得有1件未通報。 2.檢查資訊安全事件通報單，是否重複發生相同資安事故之件數，須少於1件。		年
		A.16.1.2 通報資訊安全事件			
		A.16.1.3 通報資訊安全弱點			
		A.16.1.4 對資訊安全事件之評鑑及決策			
		A.16.1.5 對資訊安全事故之回應			
		A.16.1.6 由資訊安全事故中學習			
		A.16.1.7 證據之收集			
A.17 營運持續管理之資訊安全層面	A.17.1 資訊安全持續	A.17.1.1 規劃資訊安全持續	1.檢查是否依程序執行營運持續計畫之更新作業。 2.檢查是否執行營運持續計畫演練1次以上。		年
		A.17.1.2 實作資訊安全持續			
		A.17.1.3 查證、審查並評估資訊安全持續			
	A.17.2 多重備援	A.17.2.1 資訊處理設施之可用性			
A.18 遵循性	A.18.1 對法律及契約要求事項之遵循	A.18.1.1 適用之法規及契約的要求事項之識別			

控制目標	控制措施群組	控制措施	量測方式	量測結果	監測周期
		A.18.1.2 智慧財產權	檢查是否每半年至少1次更新「資訊安全暨個資保護法令及法規現況一覽表」。		年
		A.18.1.3 紀錄之保護			
		A.18.1.4 個人可識別資訊之隱私及保護			
		A.18.1.5 密碼式控制措施之監管			
	A.18.2 資訊安全審查	A.18.2.1 資訊安全之獨立審查	檢查資訊安全管理審查會議每年至少召開1次。		年
		A.18.2.2 安全政策及標準之遵循性	是否執行內部稽核每年至少1次。		年
		A.18.2.3 技術遵循性審查			

N/A 表本驗證範圍目前無此業務或無法進行量測

檢查人：