Deloitte.

勤業眾信

證券暨期貨市場各服務事業資通系統安全防護基準參考指引說明

Deloitte Risk Advisory、2022/05

Agenda

- 目的 & 總說明
- 條文說明
- 問題與討論

勤業眾信版權所有 保留一切權利

目的 & 總說明

勤業眾信版權所有 保留一切權利

目的 & 總說明

目的
為強化證券商、期貨商及投信投顧業者之資通安全，依據金融監督管理委員會「金融資安行動方案」強化金融業資安防護能力，針對資通系統安全議題，擬定資通系統安全防護基準參考指引。
總說明
本參考指引係參考資通安全管理法、資通安全責任等級分級辦法附表十資通系統防護基準、證券暨期貨市場各服務事業建立內部控制制度處理準則、證券商內部控制制度標準規範、期貨商內部控制制度標準規範、建立證券商資通安全檢查機制、建立期貨商資通安全檢查機制、金融機構資通安全防護基準、行政院資通安全處所公布資通安全管理法常見問題等，經蒐集實務做法併邀集業者共同研議相關參考指引，以強化資通系統安全。 本指引共二十六條，其要點如下： 一、 說明本指引之立法意旨。(第一條) 二、 說明本指引之適用範圍。(第二條) 三、 明定本指引提及之名詞解釋。(第三條) 四、 明定存取控制要求。(第四條至第六條) 五、 明定事件日誌與可歸責性要求。(第七條至第十一條) 六、 明定營運持續計畫要求。(第十二條至第十三條) 七、 明定識別與鑑別要求。(第十四條至第十七條) 八、明定系統與服務獲得要求。(第十八條至二十一條) 九、明定系統與通訊保護要求。(第二十二條) 十、明定系統與資訊完整性要求。(第二十三條至二十六條)

勤業眾信版權所有 保留一切權利

條文說明

勤業眾信版權所有 保留一切權利

概要說明

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引**適用對象**

適用對象		
本指引適用對象包含證券商、期貨商、證券投資信託事業及證券投資顧問事業		
適用對象分類		
第一類	**第二類**	**外資**
（一）「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之組織。 （二）「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級證券商。 （三）「建立期貨商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級期貨商。	非屬第一類範圍之組織。	外資集團在台子公司或分公司，其資安管理政策由外國母公司或總公司控制與建置者，如其母公司或總公司已建置或設立相關控制措施，且有較佳之規範，則從其規範；若無，則應遵循本國法令法規規範。

「證券暨期貨市場各服務事業建立內部控制制度處理準則」第36條之2條文

一、　證券商實收資本額達新臺幣(以下同)一百億元以上或電子下單達一定比率；電子下單一定比率為網際網路下單加計電子式專屬線路下單(Direct Market Access，以下簡稱DMA)成交金額達公司成交金額百分之六十，經紀業務成交金額市占率達全市場百分之二，且自然人客戶數達公司客戶數百分之五十者。

二、　期貨商實收資本額達二十億元以上，且電子下單達一定比率；電子下單一定比率為網際網路下單加計DMA下單成交口數達公司成交口數百分之六十，經紀業務成交口數市占率達全市場百分之二，且自然人客戶數達公司客戶數百分之五十者。

三、　證券投資信託事業及證券投資顧問事業前一年度月平均境內外管理資產規模達六千億元以上者。

註1：參考資料為「證券暨期貨市場各服務事業建立內部控制制度處理準則」第36條之2條文

註2：以下參考指引如無特別說明，皆為第一類及第二類組織應遵循之事項。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引名詞定義

條文	內容
資通系統	係指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
核心系統	係指直接提供客戶交易或支持交易業務持續運作之必要系統（如交易系統、報價系統、中台風控、盤後結算系統、帳務系統等維持交易業務之必要系統），其餘皆為非核心系統。
非客戶帳號	係指非客戶所使用之資通系統帳號（如：提供內部人員、管理者及廠商等所使用之資通系統帳號）。
資訊資產	係指與資訊處理相關之資產，包括硬體、軟體、資料及文件等（如：伺服器主機及使用者電腦之作業系統及應用程式等軟體資訊）。

勤業眾信版權所有 保留一切權利

條文總覽

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第二章 存取控制

條文	內容
第四條(帳號管理)	一、組織應建立資通系統帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 二、組織如有核准臨時或緊急使用之資通系統帳號，於作業結束後，應即時刪除或禁用該等資通系統帳號。 三、組織應禁用資通系統閒置帳號。 四、組織應定期(至少每半年一次)審查資通系統帳號及權限之適切性。 五、第一類組織應定義核心系統之閒置時間或可使用期限與核心系統之使用情況及條件（如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等）。 六、第一類組織核心系統逾越所定之許可閒置時間或可使用期限時，系統宜自動將使用者帳號登出。 七、第一類組織應依組織規定之情況及條件，使用核心系統。 八、提供網際網路下單服務之組織，應每日針對核心系統帳號、非客戶帳號登入嘗試紀錄等進行監控及分析，如發現帳號違常使用時回報管理者並進行後續處理。 九、組織不得使用客戶之顯性資料（如統一編號、身分證號、手機號碼、電子郵件帳號、信用卡號、存款帳號等）作為唯一之識別，否則應另行增設使用者代號以資識別。
第五條(最小權限)	一、資通系統帳號授權應採最小權限原則，僅允許使用者（或代表使用者行為之程序）依組織部門權責及業務功能，完成作業所需之授權存取。 二、組織應定義人員角色及責任並區隔相互衝突的角色。
第六條(遠端存取)	一、組織應訂定遠端連線管理辦法，建立使用限制、組態需求、連線需求及文件化，對於任一允許之遠端存取類型，均應先取得授權，並留存相關紀錄。 二、組織應於伺服器端完成資通系統帳號權限登入驗證作業。 三、組織應監控使用外部網路遠端連線存取組織內部網段之連線。 四、資通系統應採用連線加密機制。 五、資通系統遠端存取之來源應為組織已核准之存取控制點。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第三章 事件日誌與可歸責性(1/2)

條文	內容
第七條(記錄事件)	一、組織應訂定資通系統電腦稽核紀錄（日誌）之記錄時間週期及保存政策，並至少保存三年。 二、資通系統應確有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、資通系統應記錄管理者帳號所執行之各項功能，且應於核心系統最高權限帳號、特殊功能(如程式或軟體異動、參數或組態變更權限等)權限帳號被使用時，每日覆核使用結果。 四、組織應定期審查核心系統產生之電腦稽核紀錄（日誌），非核心系統宜定期審查。
第八條(電腦稽核紀錄（日誌）記錄內容與容量)	一、資通系統產生之電腦稽核紀錄（日誌）應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，宜採用單一日誌機制，確保輸出格式之一致性，並應依組織所訂之資通安全政策及相關法令要求及組織業務需求納入其他相關資訊。 二、資通系統應依據電腦稽核紀錄（日誌）儲存需求，配置所需之儲存容量。
第九條(電腦稽核紀錄（日誌）處理失效之回應)	一、組織於資通系統電腦稽核紀錄（日誌）處理失效時，應採取適當之行動。 二、第一類組織之核心系統規定需要即時通報之電腦稽核紀錄（日誌）處理失效事件發生時，核心系統宜於組織規定之時效內，對特定人員提出警告。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第三章 事件日誌與可歸責性(2/2)

條文	內容
第十條(時戳及校時)	一、資通系統應使用系統內部時鐘產生電腦稽核紀錄（日誌）所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 二、資通系統內部時鐘應定期與基準時間源進行同步。
第十一條(電腦稽核紀錄（日誌）資訊之保護)	一、對電腦稽核紀錄（日誌）之存取管理，僅限於有權限之使用者。 二、核心系統應運用雜湊或其他適當方式之完整性確保機制，非核心系統宜有完整性確保機制。 三、第一類組織之核心系統應定期備份電腦稽核紀錄（日誌）至原系統外之其他實體系統。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第四章 營運持續計畫

條文	內容
第十二條(系統備份)	一、組織應訂定資通系統可容忍資料損失之時間要求。 二、組織應執行資通系統程式原始碼與資料備份。 三、組織應定期測試資通系統備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 四、第一類組織之核心系統應將備份還原，作為營運持續計畫測試之一部分。 五、第一類組織之核心系統應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。
第十三條(系統備援)	一、組織應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。 二、資通系統原服務中斷時，組織應於可容忍時間內，由備援設備或其他方式取代並提供服務。 三、組織應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第五章 識別與鑑別

條文	內容
第十四條(內部使用者之識別與鑑別)	一、資通系統應具備唯一識別及鑑別組織內部使用者(或代表組織使用者行為之程序)之功能，禁止使用共用帳號。 二、透過網際網路使用管理帳號登入核心系統時，應採用多因子認證機制，第一類組織之核心系統對內部使用者存取宜採取多因子認證機制。
第十五條(身分驗證管理)	一、使用者使用預設密碼登入資通系統時，應於登入後要求立即變更預設密碼後方可繼續作業。 二、資通系統身分驗證相關資訊不以明文傳輸。 三、資通系統具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用組織自建之失敗驗證機制。屬電子式交易者，密碼輸入錯誤次數達三次者，應記錄登入失敗事件、鎖定該登入帳號並中斷連線；受理解除鎖定之申請時，應確實辨認身分，並留存相關紀錄後，始得解除鎖定。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、上開兩項所定措施，對非內部使用者，可依組織自行規範辦理。 七、核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。 八、核心系統密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記（如：網站連結或一次性密碼One-time password,OTP，至使用者登記之電子信箱或手機）或其他驗證身分方式，非核心系統密碼重設後宜有驗證身分方式。
第十六條(鑑別資訊回饋與加密模組識別)	一、組織應遮蔽資通系統鑑別過程中之資訊。 二、組織如以密碼進行資通系統鑑別時，該密碼應加密或經雜湊處理後儲存。
第十七條(非內部使用者之識別與鑑別)	資通系統應識別及鑑別非組織使用者（或代表組織使用者行為之程序）。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第六章 系統與服務獲得

條文	內容
第十八條(系統發展生命週期需求分析與設計階段)	一、組織於系統需求分析階段，應針對資通系統安全需求（含機密性、可用性、完整性）進行確認。 二、組織應根據核心系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估，非核心系統宜進行威脅識別、風險分析及評估。 三、組織應將核心系統風險評估結果回饋需求階段之檢核項目，並提出安全需求修正，非核心系統宜依風險評估結果修正安全需求。
第十九條(系統發展生命週期開發與測試階段)	一、資通系統應針對安全需求實作必要控制措施。 二、資通系統應注意避免軟體常見漏洞及實作必要控制措施。 三、資通系統發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 四、提供網際網路下單服務之組織，核心系統宜執行「源碼掃描」安全檢測。 五、第一類組織之核心系統宜具備發生嚴重錯誤時之通知機制。 六、提供網際網路下單服務之組織，應定期（至少每半年乙次）辦理資通系統「弱點掃描」安全檢測。 七、提供網際網路下單服務之組織，應定期對提供網際網路服務之核心系統辦理「滲透測試」安全檢測。
第二十條(系統發展生命週期部署、維運與委外階段)	一、組織於部署環境中應針對資通系統相關安全威脅與漏洞，進行更新與修補，並關閉不必要服務及埠口。 二、組織應檢視現有之資通系統，應設定使用優質密碼，且應避免使用預設密碼。 三、組織於資通系統發展生命週期之維運階段，應執行版本控制與變更管理。 四、組織如委外辦理資通系統開發，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、可用性、完整性）納入委外契約
第二十一條(獲得程序與系統文件)	一、資通系統正式作業環境應與開發、測試作業環境區隔。 二、組織應儲存與管理資通系統發展生命週期之相關文件。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第七章 系統與通訊保護

條文	內容
第二十二條(傳輸之機密性、完整性與資料儲存安全)	一、透過網際網路傳輸個人或機敏資料，核心系統應採用加密傳輸機制，以防止未授權之資訊揭露或偵測資訊之變更。 二、第一類組織於內部網路傳輸個人或機敏資料，核心系統宜採加密傳輸機制。 三、上開兩項，傳輸過程中如有替代之實體保護措施者，則無需採加密傳輸機制。 四、如有國際傳輸機敏資料，組織應建立加密傳輸機制且應就受委託機構（外資組織因內部分工將資訊委外至總公司、國外分支機構境外處理者）對客戶資訊之蒐集、處理、利用、國際傳輸及控管情形確認符合我國個人資料保護法相關規定，傳輸前應取得當事人授權且不違反主管機關對國際傳輸之限制，並留存完整稽核紀錄。 五、加密機制應使用公開、國際機構驗證且未遭破解之演算法。 六、加密機制之金鑰或憑證應定期更換。 七、加密機制宜支援演算法最大長度金鑰。 八、加密機制於伺服器端之金鑰保管宜訂定管理規範及實施應有之安全防護措施。 九、第一類組織之核心系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。 十、加解密程式或具變更權限之公用程式（如資料庫工具程式）應列管並限制使用，防止未經授權存取並保留稽核軌跡。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第八章 系統與資訊完整性(1/2)

條文	內容
第二十三條(漏洞修復)	一、組織對於資通系統之漏洞檢測應以全部資訊資產為原則，漏洞修復應測試有效性及潛在影響，並定期更新。 二、組織應定期確認資通系統相關漏洞修復之狀態，應針對所發現漏洞之風險高低及是否對外提供服務，設定修補期限，未修補前應加強防護及異常偵測，以確保弱點管理之即時性及有效性。
第二十四條(資通系統監控)	一、如發現資通系統有被入侵跡象時，應通報組織特定人員。 二、組織應監控核心系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用，非核心系統宜進行監控。 三、核心系統宜採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。
第二十五條(軟體及資訊完整性)	一、核心系統應使用完整性驗證工具，以偵測未授權變更特定軟體及資訊，非核心系統宜使用完整性驗證工具。 二、核心系統使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、資通系統發現於違反完整性時，應實施組織指定之安全保護措施。 四、第一類組織之核心系統宜定期執行軟體與資訊完整性檢查。

勤業眾信版權所有 保留一切權利

資通系統安全防護基準參考指引-第八章 系統與資訊完整性(2/2)

條文	內容
第二十六條(個人資料保護)	一、為維護所保有個人資料之安全，應採取下列資料安全管理措施： （一）訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。 （二）針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。 （三）作業過程有備份個人資料之需要時，對備份資料予以適當保護。 二、保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施： （一）實施適宜之存取管制。 （二）訂定妥善保管媒介物之方式。 （三）依媒介物之特性及其環境，建置適當之保護設備或技術。 三、為維護所保有個人資料之安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。 四、應針對核心系統及各類電腦系統確認所保有之個人資料進行風險評估及控管。 五、應針對核心系統及各類電腦系統建置留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。 六、應建立資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案等方式傳輸，並應留存相關紀錄、軌跡及證據。 七、如刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： （一）刪除、停止處理或利用之方法、時間。 （二）將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

勤業眾信版權所有 保留一切權利

條文內容說明

勤業眾信版權所有 保留一切權利

存取控制

第四條(帳號管理)

一、組織應建立資通系統帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。

佐證資料

- 組織訂定之資通系統帳號管理規範
- 資通系統帳號申請異動單(如帳號權限申請表、使用者帳號異動申請單等)
- 系統線上帳號權限申請或異動紀錄

內容說明

- 須建立資通系統帳號管理機制，以適切管理資通系統使用者帳號、後臺主機作業系統帳號及資料庫管理者帳號等。
- 除對外服務系統可能因使用需求，讓非組織內部使用者(如一般民眾等)自行建立使用外，組織內部使用者使用資通系統應符合組織訂定之帳號管理程序，包含帳號之申請、建立、修改、啟用、停用及刪除等作業規範並落實執行。
- 除因緊急需求外，原則上所有帳號異動不可由系統管理者任意調整異動，宜由相關權責人員提出異動申請，並通過審核程序後始可進行異動作業。而帳號異動流程，一般可透過紙本或電子化系統完成，填寫相關表單(如系統帳號/權限異動申請單等)。

勤業眾信版權所有 保留一切權利

第四條(帳號管理)

二、組織如有核准臨時或緊急使用之資通系統帳號，於作業結束後，應即時刪除或禁用該等資通系統帳號。

系統帳號/權限異動申請單

紀錄編號	
申請組別/申請人	
申請日期	
申請期限	◉有期限 ○無期限 2021/12/31 18:00 日期與時間
申請類別	○新進人員 ○離職 ○組別異動 ◉業務需求 ○其他
備註	緊急業務使用

內容說明

- 基於實際作業需要，得建立短期性與臨時性使用者帳號，如為提供廠商或安全測試人員短期使用、代理工作的需要或因應突發情況而須迅速建立並啟用帳號，惟使用完畢後應盡速取消其使用權限。
- 應定義臨時帳號與緊急帳號之使用期限，如資通系統允許使用者申請臨時帳號，使用效期30天，或者由系統管理者開立緊急帳號並設定使用截止日期。
- 應具備帳號檢查機制，將逾期之臨時或緊急帳號刪除或禁用，例如可人工定期進行帳號清查，或於資通系統實作自動管理逾時帳號之功能，如系統自動刪除自建立日起已達30天之臨時帳號。

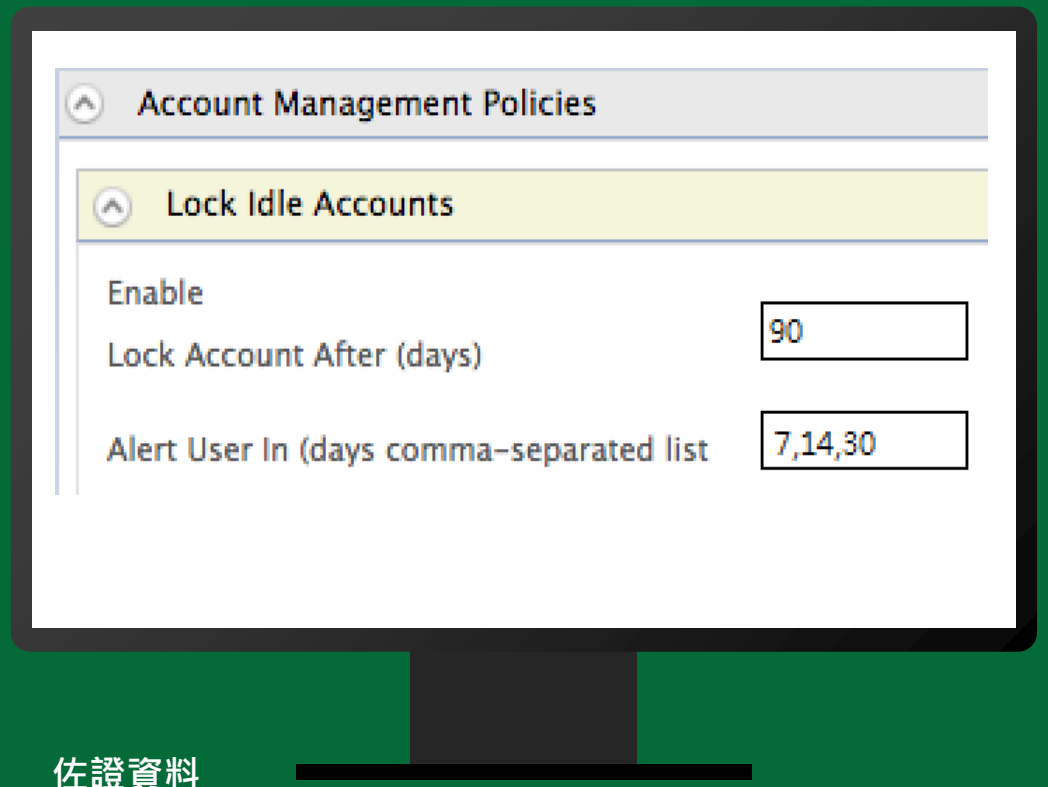
佐證資料

- 組織訂定之**資通系統帳號管理程序**
- 資通系統**帳號申請異動單**
- 資通系統**帳號管理功能之測試紀錄**
- 資通系統**帳號清查紀錄**

勤業眾信版權所有 保留一切權利

存取控制

第四條(帳號管理)
三、組織應禁用資通系統閒置帳號。



佐證資料

- 組織訂定之資通系統帳號管理程序
- 資通系統帳號申請異動單
- 資通系統帳號管理功能之測試紀錄
- 資通系統帳號清查紀錄

內容說明

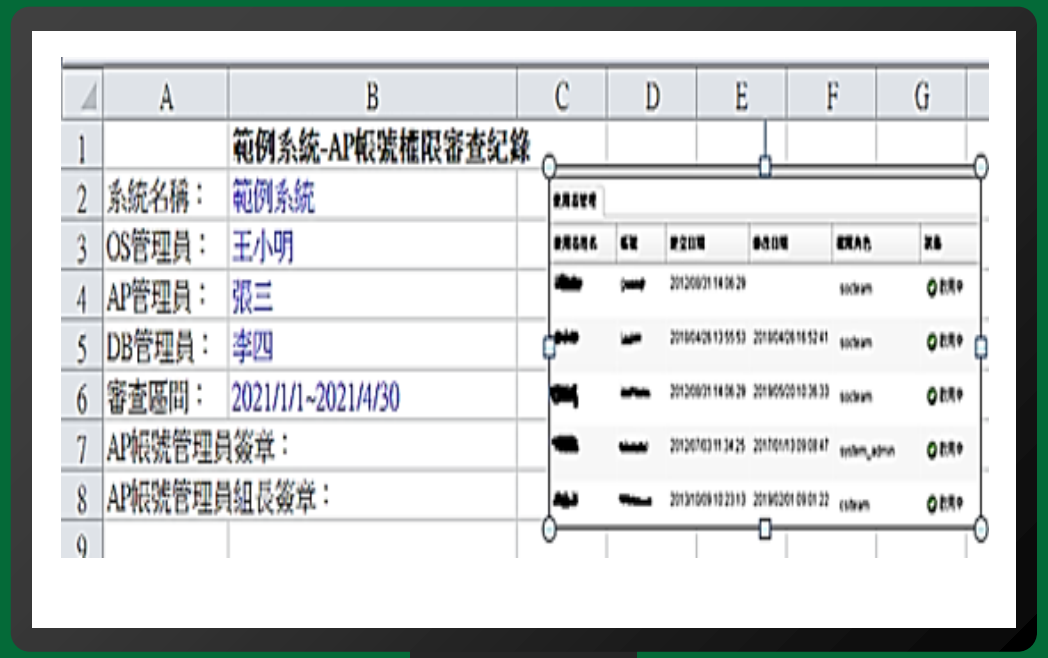
- 閒置帳號係指久未登入(如90天等)使用系統服務的帳號，常見原因如未移除已調、離(退)職人員之帳號權限等。
- 應具備帳號檢查機制，將閒置帳號禁用，拒絕其登入行為，使用者需申請重新啟用後始可登入。常見作法為在發現帳號接近逾期前(如7天等)，先向使用者寄發警示信件，以提醒使用者進行登入動作。
- 惟實務上仍可針對不同類型之資通系統與帳號，個別評估其使用需求與資安風險，定義其帳號之閒置期限。組織可定期以人工完成帳號審查作業，或是評估於系統上實作相關功能，如依組織設定之期限自動禁用逾期之閒置帳號。

勤業眾信版權所有 保留一切權利

存取控制

第四條(帳號管理)

四、組織應定期(至少每半年一次)審查資通系統帳號及權限之適切性。



	A	B	C	D	E	F	G
1		範例系統-AP帳號權限審查紀錄					
2	系統名稱：	範例系統					
3	OS管理員：	王小明					
4	AP管理員：	張三					
5	DB管理員：	李四					
6	審查區間：	2021/1/1~2021/4/30					
7	AP帳號管理員簽章：						
8	AP帳號管理員組長簽章：						
9							

內容說明

- 應定期(至少每半年一次)透過系統帳號清查活動，以審核帳號之申請、建立、修改、啟用、停用及刪除等相關紀錄，以發現未經授權的帳號變更行為。
- 帳號審核範圍，宜包含系統管理者帳號、後臺主機作業系統帳號及資料庫管理者帳號等，亦可評估實際執行需求，納入組織內部及外部一般使用者帳號，並應依組織規定清查應禁用或刪除之帳號，如臨時帳號、緊急帳號及閒置帳號等。

佐證資料

- 組織訂定之資通系統帳號管理程序
- 資通系統帳號申請異動單
- 資通系統帳號清查紀錄

勤業眾信版權所有 保留一切權利

存取控制

五、第一類組織應定義核心系統之閒置時間或可使用期限與核心系統之使用情況及條件（如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等）。

```
<configuration>
    <system.web>
        <sessionState  mode="InProc" cookieless="true" timeout="20" />
    </system.web>
</configuration>
```

佐證資料

- 組織訂定之資通系統發展維護辦法
- 資通系統功能規格書
- 資通系統應用程式原始碼或組態設定檔等與會談相關之設定值

內容說明

- 閒置時間係指使用者久未操作系統之閒置行為，當閒置過久，可能是使用者已離開系統操作環境卻未自行登出帳號，此時容易造成帳號被他人惡意盜用的風險；可使用期限如每次登入帳號後能進行系統操作時間限制(如1小時等)或時段限制(如18:00前等)。資通系統之使用情況及條件係指資通系統帳號的使用限制，如帳號類型與功能限制、操作時段限制、來源位址、連線數量及存取資源等。

- 實務上因各資通系統使用需求之差異，系統管理者可設定不同的閒置時間或可使用期間，並限制各種使用情況及條件以確保安全性。這些條件限制，可能描述於組織相關管理規範內，亦可能是未明文規定的使用慣例要求，惟系統管理者及相關權責人員應熟知這些使用限制，並應確保資通系統已啟用相關設定，例如會談(Session)機制常被利用來管理使用者與伺服器之間的連線狀態，多數開發框架皆會內建會談管理功能，並設定使用者操作的閒置期限。以.NET開發框架為例，設定會談逾期時間預設值為20分鐘，當使用者操作閒置達20分鐘時即自動登出。

勤業眾信版權所有 保留一切權利

存取控制

第四條(帳號管理)

六、第一類組織核心系統逾越所定之許可閒置時間或可使用期限時，系統宜自動將使用者帳號登出。

內容說明

- 將系統設定為組織所定義的操作閒置期限以自動登出帳號，可減少帳戶被盜用的風險。建議使用開發框架內建的會談管理機制，通常已經過嚴謹的測試，不僅方便使用，亦能提供足夠的安全保護。
- 若由開發人員自行設計帳號登出機制，應確保進行帳號登出時已確實將會談資料作廢。一種常見的系統設計缺失是在逾期後僅將操作頁面導向登入畫面，卻仍然繼續留存著舊有的會談資料，此時惡意使用者可能會利用瀏覽器網頁瀏覽紀錄或「回上一頁」功能，取得原始的帳號登入狀態。

佐證資料

- 組織訂定之資通系統發展維護辦法
- 資通系統功能規格書
- 資通系統應用程式原始碼或組態設定檔等與會談相關之設定值
- 資通系統閒置自動登出功能之測試紀錄

勤業眾信版權所有 保留一切權利

存取控制

第四條(帳號管理)

七、第一類組織應依組織規定之情況及條件，使用核心系統。

```
<Context privileged="true">
        <Valve className="org.apache.catalina.valves.RemoteAddrValve"
               allow="127\.0\.0\.1"/>
</Context>
```

內容說明

- 為強化資通系統安全性，系統管理者可限制各種不同使用情況及條件，使用者應符合所規定之使用規範。
- 舉例說明：組織內部系統僅允許組織同仁利用AD目錄服務帳號登入，並限制帳號來源IP位址: 10.0.2.1~10.0.2.250，而資通系統後臺僅限管理者帳號利用本機位址(127.0.0.1)存取管理頁面，禁止從遠端登入管理者帳號。以Apache Tomcat 9為例，可透過組態設定檔案manager.xml內新增RemoteAddrValve參數，允許或拒絕特定來源位址的連線，僅開放本機存取之設定範例。

佐證資料

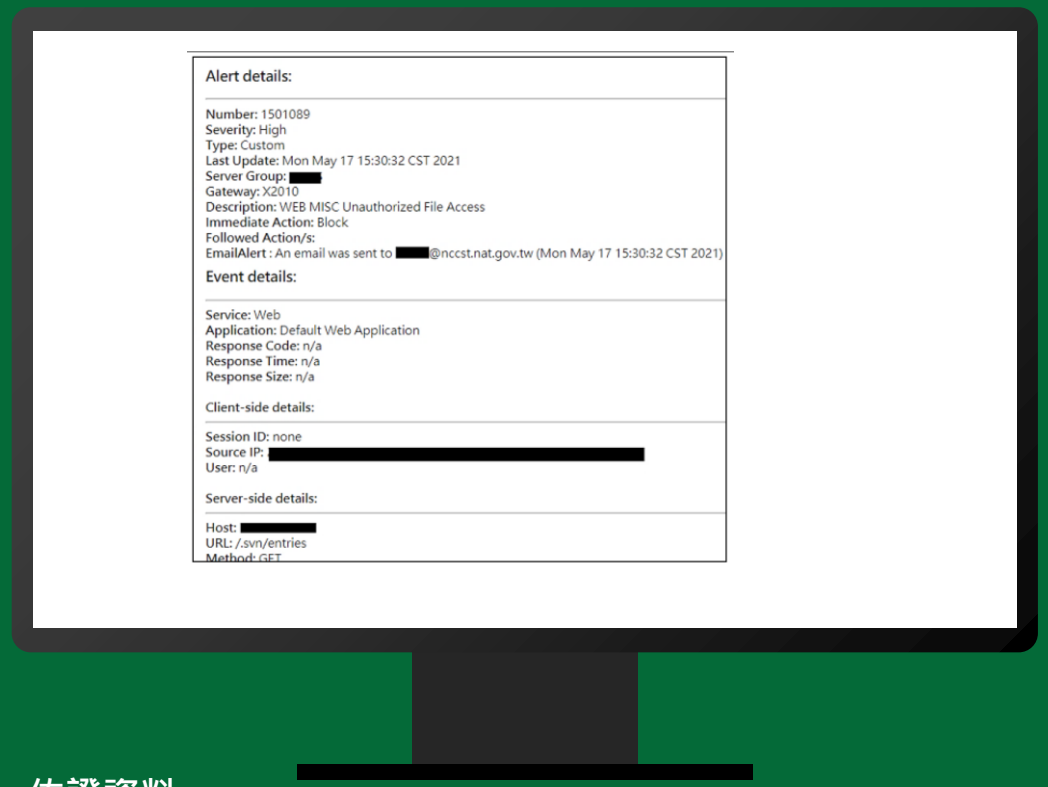
- 組織訂定之資通系統發展維護辦法
- 資通系統帳號清查紀錄
- 系統日誌

勤業眾信版權所有 保留一切權利

第四條(帳號管理)

存取控制

八、提供網際網路下單服務之組織，應每日針對核心系統帳號、非客戶帳號登入嘗試紀錄等進行監控及分析，如發現帳號違常使用時回報管理者並進行後續處理。



Alert details:

Number: 1501089
Severity: High
Type: Custom
Last Update: Mon May 17 15:30:32 CST 2021
Server Group: [redacted]
Gateway: X2010
Description: WEB MISC Unauthorized File Access
Immediate Action: Block
Followed Action/s:
EmailAlert : An email was sent to [redacted]@nccst.nat.gov.tw (Mon May 17 15:30:32 CST 2021)

Event details:

Service: Web
Application: Default Web Application
Response Code: n/a
Response Time: n/a
Response Size: n/a

Client-side details:

Session ID: none
Source IP: [redacted]
User: n/a

Server-side details:

Host: [redacted]
URL: /.svn/entries
Method: GET

內容說明

- 帳號違常使用係指與使用者日常工作使用模式不相符之行為，例如於異常時間登入資通系統、於非業務期間存取重要系統服務、存取機敏資料出現不正常的瀏覽流量，或是頻繁觸發帳號身分驗證失敗等情況。
- 資通系統帳號之監控，如部署各式資安監控防護產品，包含但不限於安全資訊事件管理(Security Information and Event Management, SIEM)、入侵偵測系統(Intrusion Detection System, IDS)、入侵預防系統(Intrusion Prevention System, IPS)、網站應用程式防火牆(Web Application Firewall, WAF)、身分識別與存取管理(Identity and Access Management, IAM)以及特權帳號管理(Privileged Account Manager, PAM)等，亦可評估導入SOC服務，或於資通系統設計異常警示功能，如實作系統例外處理(Exception Handling)機制，當發生帳號疑似惡意破解、越權存取及違規使用行為時提出警告。
- 向管理者回報方式，如人工回報、於系統操作頁面顯示警告畫面，以及寄送警示信件或簡訊等各種通知方式。

佐證資料

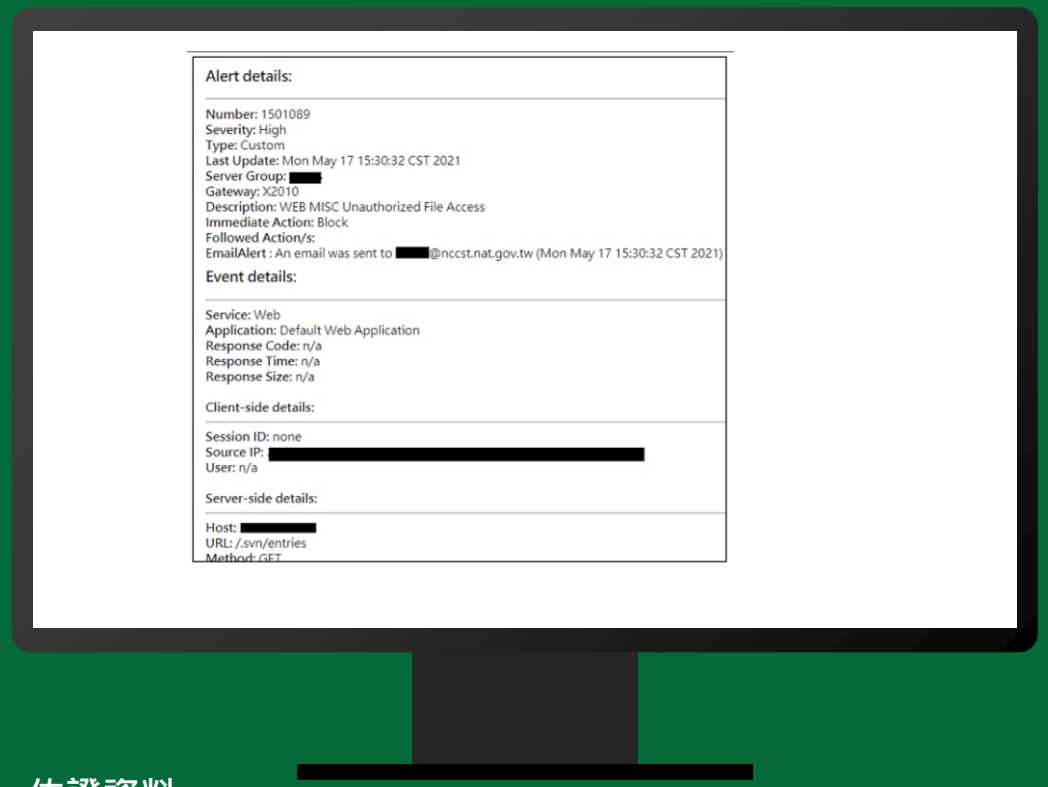
- 組織訂定之資通系統發展維護辦法
- 監控防護相關紀錄，如SOC維運紀錄、WAF日誌等
- 資通系統日誌(logs)

勤業眾信版權所有 保留一切權利

第四條(帳號管理)

存取控制

九、組織不得使用客戶之顯性資料（如統一編號、身分證號、手機號碼、電子郵件帳號、信用卡號、存款帳號等）作為唯一之識別，否則應另行增設使用者代號以資識別。



Alert details:

Number: 1501089
Severity: High
Type: Custom
Last Update: Mon May 17 15:30:32 CST 2021
Server Group: [redacted]
Gateway: X2010
Description: WEB MISC Unauthorized File Access
Immediate Action: Block
Followed Action/s:
EmailAlert : An email was sent to [redacted]@nccst.nat.gov.tw (Mon May 17 15:30:32 CST 2021)

Event details:

Service: Web
Application: Default Web Application
Response Code: n/a
Response Time: n/a
Response Size: n/a

Client-side details:

Session ID: none
Source IP: [redacted]
User: n/a

Server-side details:

Host: [redacted]
URL: /.svn/entries
Method: GET

內容說明

- 當使用者登入應進行身分確認，得以帳號及固定密碼登入。
- 帳號如使用顯性資料（如商業統一編號、身分證統一編號、行動電話號碼、電子郵件帳號、信用卡卡號、存款帳號等）作為唯一之識別，應另行增設使用者代號以資識別。使用者代號亦不得為上述顯性資料。

佐證資料

- 組織訂定之資通系統發展維護辦法
- 資通系統功能規格書

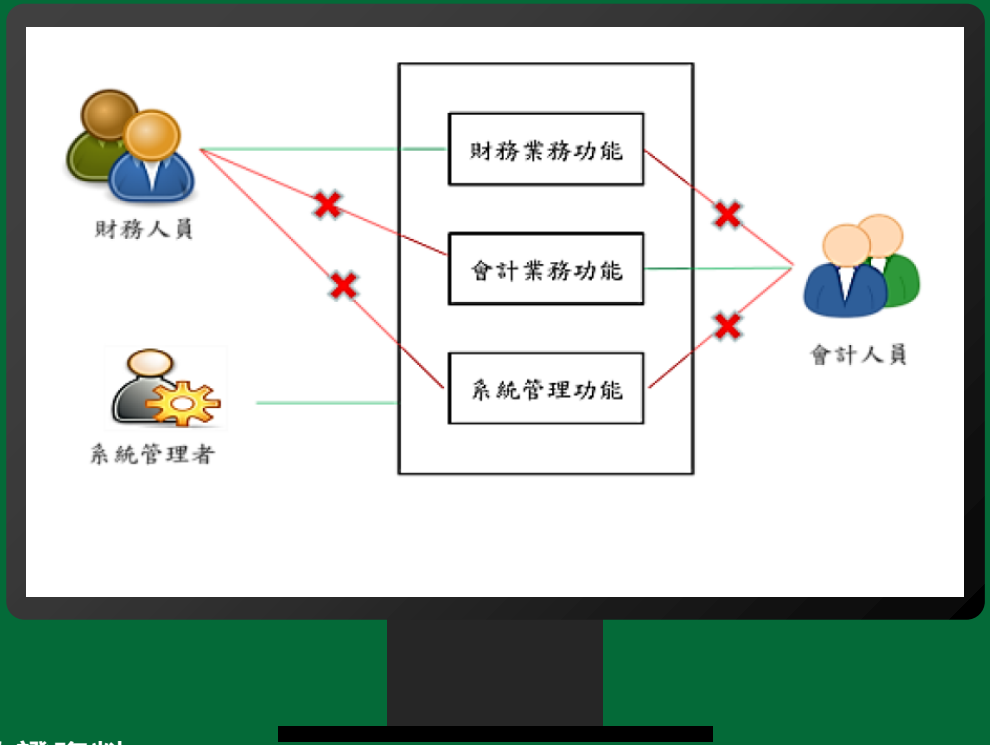
勤業眾信版權所有 保留一切權利

存取控制

第五條(最小權限)

一、資通系統帳號授權應採最小權限原則，僅允許使用者（或代表使用者行為之程序）依組織部門權責及業務功能，完成作業所需之授權存取。

二、組織應定義人員角色及責任並區隔相互衝突的角色。



內容說明

- 應依資通系統使用需求，賦予各級人員必要之系統存取權限。組織員工之系統存取權限，應以執行法定任務所必要者為限，例如不同業務單位因使用需求差異，所賦予的資通系統存取權限亦會有所區別，應針對使用者及角色，僅賦予所需要的最低權限。軟體程序(process)及伺服器服務之執行權限，亦應符合最小權限原則，例如以一般使用者權限啟動執行，儘量避免使用系統管理者或最高權限。
- 配發系統最高管理權限之人員及掌理重要技術與作業控制之特定人員帳號時，應經過審慎之評估與限制，防範非業務必要所需之組織人員與非組織使用者執行特權功能，如創建帳號、管理加密金鑰或變更系統重要組態設定等。組織亦可透過定期帳號權限清查，審核帳號使用者與其權限是否符合其業務所需之最小權限。
- 資通系統應具備存取控制安全機制，採用最小權限之設計原則，組織可以考慮增設程序、使用者角色及系統帳號，並透過服務組態參數與存取控制列表等方式設定授權存取以實現最小權限。最小權限原則設計示意圖。
- 市面上亦發展多種帳號管理解決方案，可協助管理一般使用者與特權使用者帳號並控制其存取權限，如身分識別與存取管理(Identity and Access Management, IAM)與特權帳號管理(Privileged Account Manager, PAM)等。這些解決方案可快速建立一致性的存取控制政策、部署存取規則及提供儀錶板操作檢視等，依產品類型不同，管理範圍包含系統、網路與主機的單一登入、使用者資料管理與認證及目錄服務(AD)等。

佐證資料

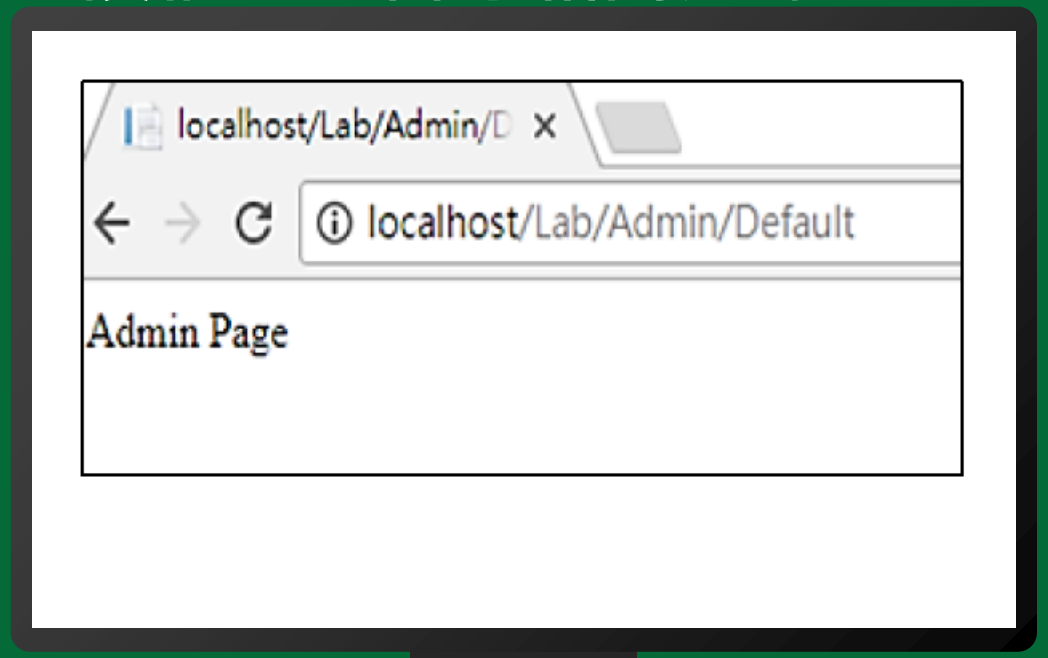
- 組織訂定之資通系統發展維護辦法
- 資通系統存取控制功能之測試紀錄

勤業眾信版權所有 保留一切權利

存取控制

第六條(遠端存取)

一、組織應訂定遠端連線管理辦法，建立使用限制、組態需求、連線需求及文件化，對於任一允許之遠端存取類型，均應先取得授權，並留存相關紀錄。



內容說明

- 遠端存取係指使用者(或代表使用者行為程序)透過非本地端網路(如網際網路等)通信存取組織資通系統之連線行為，常用網路協定包含但不限於HTTP(S)、SSH、遠端桌面(RDP)及VPN等。
- 應控管資通系統所有允許的遠端連線行為，其中包含對於應用程式及作業系統資源的存取控制，應通過授權檢查後始可放行。例如，組織官方網站常會公開授權所有民眾存取，惟進階操作或後台管理功能，則只開放給具有相應權限之使用者帳號使用，須完成身分驗證及授權檢查後，始可存取相關功能資源。為有效進行存取控制，資通系統應建立相關使用限制、組態需求及連線需求，其中包含使用者身分類型、來源位址、連線人數上限、網路連線類型、開放時段、允許存取的功能資源及任何先備條件等限制。
- 使用情境如資通系統為因應遠距辦公之需求而開放VPN連線存取，但限制使用者須為組織同仁透過AD帳號登入，並使用組織配發之OA電腦，檢測已安裝及更新防毒軟體後始可連線，連線後僅允許存取特定系統功能。
- 將資通系統存取控制資訊文件化，有助於日常維運遵循與日後稽核查檢作業，如可將相關使用規範描述於資通系統開發維護文件或是統一規範於組織相關管理辦法。

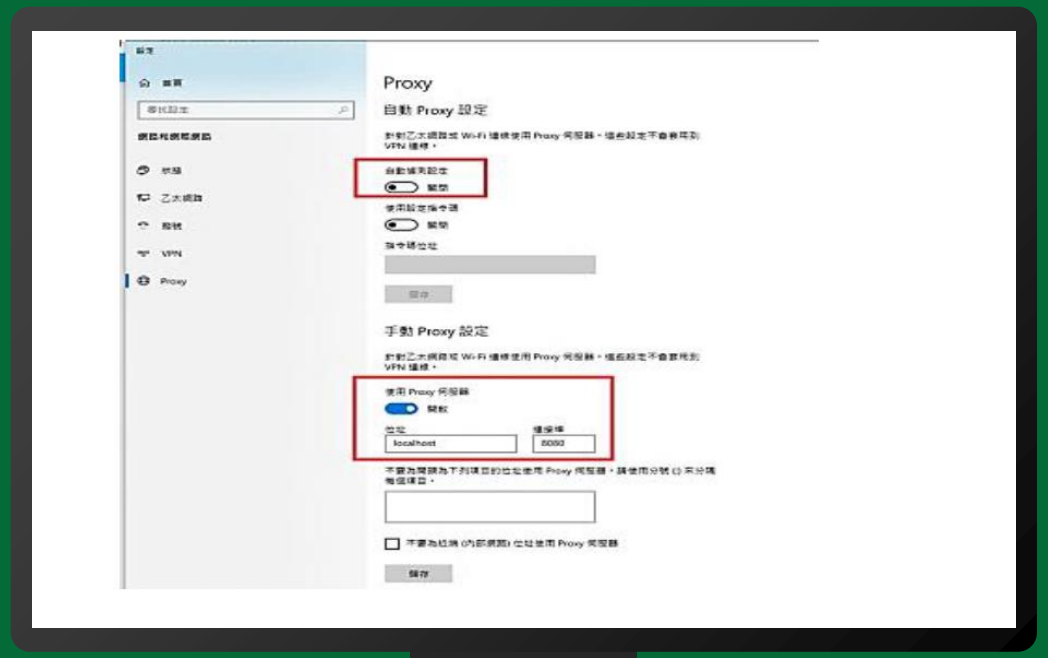
佐證資料

- 組織訂定之網路管理規範
- 防火牆規則、存取控制列表(ACL)
- 資通系統存取控制功能之測試紀錄
- 系統連線日誌

勤業眾信版權所有 保留一切權利

存取控制

第六條(遠端存取)
二、組織應於伺服器端完成資通系統帳號權限登入驗證作業。



內容說明

- 資通系統應檢查使用者存取權限，禁止未經系統授權存取行為；惟若系統將權限檢查作業實作於使用者端(如JavaScript、Mobile App等)則可視為無效，因其可能被惡意使用者利用竄改網站Cookies內容或網路封包內容等手法繞過檢查機制，故資通系統應於伺服器端實作授權檢查。

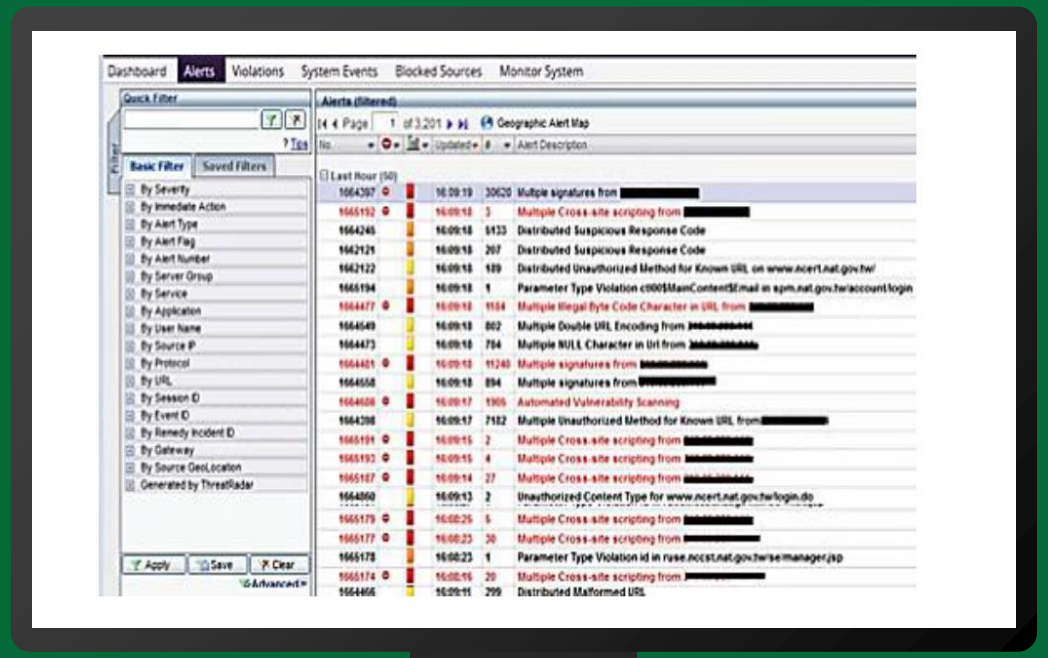
佐證資料
- 組織訂定之網路管理規範
- 資通系統存取控制功能測試紀錄

勤業眾信版權所有 保留一切權利

存取控制

第六條(遠端存取)

三、組織應監控使用外部網路遠端連線存取組織內部網段之連線。



內容說明

- 組織可能因使用需求，而允許組織內部使用者(如外點單位、居家辦公等)或廠商自遠端來源存取組織內部網段或資通系統後台，以進行系統管理維護作業。實務上常透過VPN建立安全通道，以保護連線過程的機密性與完整性，惟此種遠端連線行為因具備高度資安風險，很可能被惡意攻擊者利用作為系統入侵管道，故組織宜使用網路安全監控設備(如Firewall、WAF及IPS/IDS等)或服務(如SOC監控等)，監控遠端存取組織內部網段或資通系統後臺之連線，以及時發現異常連線或惡意攻擊行為。

佐證資料

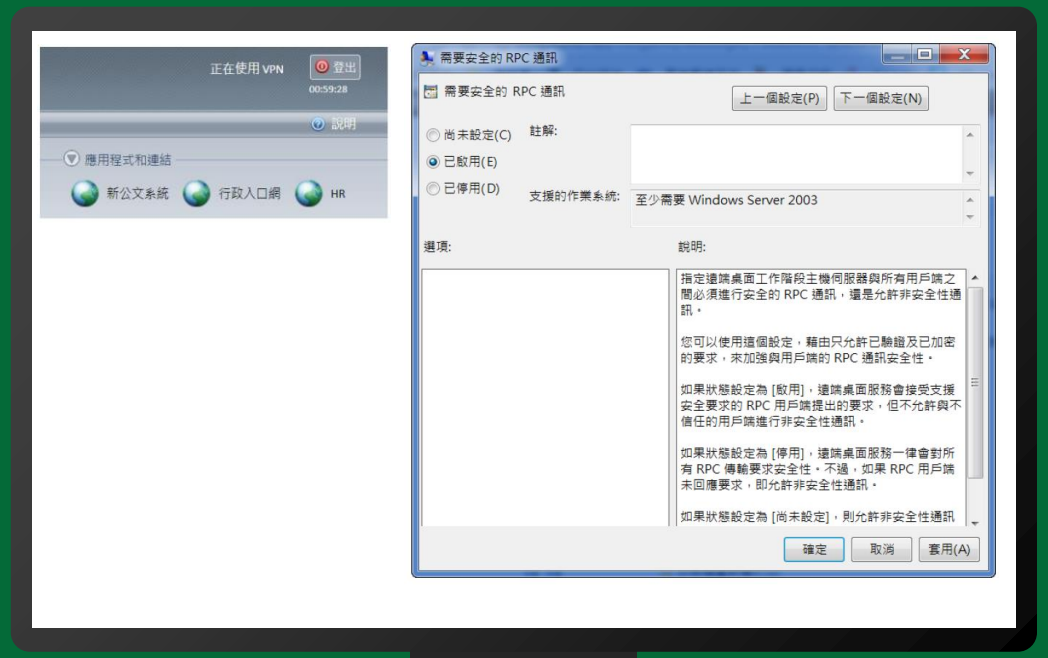
- 組織訂定之系統監控程序
- 系統監控紀錄

勤業眾信版權所有 保留一切權利

第六條(遠端存取)

四、資通系統應採用連線加密機制。

存取控制



佐證資料

- 組織訂定之網路管理規範
- 資通系統加密連線之測試紀錄

內容說明

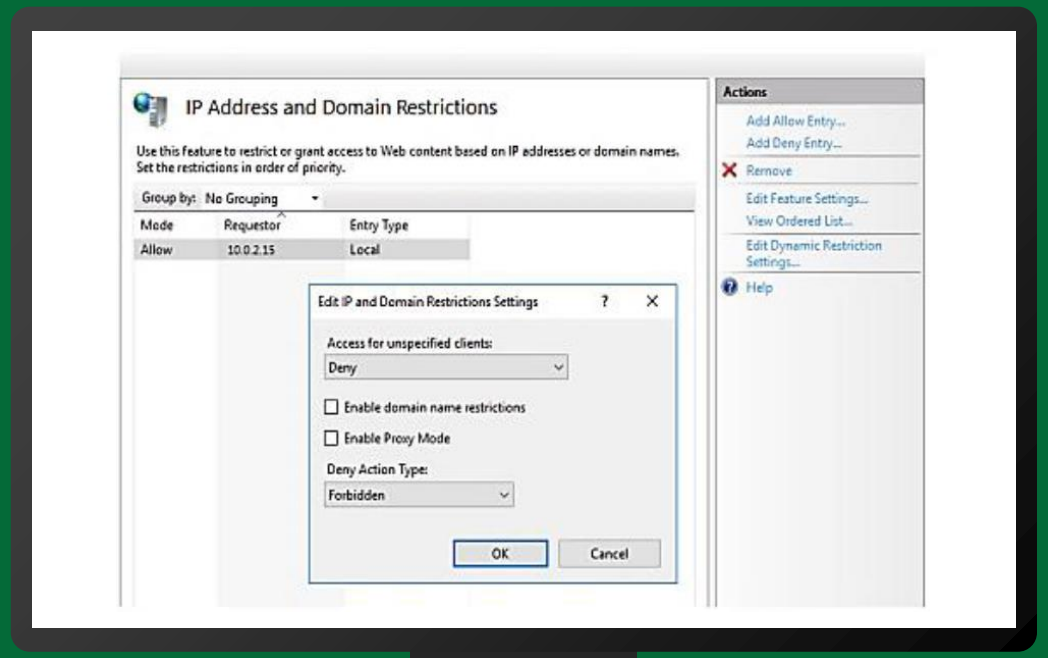
- 為保護遠端存取連線的機密性與完整性，資通系統應採用加密機制以建立安全通道，最常見應用如啟用HTTPS TLS 1.2加密傳輸協定等。
- 實務上組織可能因居家辦公等使用需求，而允許同仁或系統維護人員遠端存取內部網段之服務或資通系統後臺，此時常會建立VPN安全通道，並可限制遠端來源以降低存取風險，VPN遠端存取資通系統服務。
- 如資通系統允許管理人員透過遠端桌面服務登入伺服器進行維護操作，為降低被駭客利用遠端桌面服務入侵的機率，亦應強化伺服器本機資安防護設定，啟用加密連線機制。如參照政府組態基準之建議，於Windows Server環境啟用「需要安全的RPC通訊」組態設定，RPC介面是用於管理及設定遠端桌面服務，啟用安全的RPC通訊後，遠端桌面服務只會接受支援安全要求的RPC用戶端提出要求，禁止與未受信任用戶端進行非安全性通訊，以此加強與用戶端遠端桌面服務連線安全性。

勤業眾信版權所有 保留一切權利

第六條(遠端存取)

五、資通系統遠端存取之來源應為組織已核准之存取控制點。

存取控制



內容說明

- 遠端存取行為應通過授權後始可放行，若有必要允許外部遠端存取之系統功能時，應限制遠端存取控制點以降低遭受攻擊機會，如識別來源主機、來源端IP位址、目的端IP位址、埠口及通訊協定等連線限制，避免全面性開放存取。
- 以Winows IIS伺服器為例，可利用「IP Address and Domain Restrictions」功能，設定來源網址的黑(白)名單

佐證資料

- 組織訂定之網路管理規範
- 組織部署之防火牆規則、ACL
- 資通系統存取控制功能測試紀錄
- 系統連線日誌

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第七條(記錄事件)

一、組織應訂定資通系統電腦稽核紀錄（日誌）之記錄時間週期及保存政策，並至少保存三年。

(一)作業系統及應用系統之日誌(帳號登入、帳號登出、存取成功、存取失敗、管理者行為、系統組態變更等資訊）至少需留存六個月，並應視其重要性進行必要備份及保護，避免竄改及未經授權之存取。

內容說明

- 應訂定相關管理辦法以妥善留存資通系統日誌，包含但不限於資通系統伺服器日誌、資料庫日誌檔案及伺服器作業系統日誌等，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。資通系統日誌留存期限應至少保留三年。

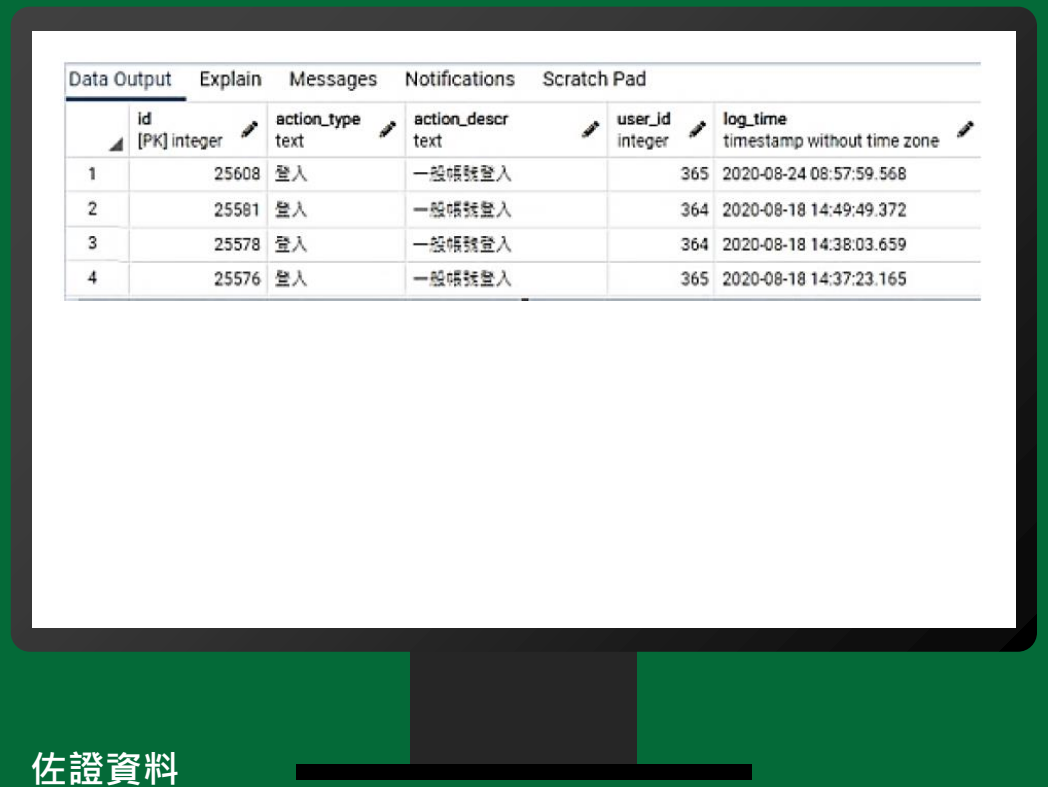
佐證資料

- 組織訂定之日誌相關管理辦法
- 資通系統日誌

勤業眾信版權所有 保留一切權利

第七條(記錄事件)

二、資通系統應確有記錄特定事件之功能，並決定應記錄之特定資通系統事件。



Data Output | Explain | Messages | Notifications | Scratch Pad

	id [PK] integer	action_type text	action_descr text	user_id integer	log_time timestamp without time zone
1	25608	登入	一般帳號登入	365	2020-08-24 08:57:59.568
2	25581	登入	一般帳號登入	364	2020-08-18 14:49:49.372
3	25578	登入	一般帳號登入	364	2020-08-18 14:38:03.659
4	25576	登入	一般帳號登入	365	2020-08-18 14:37:23.165

佐證資料

- 組織訂定之日誌相關管理辦法
- 資通系統日誌

內容說明

- 資通系統事件係指任何發生在組織資通系統中可觀察到行為的結果，當具備資安風險之特定系統事件發生時，資通系統應觸發記錄系統日誌功能，以描述事發時系統狀態。為使日誌分析可有效發揮作用，組織應仔細評估系統使用需求與資安風險後，定義哪些系統事件需要留下日誌，避免記錄功能流於形式，惟亦應避免留存不必要之系統事件日誌，過於冗雜的內容對日誌分析活動沒有幫助，反而可能危害系統效能及儲存空間。

- 實務上建議可包含(但不限於)以下系統事件：
  - 管理者行為(如調整系統組態、異動系統帳號等)
  - 身分驗證失敗(如帳號登入失敗、觸發帳戶鎖定等)
  - 存取資源失敗(如頁面失效、資料庫連線失敗等)
  - 功能錯誤(如系統功能無法使用、帳戶無法登入等)
  - 重要資料異動(如存取個人資料或機敏性資料等)
  - 重要操作行為(如變更個人密碼、金融轉帳交易等)

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第七條(記錄事件)

三、資通系統應記錄管理者帳號所執行之各項功能，且應於核心系統最高權限帳號、特殊功能(如程式或軟體異動、參數或組態變更權限等)權限帳號被使用時，每日覆核使用結果。

Data Output　Explain　Messages　Notifications　Scratch Pad

	id [PK] integer	action_type text	action_descr text	user_id integer	log_time timestamp without time zone
1	25607	登入	機關管理者帳號登入	258	2020-08-24 08:56:28.994
2	25605	登入	機關管理者帳號登入	258	2020-08-20 14:36:56.266
3	25604	登入	機關管理者帳號登入	258	2020-08-20 14:32:32.808
4	25602	登入	機關管理者帳號登入	258	2020-08-20 13:50:21.884
5	25600	登入	機關管理者帳號登入	258	2020-08-20 11:58:05.661
6	25598	登入	機關管理者帳號登入	258	2020-08-20 11:54:57.422
7	25596	登入	機關管理者帳號登入	258	2020-08-20 11:51:12.689

內容說明

- 資通系統管理者帳號具有最高系統操作權限，無論是故意或非故意操作行為，都具有高度操作風險，可能對組織產生重大且不利影響，而駭客入侵時，亦常試圖取得系統管理者帳號權限，以進行更進一步攻擊行為，故記錄管理者帳號執行各項功能，不僅有助於強化內部控制與稽核，亦有助於追蹤資安事件行為軌跡。

佐證資料

- 組織訂定之日誌相關管理辦法
- 資通系統日誌

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第七條(記錄事件)

四、組織應定期審查核心系統產生之電腦稽核紀錄（日誌），非核心系統宜定期審查。

(1) 應用系統屬於中風險等級以上者，應每季審查稽核事件(帳號異動、密碼異動、登入失敗)，檢視已稽核的事件集合仍有必要且已滿足稽核需求。

佐證資料

- 組織訂定之日誌相關管理辦法
- 日誌審查紀錄

內容說明

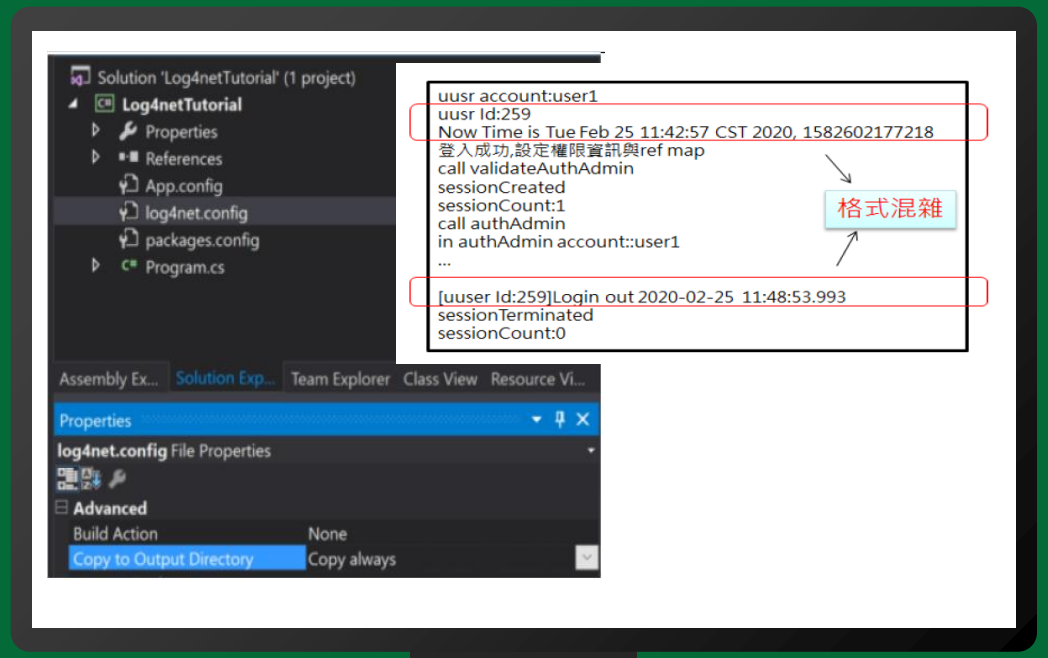
- 應定期審查分析資通系統產生之日誌內容，以掌握是否在期間內曾發生重要資安事件，如異常存取行為、重大系統錯誤等。
- 市面上有多款日誌管理(Log Management)或資安事件管理(Security Information Event Management，SIEM)解決方案，其功能為自動化收集各種系統元件或設備所產生日誌，並在符合資通安全政策及相關法規要求下，進行日誌收容、事件分類、日誌關聯分析、日誌監看、觸發警告及建立報表等功能，可協助相關權責人員進行日誌分析與管理審查活動，減輕管理人員的負擔。
- 應參考所訂定之日誌留存政策並決定日誌審查之週期。例如，若組織規定日誌留存期限為6個月，則至少應每6個月內完成1次以上之審查活動。

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第八條(電腦稽核紀錄（日誌）記錄內容與容量)

一、資通系統產生之電腦稽核紀錄（日誌）應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，宜採用單一日誌機制，確保輸出格式之一致性，並應依組織所訂之資通安全政策及相關法令要求及組織業務需求納入其他相關資訊。



佐證資料

- 組織訂定之日誌相關管理辦法
- 資通系統RFP
- 資通系統日誌

內容說明

- 日誌應詳細描述所觸發事件，包含人、事、時、地、物等關鍵資訊，如使用者帳號、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。惟須注意應避免在日誌內留下個人資料及涉及隱私內容，以符合我國個人資料保護法相關規定。

- 日誌輸出格式的可讀性對日誌關聯分析效率影響甚鉅，尤其資通系統開發人員常會利用開發框架內建或第三方所提供日誌記錄工具或函式庫，以留存客製化日誌內容，此時若因各程式功能模組實作差異或是多位開發人員不同程式撰寫習慣，就很容易產生不同格式日誌，造成檢視分析上的困難。例如，使用.NET開發框架資通系統，開發人員可能選擇使用.NET Logger、Apache Log4NET及NLog等元件產生日誌，而Java資通系統則可能選擇Java Util Logging或Apache Log4j等元件。資通系統日誌格式上混雜，如功能模組1的日期格式採用MM-DD-YYYY，而功能模組2卻採用YYYY/MM/DD。為減少這種日誌格式混雜現象，宜要求委外廠商或內部開發人員遵照一致性程式撰寫標準(Coding Standard)，避免同時混用多種日誌框架與不同格式，以確保日誌內容品質。

- 應確保日誌已納入所有必要之資訊。日誌的需求，包含系統維運或業務使用需求，同時也要考慮法律規章、行政命令、政策、產業標準及合約等要求。適用情境，例如「電子支付機構資訊系統標準及安全控管作業基準辦法」第13條第五款規定：「電子支付作業環境之個人資料保護應建置留存個人資料使用軌跡(如登入帳號、系統功能、時間、系統名稱、查詢指令或結果)或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，包括檔案、螢幕畫面、列表。」，資通系統如涉及電子支付作業，為符合此項規範就應依規定將登入帳號、系統功能、時間、系統名稱、查詢指令或結果等資訊納入系統日誌內。

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第八條(電腦稽核紀錄（日誌）記錄內容與容量)

二、資通系統應依據電腦稽核紀錄（日誌）儲存需求，配置所需之儲存容量。

內容說明

- 資通系統應配置足夠之日誌儲存容量，如硬碟或資料庫空間，以避免因容量不足造成日誌損失或是降低記錄能力，此時可透過檢查剩餘容量即可推算是否符合日誌儲存需求。
- 亦可實作其他控制措施以維持可用之儲存空間，例如：
  - 定期檢查剩餘容量
  - 超過容量警戒值時通知相關人員
  - 定期壓縮或歸檔日誌
  - 定期刪除超過保存期限之日誌

佐證資料

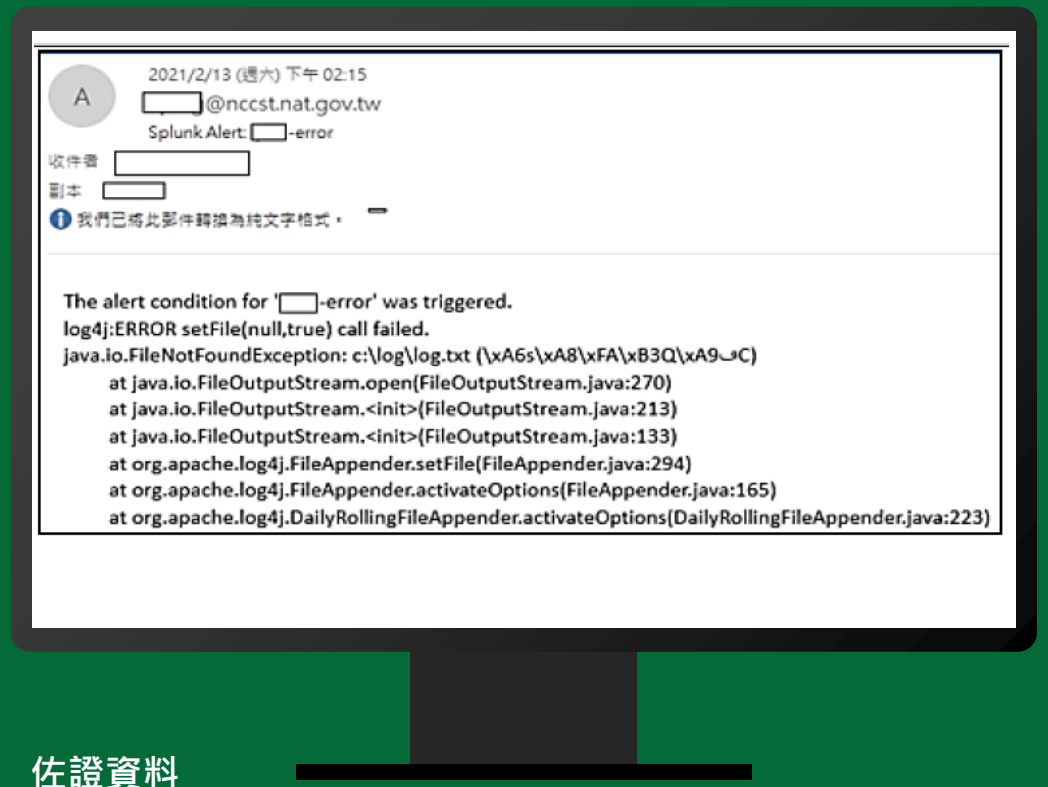
- 組織訂定之日誌相關管理辦法
- 資通系統日誌主機或資料庫容量資訊

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第九條(電腦稽核紀錄（日誌）處理失效之回應)

一、組織於資通系統電腦稽核紀錄（日誌）處理失效時，應採取適當之行動。



佐證資料

- 組織訂定之日誌相關管理辦法
- 資通系統日誌處理失效之測試紀錄

內容說明

- 應識別任何可能造成資通系統引發日誌處理失效狀況，並評估可能對資通系統造成的危害。日誌處理失效狀況，如軟/硬體錯誤、無法順利產生或留存日誌，以及日誌儲存容量飽和或超過等。可評估為不同日誌處理失效選擇定義額外動作(如依類型、依地理位置、依嚴重程度，或這些因素組合)，因應資通系統日誌處理失效之處理行動須符合組織資安規範與系統使用需求。
- 以信件、簡訊或其他方式警示特定人員或角色，警示信件範例。
- 於系統畫面顯示警示訊息
- 覆寫最舊的日誌
- 停止產生日誌
- 全系統關閉
- 部分系統關閉或有限的任務與維運功能降級操作

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第九條(電腦稽核紀錄（日誌）處理失效之回應)

二、第一類組織之核心系統規定需要即時通報之電腦稽核紀錄（日誌）處理失效事件發生時，核心系統宜於組織規定之時效內，對特定人員提出警告。

內容說明

- 應依照資安政策或相關規定，定義需要即時通報之特定記錄失效事件、時效及特定通知對象。
- 資通系統應依定義實作相關通知機制，以利及早釐清事件發生原因並進行故障排除。例如，當日誌伺服器(Log Server)無法連線造成日誌寫入失敗時，即時以信件或簡訊通知系統管理者。
- 如組織未另外訂定管理辦法，仍須遵循我國相關法規進行通報作業，如「資通安全事件通報及應變辦法」等。

佐證資料

- 組織訂定之日誌相關管理辦法或通報應變作業程序
- 資通系統日誌處理失效之測試紀錄

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第十條(時戳及校時)

一、資通系統應使用系統內部時鐘產生電腦稽核紀錄（日誌）所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。

	id [PK] integer	action_type text	action_descr text	user_id integer	log_time timestamp without time zone
1	25608	登入	一般帳號登入	365	2020-08-24 08:57:59.568
2	25607	登入	機關管理者帳號登入	258	2020-08-24 08:56:28.994
3	25605	登入	機關管理者帳號登入	258	2020-08-20 14:36:56.266
4	25604	登入	機關管理者帳號登入	258	2020-08-20 14:32:32.808
5	25587	登入	機關管理者帳號登入	258	2020-08-19 16:33:58.833
6	25583	登入	機關管理者帳號登入	400	2020-08-19 14:17:18.19
7	25582	登入	一般帳號登入	366	2020-08-19 09:00:03.971

內容說明

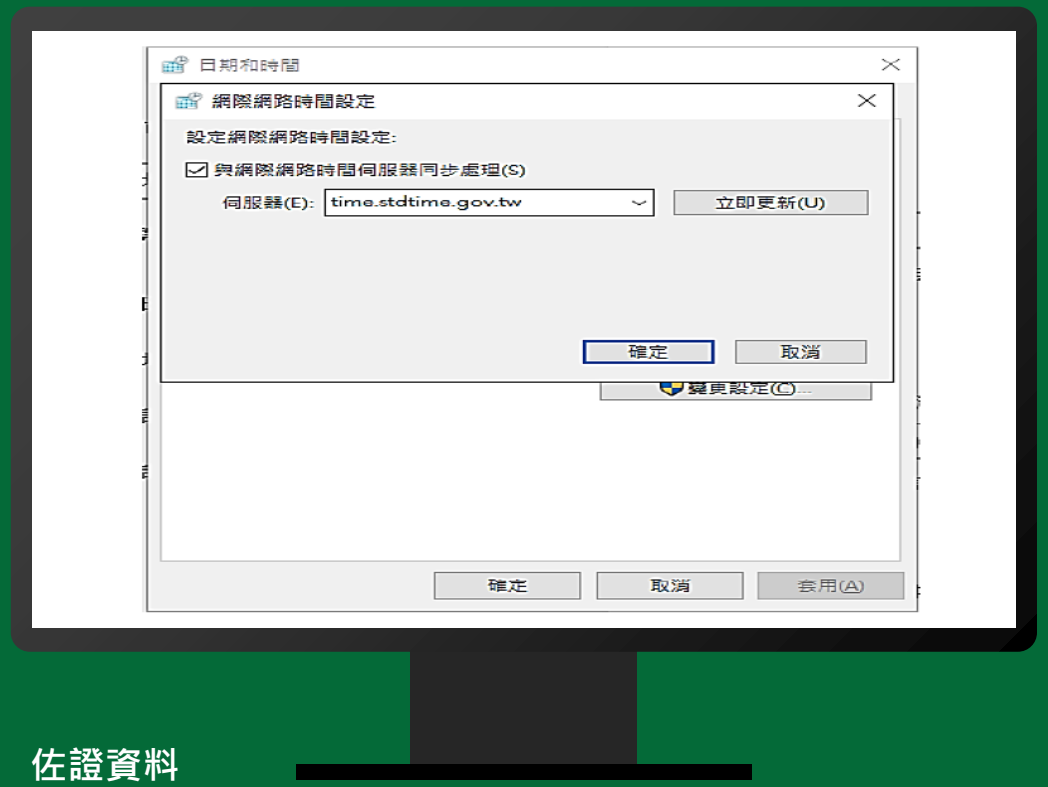
- 資通系統應使用系統內部時鐘產生日誌所需時戳，如作業系統日期與時間等。日誌中所使用時戳格式，通常以世界協調時間(UTC)、格林威治標準時間(GMT)或本地時間與UTC偏移時間來表示。

佐證資料

- 組織訂定之日誌相關管理辦法
- 資通系統日誌

勤業眾信版權所有 保留一切權利

第十條(時戳及校時)
二、資通系統內部時鐘應定期與基準時間源進行同步。



內容說明

- 資通系統應使用系統內部時鐘產生日誌所需時戳，而內部時鐘亦應定期進行同步以確保時間正確性。若以人工定期校正時間雖仍可保持時間正確性，但效率不佳且容易疏漏，故實務上常使用網際網路時間伺服器(NTP Server)或由組織自建之伺服器，並設定由系統依排程自動同步處理。使用情境如AD成員主機向AD伺服器同步時間，而AD伺服器則與網際網路伺服器(如time.stdtime.gov.tw等)進行同步。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統時間同步之測試紀錄

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第十一條(電腦稽核紀錄（日誌）資訊之保護)

一、對電腦稽核紀錄（日誌）之存取管理，僅限於有權限之使用者。

內容說明

- 日誌應妥善留存，以符合程式除錯、行為歸責、稽核取證及法律規範等使用需求，且其中可能存在機敏資訊，故應禁止未授權的存取、刪除及修改。應施行日誌(及其備份)之存取控管，僅限有權限之特定人員(如系統或資料庫管理者等)存取日誌(如日誌檔案或日誌主機等)，以保護機密性、完整性及可用性，此存取控制可能利用實體安全、系統功能實作帳號與權限管理或其他適用之管控機制來達成。

佐證資料

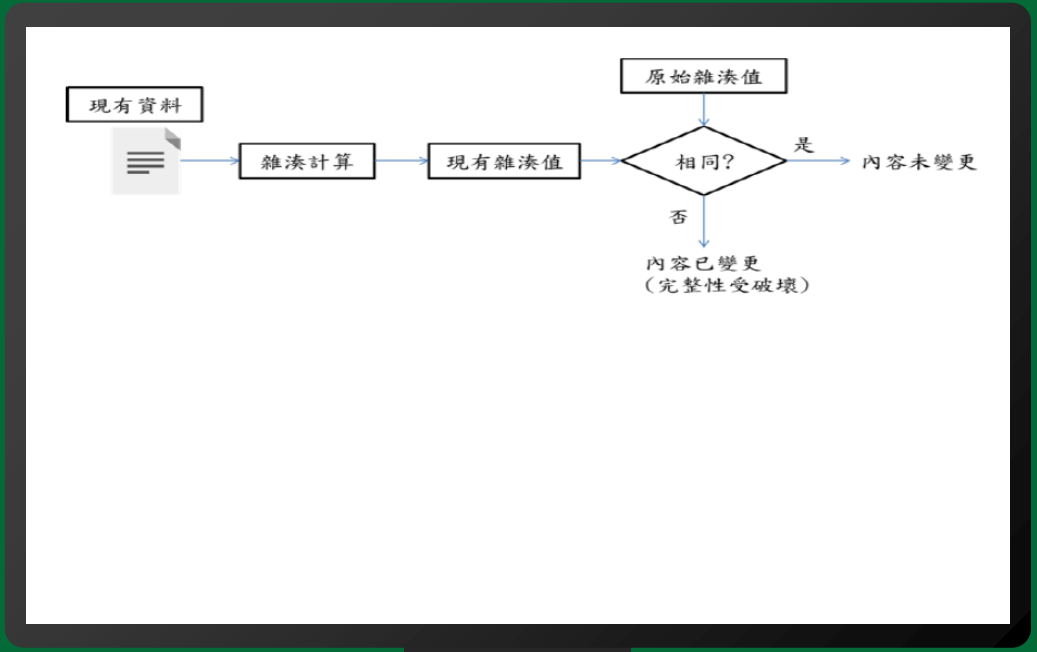
- 組織訂定之日誌相關管理辦法
- 日誌存取控制權限申請/審核紀錄
- 存取日誌之測試紀錄

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第十一條(電腦稽核紀錄（日誌）資訊之保護)(1/2)

二、核心系統應運用雜湊或其他適當方式之完整性確保機制，非核心系統宜有完整性確保機制。



佐證資料

組織訂定之日誌相關管理辦法

組織導入之完整性確保機制，如提供雜湊值等

內容說明

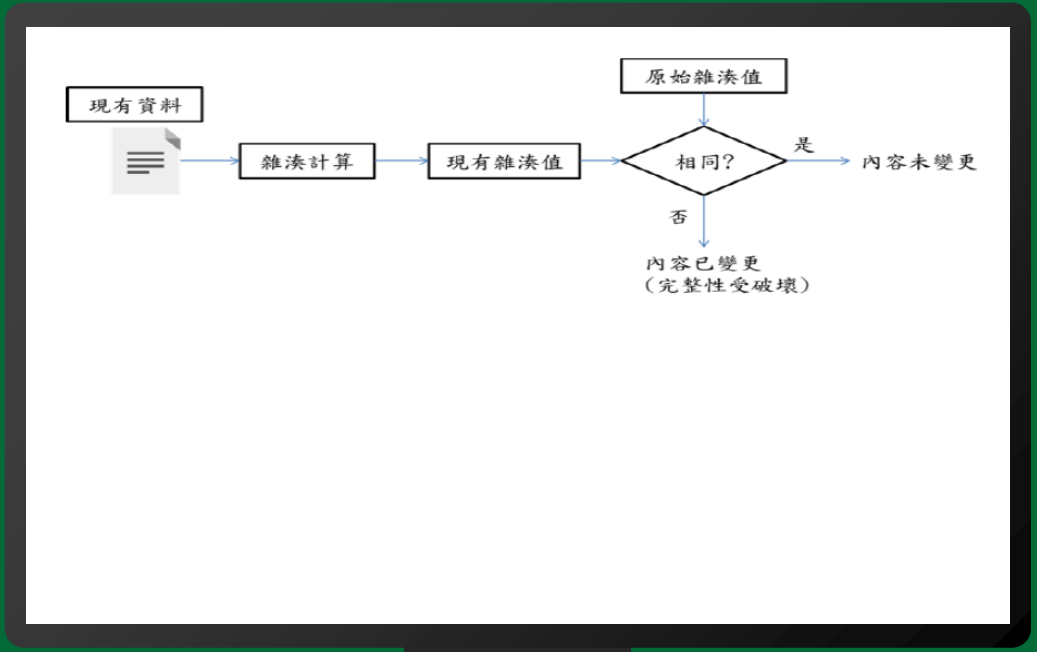
- 資通系統日誌可作為資安事件追蹤、行為歸責與資料佐證等用途，而惡意攻擊者也可能試圖竄改或破壞日誌內容以湮滅攻擊軌跡，因此除實作日誌存取管理外，亦須實作相關控制措施以確保在日誌內容正確可靠，在日誌保存期間不會受到未經授權的竄改。
- 從日誌完整性防護又分為事前預防、事中監視及事後驗證等三種面向，包含防止日誌內容被惡意竄改、當發生竄改行為時可即時察覺提出示警，以及在懷疑資料內容真實性時可驗證日誌內容是否曾經過異動等。可評估實際使用需求及資安風險，並以縱深防禦思維實作相關安全控制措施，以下舉例說明。
- (事前預防)將日誌以CD-ROM / DVD-ROM或其他具唯讀(Read Only)特性的儲存媒體進行保存，因可禁止其內容再次變更，故可保護日誌內容之完整性；惟須注意儲存媒體使用壽命，避免因保存不當而無法使用。
- (事前預防)將日誌經過加密處理後保存或備份，因未經授權使用者難以解密而無法閱讀與修改其中內容，故同時具有維持機密性與完整性之優點；惟此時加密金鑰之存取保護變為安全管理重點。使用情境如資通系統產生日誌檔案經過工具壓縮及加密處理後，儲存至日誌伺服器或其他儲存媒體進行保存或備份。

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第十一條(電腦稽核紀錄（日誌）資訊之保護)(2/2)

二、核心系統應運用雜湊或其他適當方式之完整性確保機制，非核心系統宜有完整性確保機制。



佐證資料

組織訂定之日誌相關管理辦法

組織導入之完整性確保機制，如提供雜湊值等

內容說明

- (事中監視)目前市面上推出多款針對檔案、目錄或資料庫專用之監控工具，其功能特性為可即時偵測檔案、目錄或資料庫欄位的異動，並提出警示通知。可評估針對系統日誌檔案進行監控，使用情境如應用程式每日產生新的日誌檔案，理論上過往的日誌檔案不會再進行內容異動，故若工具偵測過往檔案異動並發出警示，就可能是有故意的竄改行為，此時宜進一步確認釐清。

- (事後驗證)雜湊為一種常用且簡單之完整性驗證機制，可利用SHA-256與HMAC-SHA-256等雜湊演算法(Hash algorithms)對資料或檔案計算出雜湊值。雜湊值是一種資料指紋的概念，經常用來識別檔案與資料是否有被竄改。雜湊原理為不同資料即使只存在細微的差異亦會產生大不相同之雜湊值，故若要驗證原始內容是否經過異動，只要比對前後兩者所產生之雜湊值即可，若相異則表示資料內容已受到竄改。但須注意的是，雜湊值亦需適當保護與管理，如將雜湊值與日誌分開存放，避免惡意攻擊者一併竄改原始內容與雜湊值。使用情境如將每日產生並不再變動日誌檔案進行雜湊計算後留存雜湊值，未來需要驗證完整性時，再把現有資料重新計算產生新雜湊值，比對兩份雜湊值應相同，表示完整性未受到破壞。

勤業眾信版權所有 保留一切權利

事件日誌與可歸責性

第十一條(電腦稽核紀錄（日誌）資訊之保護)

三、第一類組織之核心系統應定期備份電腦稽核紀錄（日誌）至原系統外之其他實體系統。

內容說明

- 應定期執行日誌備份，且不可存放在同一個系統內，以避免因實體主機損毀而造成原始資料與備份資料一併丟失。常見方式如建置日誌伺服器(Log Server)、NAS及雲端空間等，或是利用磁碟與磁帶等儲存媒體存放備份資料。

佐證資料

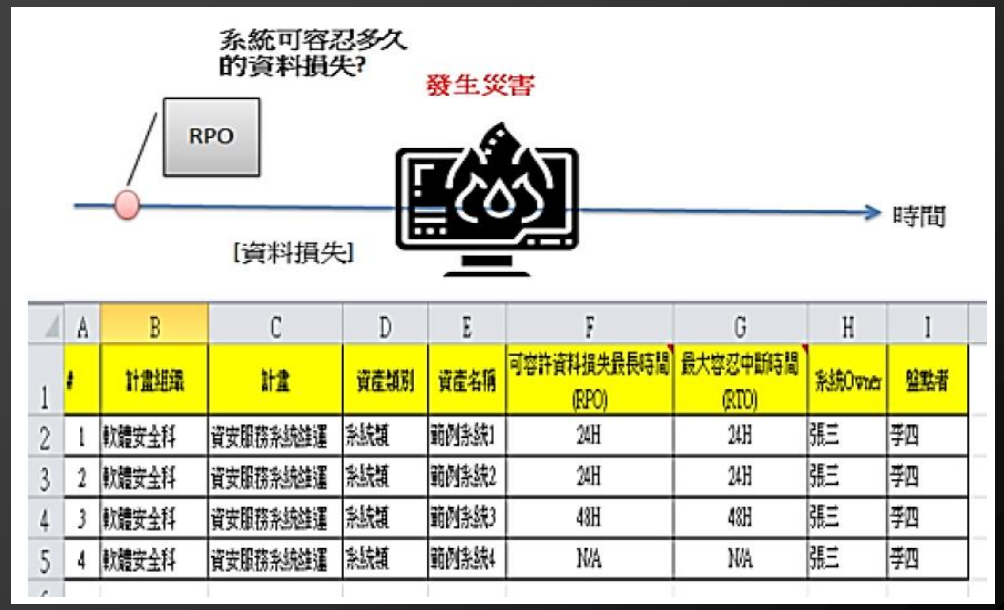
- 組織訂定之日誌相關管理辦法
- 日誌備份紀錄與結果

勤業眾信版權所有 保留一切權利

營運持續計畫

第十二條(系統備份)

一、組織應訂定資通系統可容忍資料損失之時間要求。



	A	B	C	D	E	F	G	H	I
1	#	計畫組織	計畫	資產類別	資產名稱	可容許資料損失最長時間(RPO)	最大容忍中斷時間(RTO)	系統Owner	盤點者
2	1	軟體安全科	資安服務系統維運	系統類	範例系統1	24H	24H	張三	李四
3	2	軟體安全科	資安服務系統維運	系統類	範例系統2	24H	24H	張三	李四
4	3	軟體安全科	資安服務系統維運	系統類	範例系統3	48H	48H	張三	李四
5	4	軟體安全科	資安服務系統維運	系統類	範例系統4	N/A	N/A	張三	李四

內容說明

- 應訂定可容忍資料損失之時間要求，若資安事件發生造成資料損失時，需使用最接近的備份資料進行復原，資料損失與備份資料之間的時間間隔，亦稱為復原點目標(Recovery Point Objective, RPO)
- RPO一旦訂定完成，則可協助系統維護人員選擇適合的備份機制及週期。如訂定為1小時，則至少每小時必須進行1次資料備份，所選擇儲存媒體可能為磁碟；但若RPO訂定為1週，則至少每週進行1次資料備份，使用磁帶或光碟片等媒體即可符合備份需求。

佐證資料

- 組織訂定之營運持續計畫

勤業眾信版權所有 保留一切權利

營運持續計畫

第十二條(系統備份)

二、組織應執行資通系統程式原始碼與資料備份。

佐證資料

- 組織訂定之營運持續計畫
- 源碼備份執行紀錄
- 資料備份執行紀錄

內容說明

- 資通系統應依組織資安政策及規範進行系統源碼(含原始程式碼、目的程式等)或資料(如系統業務資料等)備份作業。套裝軟體、租賃系統，或因合約特別規定允許委外廠商可不提供系統源碼者，不在此限。
- 當廠商交付驗收或是程式更版時，皆應透過有效之儲存管理機制進行備份，以有效掌控版本實際狀況。
- 實務上如建置版本控制系統，或利用(虛擬)主機備份與資料庫備份等方式達成備份效果。
- 系統源碼之版本控制與變更管理，以組織自行維護為原則，不宜全委由廠商負責變更管理作業。組織至少應留存系統源碼備份，避免委外廠商因故倒閉或更換後，無法再行還原系統源碼之情形。
- 應針對資通系統重要資料進行備份，重要資料如為維持關鍵系統服務所必須，或考量機密性、完整性及可用性而具有較高資安風險等資料。

勤業眾信版權所有 保留一切權利

營運持續計畫

第十二條(系統備份)

三、組織應定期測試資通系統備份資訊，以驗證備份媒體之可靠性及資訊之完整性。

備份資料應至少每半年執行資料回復測試，以確認備份媒體與資料之可用性，並將備份可用性測試之狀況應紀錄於「備份回復測試紀錄表」。

內容說明

- 常見之資料儲存媒體如磁碟、光碟及磁帶等，因使用方式及保存環境之差異，可能影響儲存媒體壽命而造成備份資料損毀，故應定期檢查儲存媒體仍可正常使用，並測試其中資料仍正確完整。

佐證資料

- 組織訂定之營運持續計畫
- 營運持續計畫測試紀錄

勤業眾信版權所有 保留一切權利

營運持續計畫

第十二條(系統備份)

四、第一類組織之核心系統應將備份還原，作為營運持續計畫測試之一部分。

表1 演練時程規劃表

NO	演練項目	預計完成時間			負責人	演練方式
		開始	結束	總計		
1	通報並於臨時指揮中心集合	09：00	09：30	30m	管理代表	☒模擬 ☐實際
2	成立緊急應變小組進行任務分派	09：31	09：40	10m	管理代表	☒模擬 ☐實際
3	中心長官聯繫	09：41	09：50	10m	中心 PO	☒模擬 ☐實際
4	系統維護人員進行檢查和處理，無法救回	09:50	10:00	10m	系統維護人員	☒模擬 ☐實際
5	請網管人員進行VM備份還原	10:00	16:50	6h50m	網管人員	☐模擬 ☒實際
6	系統維護人員進行測試，確認系統復原正常運作	16:50	17:00	10m	系統維護人員	☐模擬 ☒實際

內容說明

- 災害復原是營運持續計畫中相當重要之環節，其目的是為在發生天災、人為疏失或惡意破壞造成資通系統損害時，能快速回復至正常或可接受的營運水準。
- 營運持續計畫應定期完整測試、演練，以驗證計畫之適切性及有效性，在災害復原過程中應使用備份資料，以驗證備份機制是否正確可靠

佐證資料

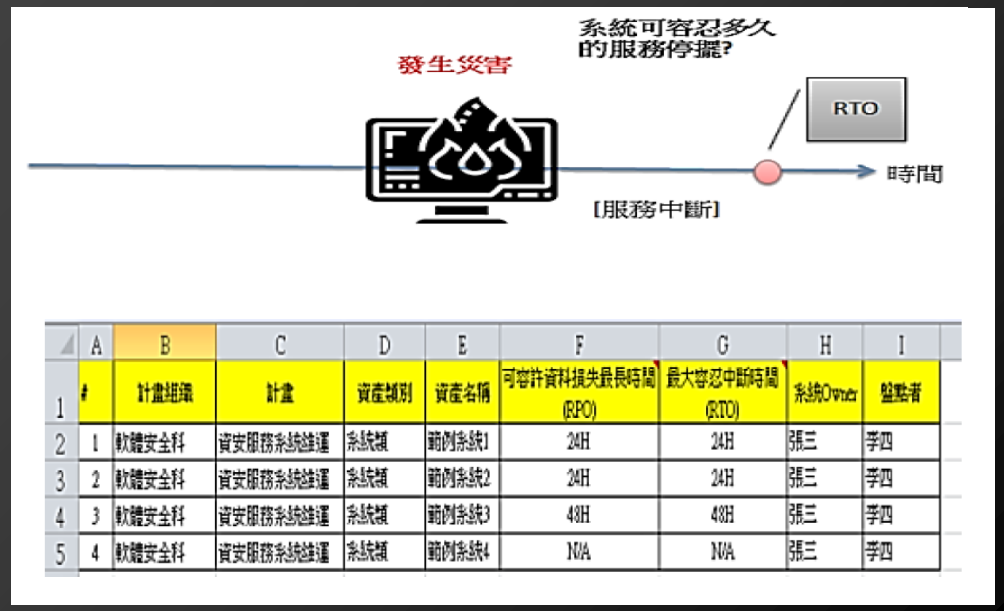
- 組織訂定之營運持續計畫
- 營運持續計畫測試紀錄

勤業眾信版權所有 保留一切權利

營運持續計畫

第十三條(系統備援)

一、組織應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。



	A	B	C	D	E	F	G	H	I
1	#	計畫組織	計畫	資產類別	資產名稱	可容許資料損失最長時間(RPO)	最大容忍中斷時間(RTO)	系統Owner	盤點者
2	1	軟體安全科	資安服務系統維運	系統類	範例系統1	24H	24H	張三	李四
3	2	軟體安全科	資安服務系統維運	系統類	範例系統2	24H	24H	張三	李四
4	3	軟體安全科	資安服務系統維運	系統類	範例系統3	48H	48H	張三	李四
5	4	軟體安全科	資安服務系統維運	系統類	範例系統4	N/A	N/A	張三	李四

內容說明

- 應考量服務需求、使用現況、相關資源項目，以及資安事件發生之風險，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，亦可稱為復原時間目標(Recovery Time Objective, RTO)

佐證資料

- 組織訂定之營運持續計畫
- 營運持續計畫測試紀錄

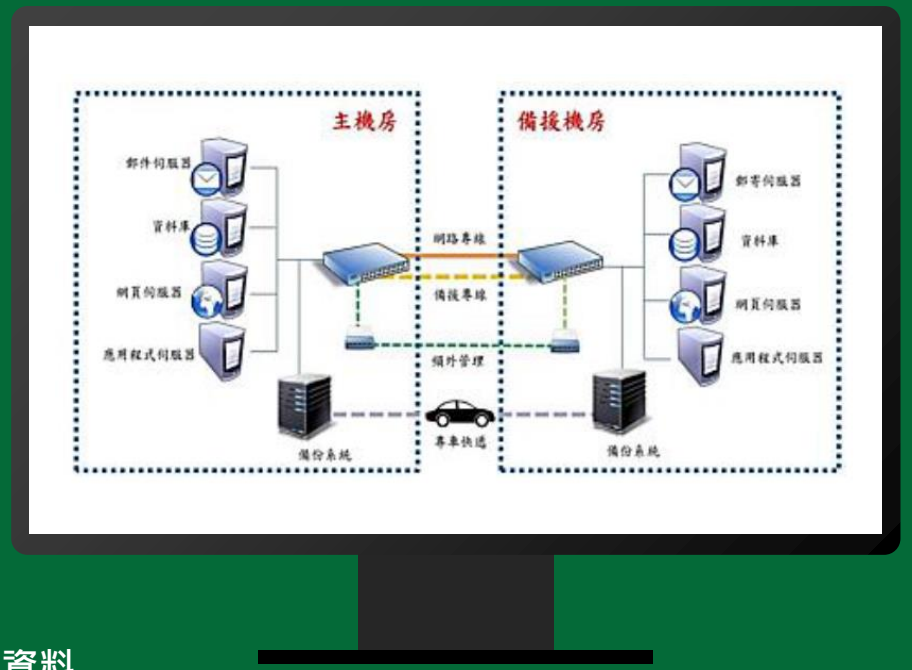
勤業眾信版權所有 保留一切權利

營運持續計畫

第十三條(系統備援)

二、資通系統原服務中斷時，組織應於可容忍時間內，由備援設備或其他方式取代並提供服務。

三、組織應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。



內容說明

- 應規劃適當的備援機制，以便在發生災害時，可於所訂定之容忍時間內讓服務回復正常運作。準備足夠之備援設備可提高服務運作之可用性，實務上常以異地備援或雲端服務方式提高系統可用性，可避免因火災、水災、遭竊等災難，造成重要軟硬體資源損毀而中斷服務。

佐證資料

- 組織訂定之營運持續計畫
- 營運持續計畫測試紀錄

勤業眾信版權所有 保留一切權利

識別與鑑別

第十四條(內部使用者之識別與鑑別)

一、資通系統應具備唯一識別及鑑別組織內部使用者(或代表組織使用者行為之程序)之功能，禁止使用共用帳號。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄
- 資通系統日誌

內容說明

- 資通系統應具有身分驗證機制，內部使用者如系統管理人者與其他雇員，亦包含臨時人員、駐點廠商及工讀人員等所有可能之資通系統使用者。除允許匿名存取之功能頁面外，資通系統應利用身分驗證(如帳號密碼或自然人憑證等)機制識別內部使用者(或代表使用者行為之程序)。
- 共用帳號行為可能出現在系統特權帳號或業務使用帳號，為提高可歸責性，應避免使用共用帳號。資通系統帳號僅提供已取得授權人員使用，並以開立個人帳號為原則，除非有特殊使用需求另行規定外，不應製發匿名或多人共用帳號。
- 以國家資通安全通報應變網站為例，組織進行通報作業時仍需以個人帳號登入使用，目的就是在避免共用帳號的問題，使用範例詳見圖。

勤業眾信版權所有 保留一切權利

第十四條(內部使用者之識別與鑑別)

識別與鑑別

二、透過網際網路使用管理帳號登入核心系統時，應採用多因子認證機制，第一類組織之核心系統對內部使用者存取宜採取多因子認證機制。

內容說明

- 透過網際網路使用管理帳號登入核心系統應採取多重認證技術，使用情境如系統管理者登入系統後臺管理功能頁面進行系統維護。多重認證技術係指採用兩種以上不同身分驗證因子，意即使用MFA (Multi-Factor Authentication)。身分驗證因子依類型，可分為所知之事、所持之物及所具之形等；所知之事係指利用限使用者知道的知識內容驗證身分，如密碼、PIN碼及安全問答等；所持之物則利用使用者擁有的實體或非實體物品，如憑證、晶片卡、SMS簡訊驗證碼、符記(Token)及一次性密碼(OTP)等；而所具之形為使用者具有的生物特徵辨識技術，如臉部、聲紋、指紋及虹膜等。

- 多重認證技術使用範例，如自然人憑證或健保卡，使用時需具備晶片卡(所有之物)與PIN碼(所知之事)正確組合，才能完成驗證。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

識別與鑑別

第十五條(身分驗證管理)

一、使用者使用預設密碼登入資通系統時，應於登入後要求立即變更預設密碼後方可繼續作業。

內容說明

- 預設密碼係指由資通系統自動產生或由系統管理者協助建立之個人使用者密碼，可能於使用者初次註冊或密碼重設時產生，供使用者登入系統。
- 預設密碼變更之要求，原則上應具備一定程度之強制力，而非僅作警示用途，避免使用者選擇視而不見。例如，當使用者未完成預設密碼變更時，限制使用者的系統功能操作權限，以促使用戶變更預設密碼。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

第十五條(身分驗證管理)

二、資通系統身分驗證相關資訊不以明文傳輸。

識別與鑑別

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

內容說明

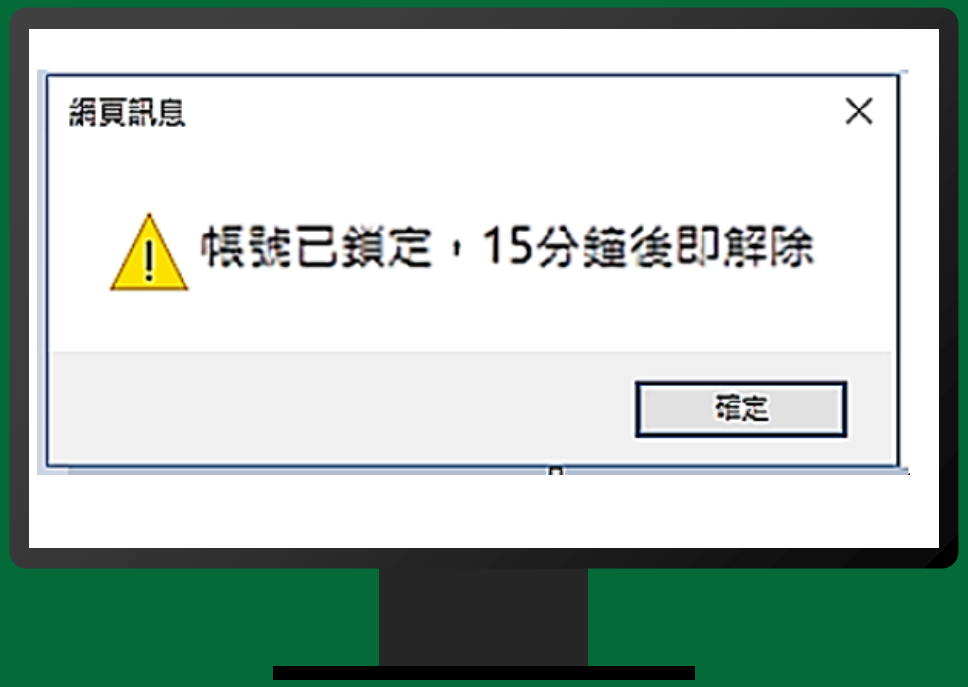
- 身分驗證相關資訊如密碼等具有機敏性，一旦外洩即可能造成帳戶被惡意盜用，切不可以未經保護的明文形式進行網路傳輸，避免攻擊者試圖攔截網路封包進而竊取其中密碼資訊。資通系統傳輸身分驗證資訊之行為，包含組織內外部使用者透過網際網路或組織內部網路登入資通系統帳戶、資通系統與其他資通系統介接時傳遞的身分驗證資訊等，皆應避免明文傳輸。
- 實務上常建立已加密之安全通道(如HTTPS與VPN等)保護傳輸資料之機密性。
- 當無法使用加密連線時，另一種替代方案如將機敏資訊先以應用程式或其他軟硬體實作加密或編碼保護後，再進行網路傳輸。

勤業眾信版權所有 保留一切權利

識別與鑑別

第十五條(身分驗證管理)

三、資通系統具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用組織自建之失敗驗證機制。屬電子式交易者，密碼輸入錯誤次數達三次者，應記錄登入失敗事件、鎖定該登入帳號並中斷連線；受理解除鎖定之申請時，應確實辨認身分，並留存相關紀錄後，始得解除鎖定。



內容說明

- 系統應實作帳戶鎖定機制以防範密碼破解攻擊，於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間則重新計次。組織得視系統使用需求，自建之失敗驗證機制，如訂定不同之鎖定觸發條件與閉鎖期，實作帳戶永久鎖定以人工解鎖，或是其他身分驗證強化機制等。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

識別與鑑別

第十五條(身分驗證管理)

四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可依組織自行規範辦理)

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

內容說明

- 應依資安政策及系統使用需求，訂定適用之密碼複雜度、最短及最長效期等使用限制。
- 最低密碼複雜度目的在產生數量足夠的密碼組合，如密碼長度或組成字元種類基本要求等。
- 密碼最短效期則在避免使用者為規避密碼歷程限制，而於短時間內頻繁變更密碼。
- 強制密碼最長效期，可避免使用者長期使用同一個密碼而提高被破解的風險，建議以不超過6個月為原則。
- 對非內部使用者，如資通系統服務係提供給一般民眾存取使用，可依組織自行規範辦理。

勤業眾信版權所有 保留一切權利

識別與鑑別

第十五條(身分驗證管理)
五、密碼變更時，至少不可以與前三次使用過之密碼相同。(對非內部使用者，可依組織自行規範辦理)

內容說明

- 資通系統密碼歷程紀錄至少須保留3代，不可重覆使用。
- 對非內部使用者，可依組織自行規範辦理。
- 非內部使用者包含所有未明確涵蓋於組織內部使用者的資通系統使用者，如一般民眾等。
- 針對非內部使用者之身分驗證，可自行規範資通系統密碼複雜度、最短效期、最長效期，以及密碼歷程等限制。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

識別與鑑別

第十五條(身分驗證管理)

七、核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。

內容說明

- 系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。防範方式如實作圖形驗證碼(CAPTCHA)，透過將驗證碼以圖形方式呈現於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式(如勾選特定選項等)，防堵自動化程式之嘗試行為；實作密碼鎖定機制亦可有效防範密碼暴力破解攻擊。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

識別與鑑別

第十五條(身分驗證管理)(1/2)

八、核心系統密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記（如：網站連結或一次性密碼One-time password,OTP，至使用者登記之電子信箱或手機）或其他驗證身分方式，非核心系統密碼重設後宜有驗證身分方式。

內容說明

- 當使用者忘記密碼時，常需使用密碼重設功能以設定新密碼，但密碼重設機制若設計不當，則容易被惡意攻擊者利用，偽冒成他人進行密碼重設，進而盜取帳戶使用權。
- 如資通系統提供使用者線上進行密碼重設，此時應有效確認使用者真實身分，常用方式如利用與帳號綁定之電子郵件或手機等僅限真實使用者存取裝置，作為密碼重設符記(Token)的載體。當進行密碼重設時，可要求使用者輸入當初註冊時所留存的電子郵件或手機號碼，比對無誤後則發送一次性及時效性的密碼重設符記，如簡訊驗證碼或Email認證連結等，必須設定有效期限(如30分鐘等)，且一旦使用過則立即作廢，不得重複使用。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

第十五條(身分驗證管理)(2/2)

識別與鑑別

八、核心系統密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記（如：網站連結或一次性密碼One-time password,OTP，至使用者登記之電子信箱或手機）或其他驗證身分方式，非核心系統密碼重設後宜有驗證身分方式。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

內容說明

- 如資通系統實作密碼重設機制，設計為由系統重新產生配發一組預設密碼，寄送給使用者後登入使用，原則上亦可視為一種形式符記；惟此時仍需實作一次性及時效性之特徵始符合此控制措施要求，如使用者以預設密碼初次登入後須強制立即變更密碼，且該預設密碼自產生後僅維持有效期限(如1小時等)，若逾期則無法登入，須申請重新產生。
- 如資通系統係透過AD服務進行身分驗證，因AD服務架構設計上限制，當使用者忘記密碼時，實務上需聯繫AD管理員協助進行密碼重設，系統並不會發送一次性及具有時效性符記，故原則上並不適用此控制措施。

勤業眾信版權所有 保留一切權利

第十六條(鑑別資訊回饋與加密模組識別)

一、組織應遮蔽資通系統鑑別過程中之資訊。

識別與鑑別

內容說明

- 遮蔽的鑑別符資訊回饋，避免有心人士在使用者輸入密碼時從後方窺視。實務上常會將密碼字元顯示為星號「*」。
- 如系統欲讓使用者檢視所輸入的密碼字元，可在遮蔽前以非常短時間顯示，或設計顯示密碼功能，惟預設應遮蔽字元，讓使用者手動勾選啟用。
- 如資通系統預設未遮蔽密碼字元，則未符合此控制措施。
- 驗證人員宜檢視系統功能頁面，並發展測試案例，在需要輸入密碼的頁面，除非使用者另行設定(如勾選「顯示密碼」)，否則不得長時間顯示密碼或PIN碼等輸入字元。

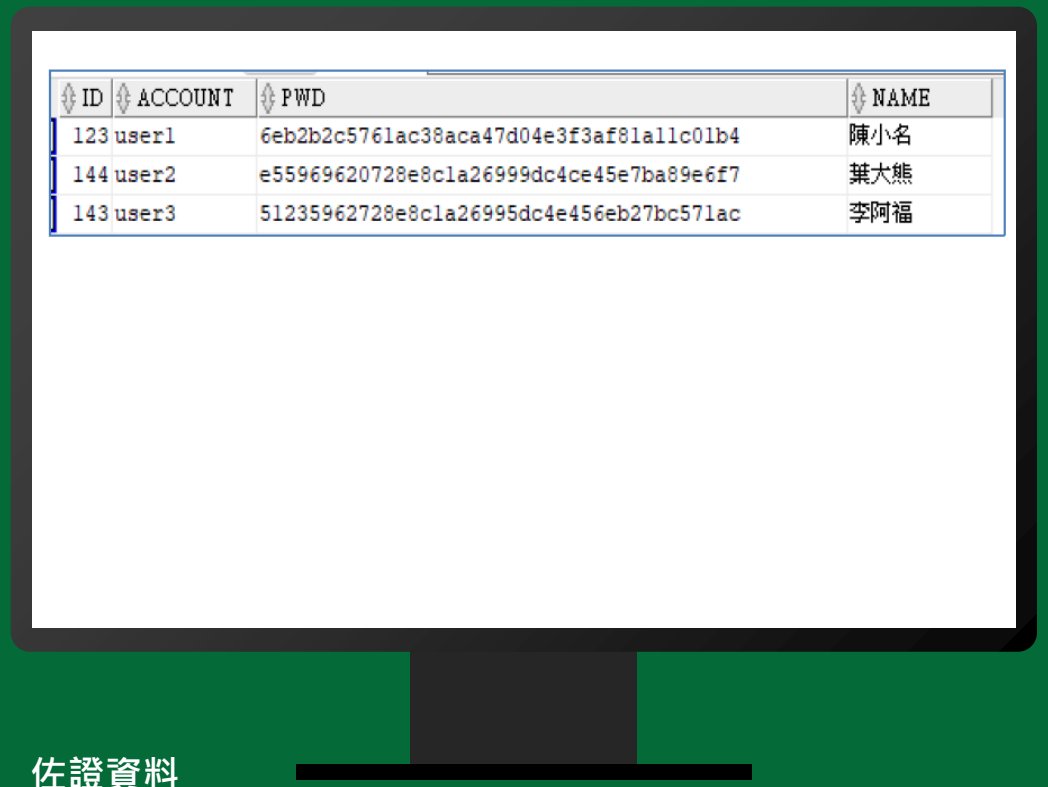
佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

第十六條(鑑別資訊回饋與加密模組識別)

二、組織如以密碼進行資通系統鑑別時，該密碼應加密或經雜湊處理後儲存。



ID	ACCOUNT	PWD	NAME
123	user1	6eb2b2c5761ac38aca47d04e3f3af81a11c01b4	陳小名
144	user2	e55969620728e8c1a26999dc4ce45e7ba89e6f7	葉大熊
143	user3	51235962728e8c1a26995dc4e456eb27bc571ac	李阿福

內容說明

- 密碼儲存時應經過加密或雜湊(Hashing)保護，實務上建議實作雜湊加鹽(Salted Hashing)技術，可有效對抗彩虹表(Rainbow Table)等密碼破解攻擊手法。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

識別與鑑別

第十七條(非內部使用者之識別與鑑別)

資通系統應識別及鑑別非組織使用者（或代表組織使用者行為之程序）。

內容說明

- 非組織使用者包含所有未明確涵蓋於組織內部使用者的資通系統使用者，如一般民眾等。
- 除公開頁面外，資通系統應利用身分驗證機制進行使用者識別及鑑別以強化可歸責性，如利用使用者帳號及密碼登入方式實作，範例詳見圖。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統功能規格書
- 資通系統身分驗證功能測試紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第十八條(系統發展生命週期需求分析與設計階段)

一、組織於系統需求分析階段，應針對資通系統安全需求（含機密性、可用性、完整性）進行確認。

附件1　資通系統資安需求項目查檢表

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
存取控制	3.2.1.1.1 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。	資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。	V	V	V	
	3.2.1.1.2 已逾期之臨時或緊急帳號應刪除或禁用。	若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。		V	V	
	3.2.1.1.3 資通系統閒置帳號應禁用。	宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。		V	V	

內容說明

- 自行開發或委外發展之系統，應在系統生命週期之初始階段，即將安全需求納入考量。
- 建議使用檢核表進行安全需求確認，好處為其可提供基本必要的安全控制項目，避免有所缺漏。實務上可自行設計發展系統安全需求檢核表，亦可參考技服中心「資通系統委外開發RFP資安需求範本(V2.0)-附件1資通系統資安需求項目查檢表」，提供相關權責人員在發展系統安全需求時參考依據，惟建議組織仍須自行調修其中項目，以符合資通系統開發專案之特性以及最新資安法規要求。
- 如部分所使用之資通系統開發完成並上線服務已久，可能當初在進行系統設計開發時並未充分考量或條列安全需求，惟現為符合資通系統防護基準之規範，建議仍應針對系統所實作之安全控制措施進行盤點並盡速補強缺漏項目，並留存相關檢核紀錄，以作為安全需求確認活動之稽核證據。

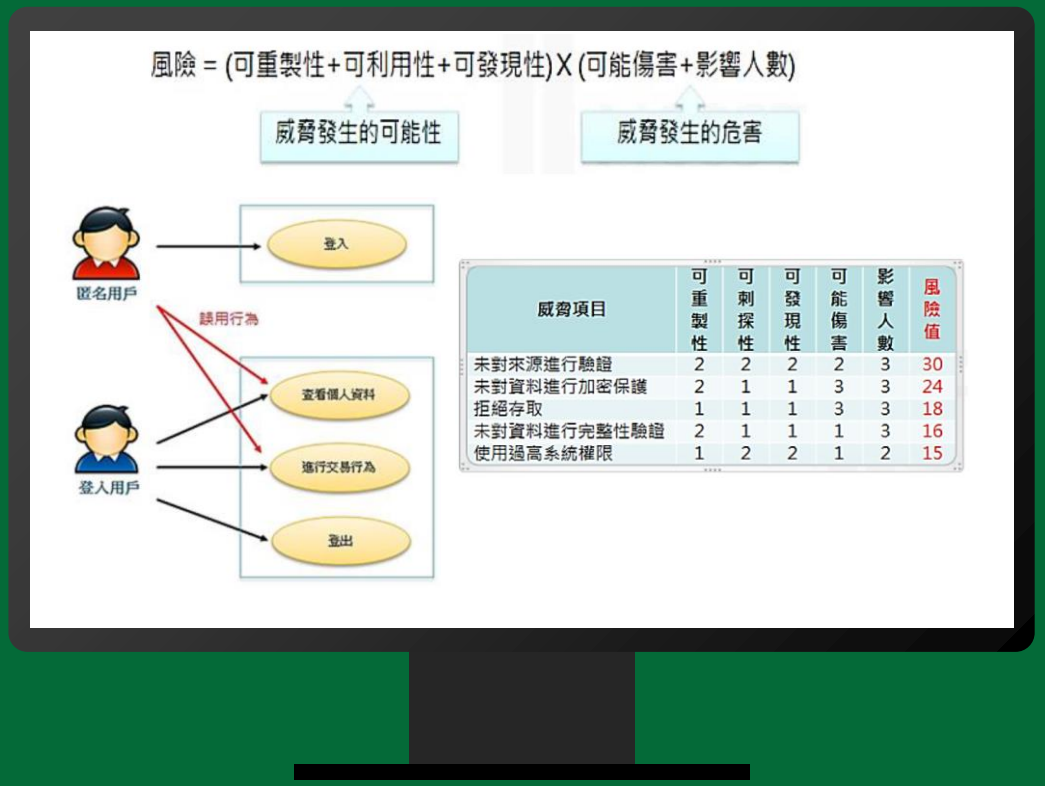
佐證資料

- 資通系統功能規格書
- 資通系統安全需求檢核表
- 安全需求確認相關紀錄

勤業眾信版權所有 保留一切權利

第十八條(系統發展生命週期需求分析與設計階段)

二、組織應根據核心系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估，非核心系統宜進行威脅識別、風險分析及評估。



威脅項目	可重製性	可刺探性	可發現性	可能傷害	影響人數	風險值
未對來源進行驗證	2	2	2	2	3	30
未對資料進行加密保護	2	1	1	3	3	24
拒絕存取	1	1	1	3	3	18
未對資料進行完整性驗證	2	1	1	1	3	16
使用過高系統權限	1	2	2	1	2	15

佐證資料

- 資通系統威脅識別執行紀錄或報告
- 資通系統風險評估執行紀錄或報告

內容說明

- 應識別資通系統所面臨之各種資安威脅，包含偽冒、竄改、否認行為、機敏資料外洩、拒絕存取服務及權限提升等，足以危害系統機密性、完整性及可用性之系統存取行為。
- 威脅識別與風險分析相關方法論，可參考包含誤用模型(Misuse case)，以及微軟所提出的威脅建模(Threat Modeling)、STRIDE威脅類別及DREAD風險計算方法等。
- 以誤用模型為例，其目的在透過發展負面的使用情境來識別系統可能之威脅，以幫助強化補足系統安全需求。誤用模型使用示意圖。因系統設計時缺失，未考量匿名用戶越權存取行為，造成匿名用戶可任意瀏覽其他人的個人資料，甚至偽冒他人進行交易行為，破壞機密性與完整性，此時應分析此威脅所產生的風險。

勤業眾信版權所有 保留一切權利

第十八條(系統發展生命週期需求分析與設計階段)

三、組織應將核心系統風險評估結果回饋需求階段之檢核項目，並提出安全需求修正，非核心系統宜依風險評估結果修正安全需求。

威脅項目	風險值	控制措施
未對來源進行驗證	30	• 採用帳號密碼登入認證 • 限制來源IP
未對資料進行加密保護	24	• 進行SSL/TLS加密
拒絕存取	18	• 使用分散式系統架構
未對資料進行完整性驗證	16	• 進行資料訊息摘要
使用過高系統權限	15	• 改採一般使用者權限執行

內容說明

- 應依規定根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估，所完成之風險評估結果應與既有之安全需求比對，以找出其中缺漏之處，其目的在強化安全需求內容，並修正安全需求檢核項目，以降低資安風險。例如，當系統風險等級變化(如中風險等級提升為高風險等級)時，應補強尚未實作之安全控制措施，此時有必要修正相關安全需求，並調整對應之需求檢核項目。例如，利用DREAD威脅風險分析結果，發展相對應的安全控制措施後，納入系統安全需求修正項目。

佐證資料

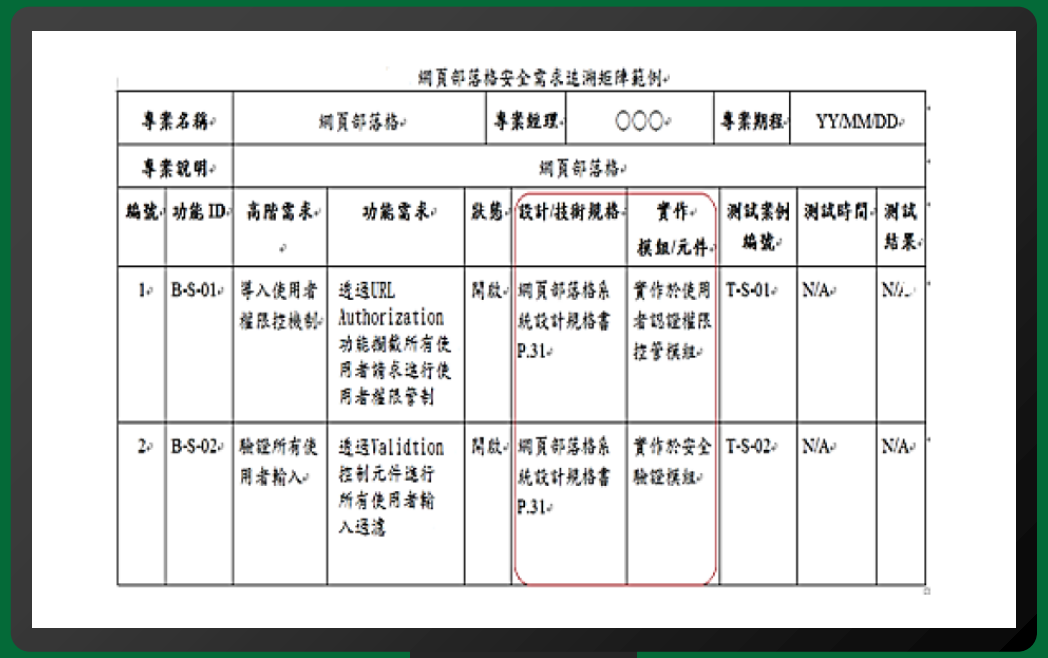
- 資通系統風險評估執行紀錄或報告
- 資通系統安全需求修正紀錄
- 組織訂定之安全需求檢核表

勤業眾信版權所有 保留一切權利

第十九條(系統發展生命週期開發與測試階段)

一、資通系統應針對安全需求實作必要控制措施。

系統與
服務獲得



網頁部落格安全需求追溯矩陣範例

專案名稱	網頁部落格			專案經理	○○○		專案期程	YY/MM/DD	
專案說明	網頁部落格								
編號	功能 ID	高階需求	功能需求	狀態	設計/技術規格	實作模組/元件	測試案例編號	測試時間	測試結果
1	B-S-01	導入使用者權限控機制	透過URL Authorization 功能攔截所有使用者請求進行使用者權限管制	開啟	網頁部落格系統設計規格書 P.31	實作於使用者認證權限控管模組	T-S-01	N/A	N/A
2	B-S-02	驗證所有使用者輸入	透過Validtion 控制元件進行所有使用者輸入過濾	開啟	網頁部落格系統設計規格書 P.31	實作於安全驗證模組	T-S-02	N/A	N/A

內容說明

- 資通系統應依照需求規格文件內容，實作相關功能或機制。安全需求可能包含組織規定之組態設定，以明確說明允許的功能、埠口、協定及服務等，或是提供必要資安防護能力，如密碼強度要求、加密強度要求、實作存取控制、身分驗證及授權機制等資安功能實作。於專案管理實務上可使用資通系統安全需求追蹤矩陣(Secure Requirement Traceability Matrix, SRTM)，將安全需求、功能實作及後續測試驗證等活動串聯起來，以便於追蹤管理。

佐證資料

- 資通系統安全需求RFP與功能規格書
- 資通系統安全需求追蹤矩陣(Secure Requirement Traceability Matrix, SRTM)
- 資通系統驗收測試報告

勤業眾信版權所有 保留一切權利

第十九條(系統發展生命週期開發與測試階段)

二、資通系統應注意避免軟體常見漏洞及實作必要控制措施。

項次	中文	英文
A01:2021	權限控制失效	Broken Access Control
A02:2021	加密機制失效	Cryptographic Failures
A03:2021	注入式攻擊	Injection
A04:2021	不安全設計	Insecure Design
A05:2021	安全設定缺陷	Security Misconfiguration
A06:2021	危險或過舊的元件	Vulnerable and Outdated Components
A07:2021	認證及驗證機制失效	Identification and Authentication Failures
A08:2021	軟體及資料完整性失效	Software and Data Integrity Failures
A09:2021	資安記錄及監控失效	Security Logging and Monitoring Failures
A010:2021	伺服端請求偽造	Server-Side Request Forgery (SSRF)

內容說明

- 常見漏洞如OWASP Top 10、CWE Top25等實作上容易產生之安全弱點及程式設計缺陷，系統開發時應避免產生具安全弱點之程式碼，如防範注入攻擊(Injection)與跨站腳本攻擊(XSS)等，並實作必要之安全控制措施，如強化身分驗證、存取控制及加密等。

佐證資料

- 教育訓練紀錄
- 安全程式碼撰寫規範
- 源碼掃描、弱點掃描、滲透測試執行紀錄與修補紀錄

勤業眾信版權所有 保留一切權利

第十九條(系統發展生命週期開發與測試階段)

三、資通系統發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。

內容說明

- 系統錯誤頁面若揭露過於詳細的錯誤訊息，可能會被被當成攻擊提示資訊而被人惡意利用，如密碼輸入錯誤之錯誤登錄嘗試、資料庫連線資訊、程式碼錯誤位置以及SQL執行語法等。此類錯誤訊息應該留存於系統日誌內，讓系統管理者進行程式除錯或故障排除即可，不應直接呈現於使用者操作頁面上。使用者頁面呈現過於詳細的錯誤訊息頁面，不僅洩露原始程式檔案位置，亦揭露程式碼實作細節，應避免顯示。

- 實務上常客製化錯誤頁面，僅顯示聯絡相關資訊與簡短錯誤代碼(如404錯誤等)，以提供使用者與客服人員或系統管理者溝通聯繫。可使用客製化頁面。

佐證資料

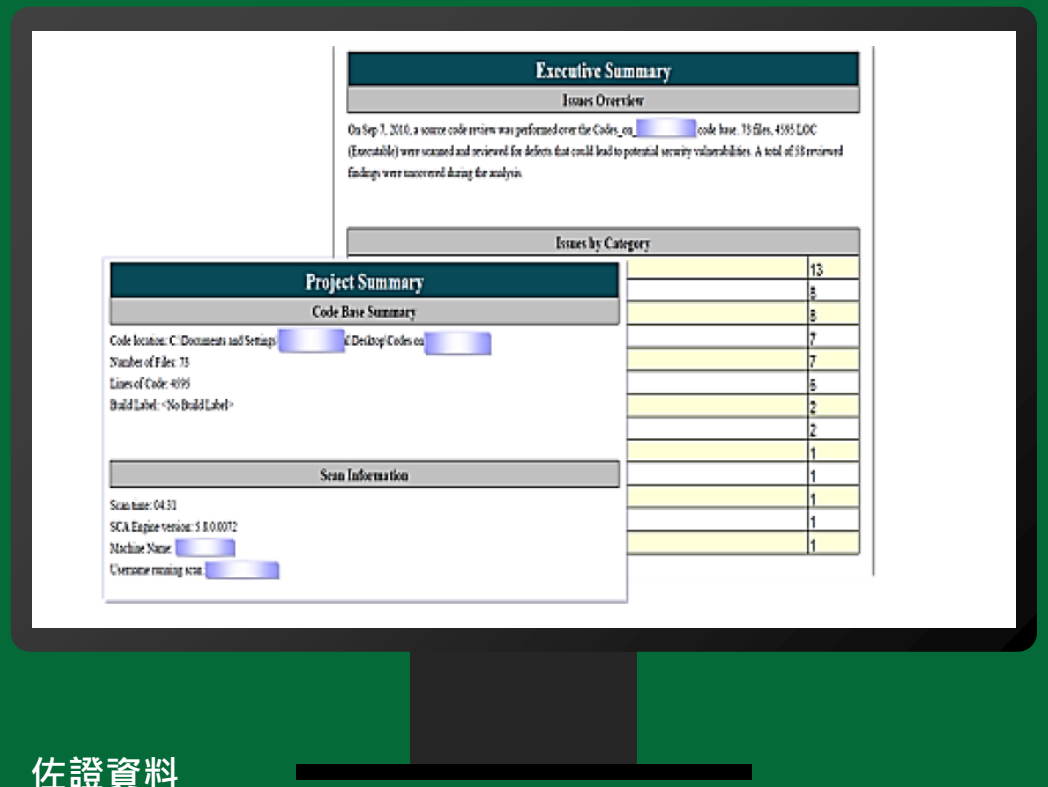
- 資通系統功能規格書
- 資通系統測試紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第十九條(系統發展生命週期開發與測試階段)

四、提供網際網路下單服務之組織，核心系統宜執行「源碼掃描」安全檢測。



內容說明

- 源碼掃描係指使用靜態分析掃描工具，識別應用程式原始碼內安全弱點，其優點為提供快速、高覆蓋率檢測結果，惟掃描工具不可避免仍會存在漏報與誤報現象，且解讀檢測結果正確性亦需要較高的專業知識。廠商交付源碼檢測報告應以市場主流，國際知名的工具所檢測產出報告為優先考量，可參考OWASP資安組織所整理之檢測工具列表。為避免檢測活動流於形式，應確實進行源碼弱點修補作業，並追蹤修復狀況。

佐證資料

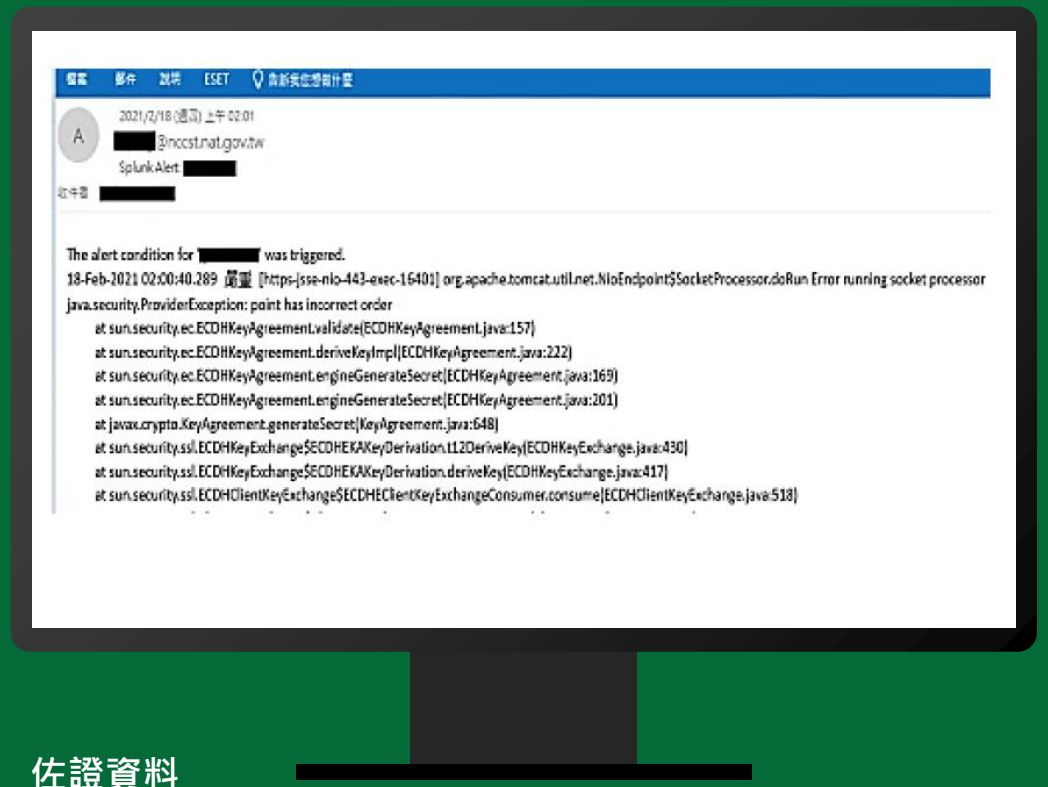
- 源碼掃描檢測報告
- 源碼掃描檢測複測報告
- 弱點修補紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第十九條(系統發展生命週期開發與測試階段)

五、第一類組織之核心系統宜具備發生嚴重錯誤時之通知機制。



內容說明

- 系統應避免產生安靜無聲的錯誤，從而錯失及時處理黃金時間，所以當偵測到資通系統發生嚴重錯誤(如局部或全部系統功能停擺等)，應啟動警示機制以通知相關人員進行後續處理。通知機制如呈現於系統執行畫面、寄發Email或簡訊通知、以電話或當面告知等。
- 偵測管道如系統實作例外捕捉(try-catch)機制、利用SOC監控服務或自動化監控程式等事先規劃之發現機制，而非僅被動接收系統使用者抱怨客訴或通知。

佐證資料

- 組織訂定之系統發展維護辦法
- 組織訂定之監控作業程序
- 資通系統錯誤處理功能測試紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第十九條(系統發展生命週期開發與測試階段)

六、提供網際網路下單服務之組織，應定期（至少每半年乙次）辦理資通系統「弱點掃描」安全檢測。

110 年第 2 季弱掃之弱點修補說明表

一、基本資料

系統負責人	張三	組別	系統安全組	科別	開發二科
系統名稱	範例系統				
系統 IP	10.20.30.40				
系統網址	https://10.20.30.40/Demo/				
檢測結果 弱點掃描 網站應用程式安全檢測	嚴重(CRITICAL)	高(HIGH)	中(MEDIUM)		
	0	1	3		
檢測結果 弱點掃描 主機安全檢測	嚴重(CRITICAL)	高(HIGH)	中(MEDIUM)		
	1	0	8		
備註	• 中心資安防護管理目標：「對外服務系統弱點掃描/滲透測試，以及資安健診之執行結果，判斷為中風險以上之弱點，應於 7 個工作天內完成矯正」。 • 無法於規定期限內完成矯正，系統負責人經組內審查同意後，應於規定期限內 2 天前提報管理代表同意。 • 本次弱點通知日期為：2021/6/1，依規定應於 2021/6/10 內完成弱點修補；若無法完成者，於 2021/6/8 前提報管理代表同意。				

二、修復說明

NO	風險等級	弱點類別	是否修復	完成日期	修補處理方式或修補困難簡述，(如可修復，請填入預估修復時間)。
1	中	Vulnerable JavaScript libraries	是	110/6/2	已於6/2針對已知弱點版本jQuery 進行升級修補與系統調整。

內容說明

- 資通系統應針對主機作業系統及應用程式執行「弱點掃描」安全檢測。執行弱點掃描安全檢測活動，並提供檢測結果報告或執行紀錄以供查檢。
- 檢測活動之執行週期應符合組織資安政策之規範。為避免檢測活動流於形式，應確實進行弱點修補作業，並追蹤修復狀況。

佐證資料

- 弱點掃描檢測報告
- 弱點掃描複測報告
- 弱點修補紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第十九條(系統發展生命週期開發與測試階段)

七、提供網際網路下單服務之組織，應定期對提供網際網路服務之核心系統辦理「滲透測試」安全檢測。

110 年第 2 季滲透測試之弱點修補說明表

一、基本資料

系統負責人	張三	組別	系統安全組	科別	開發一科
系統名稱	範例系統				
系統IP	10.20.30.40				
系統網址	https://10.20.30.40/Demo/				
滲透測試報告風險	嚴重(CRITICAL)	高(HIGH)	中(MEDIUM)		
	0	0	1		
備註	•中心資安防護管理目標：「對外服務系統弱點掃描/滲透測試，以及資安健診之執行結果，判斷為中風險以上之弱點，應於 7 個工作天內完成矯正」 •無法於規定期限內完成矯正，系統負責人經組內審查同意後，應於規定期限內 2 天前提報管理代表同意 •本次弱點通知日期為：2021/6/1，依規定應於 2021/6/10 內完成弱點修補；若無法完成者，於 2021/6/8 前提報管理代表同意				

二、修復說明

NO.	風險等級	弱點類別	是否修復	完成日期	修補處理方式或修補困難簡述(如可修復，請填入預估修復時間)
1	中	SQL Injection	是	110/6/2	已於 6/2 前完成將 SQL 語法改用 PrepareStatement 參數化查詢

內容說明

- 滲透測試是一種特殊類型評鑑，由技術熟練的資安專家模擬敵人行動，執行之白、灰、黑箱測試及分析等各種檢測活動，對資通系統或個別系統元件辨識可能被敵人利用的弱點。這種測試可用於驗證弱點，或驗證資通系統防護程度已達某種特定限制條件下(如時間、資源或技能等)能力。開始測試前，各方應協調及同意滲透測試場景與規則，宜將滲透測試規則與預期敵人進行攻擊所採用工具、技術及程序相互關聯，並依風險評鑑結果與等級需求進行滲透測試，並在定義之廣度/深度及限制因素下執行滲透測試。

- 滲透測試與弱點掃描執行目的不相同，弱點掃描僅作為滲透測試活動其中之一個環節。弱點掃描係利用自動化工具，檢查系統潛藏的已知弱點，產生弱點風險分析報告，並不會利用該弱點入侵破壞系統；而滲透測試則會試圖模仿敵人，從安全相關弱點或漏洞深度分析並加以利用，對系統進行入侵攻擊，執行過程中也會需要使用檢測工具輔助，但滲透測試成效更取決於檢測人員實務經驗與入侵技巧，而非僅仰賴自動化掃描工具。

- 自行或委外開發之高風險等級資通系統，不分內網或外網，皆應執行滲透測試安全性檢測活動，並提供檢測結果報告或執行紀錄以供查檢，檢測活動之執行週期應符合資安法(如應辦事項等)與組織資安政策之規範。為避免檢測活動流於形式，應確實進行弱點修補作業，並追蹤修復狀況。

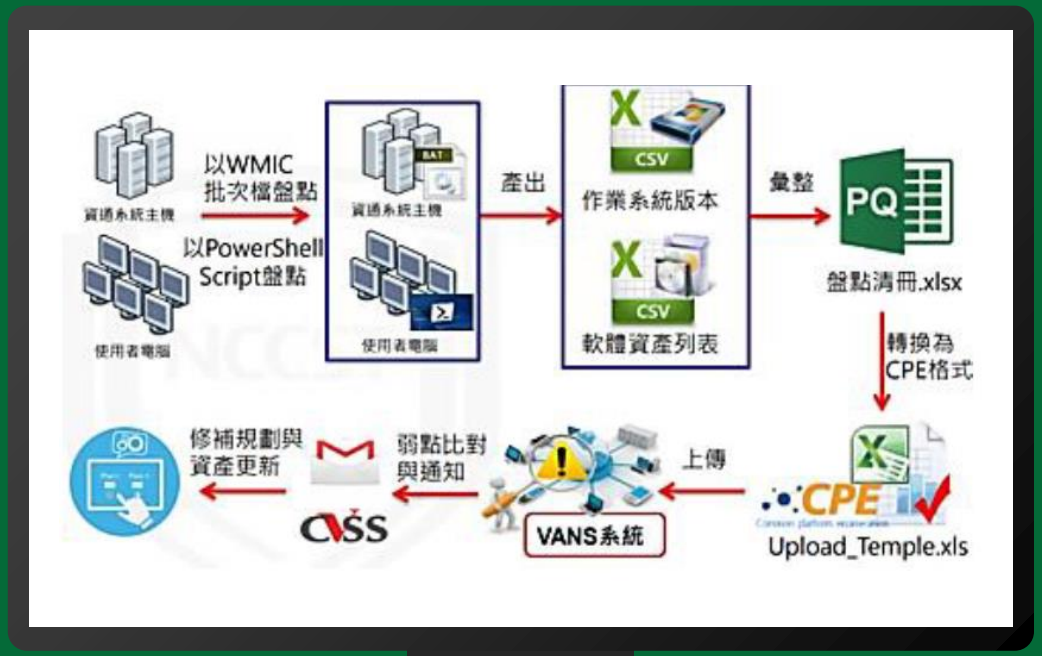
佐證資料

- 滲透測試檢測報告
- 滲透測試複測報告
- 弱點修補紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第二十條(系統發展生命週期部署、維運與委外階段)(1/2)
一、組織於部署環境中應針對資通系統相關安全威脅與漏洞，進行更新與修補，並關閉不必要服務及埠口。



內容說明

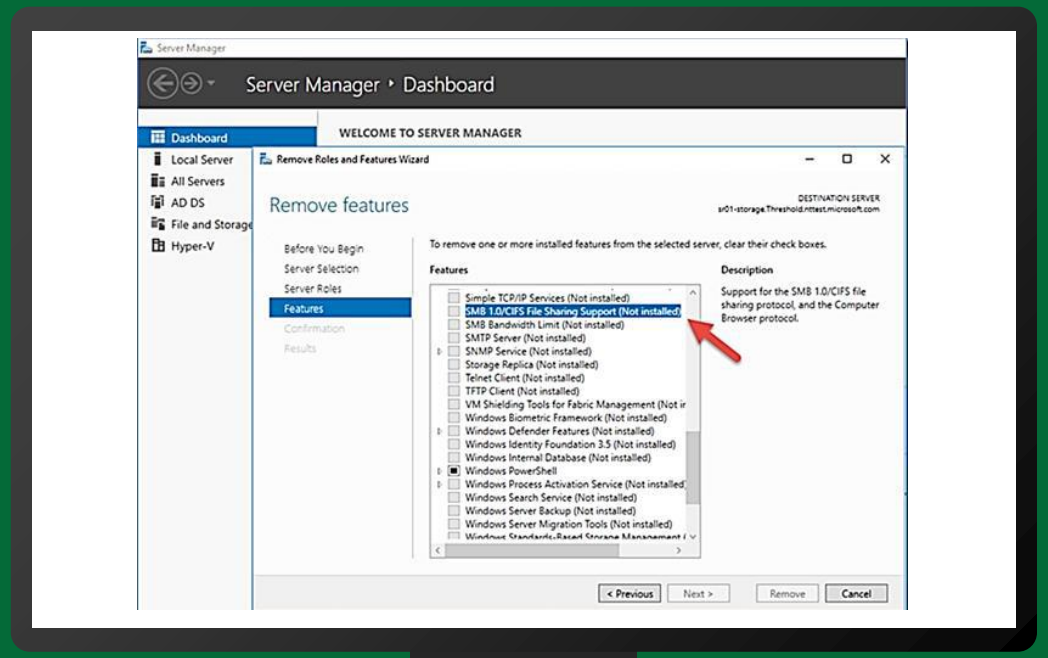
- 資通系統部署環境各個軟體元件皆可能面臨資通安全威脅，包含作業系統、網頁伺服器、執行環境(如Java Runtime Environment, JRE等)及函式庫(Library)等，因此執行版本更新與安全弱點修補相當重要，資通系統軟體元件。
- 作業系統應定期安裝更新檔案(如Windows Patch等)，當接獲資安弱點通報或相關資安訊息時，宜確認資通系統是否在威脅範圍內，利用弱點掃描等安全性檢測發現安全漏洞時，亦應進行元件更新與弱點修補。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統部署之防火牆規則
- 資通系統連線檢測紀錄

勤業眾信版權所有 保留一切權利

第二十條(系統發展生命週期部署、維運與委外階段)(2/2)
一、組織於部署環境中應針對資通系統相關安全威脅與漏洞，進行更新與修補，並關閉不必要服務及埠口。



佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統部署之防火牆規則
- 資通系統連線檢測紀錄

內容說明

- 系統管理者應盤點並保留業務運作必要開放的服務與埠口，以防止非授權連線、非授權資訊傳送或非授權通道建立。伺服器通常可同時提供廣泛多元的功能與服務，以Windows 作業系統為例，不同的服務有不同的預設啟動原則：有些預設會啟動(自動)，有些會在需要時啟動(手動)，有些預設會停用且必須先明確地啟用之後才能執行。預設啟用功能服務可能在組織業務運作上並非必要，若繼續開放這些服務及埠口連線，可能反而增加外部連線攻擊的資安風險。應限制資通系統所提供服務及埠口，以達到安全強化目的。例如，Windows作業系統透過TCP 445埠口提供Server Message Block (SMBv1)服務，而著名的WannaCry勒索軟體亦利用此埠口進行攻擊，原則上建議應停用SMBv1服務，並確認關閉445埠口以降低資安風險。Windows Server移除系統服務操作範例詳見圖。

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第二十條(系統發展生命週期部署、維運與委外階段)

二、組織應檢視現有之資通系統，應設定使用優質密碼，且應避免使用預設密碼。

```
<tomcat-users>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary.
-->
<!--
  NOTE:  The sample user and role entries below are wrapped in a comment
  and thus are ignored when reading this file. Do not forget to remove
  <!.. ..> that surrounds them.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="tomcat" roles="tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
-->
</tomcat-users>
```

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統測試紀錄

內容說明

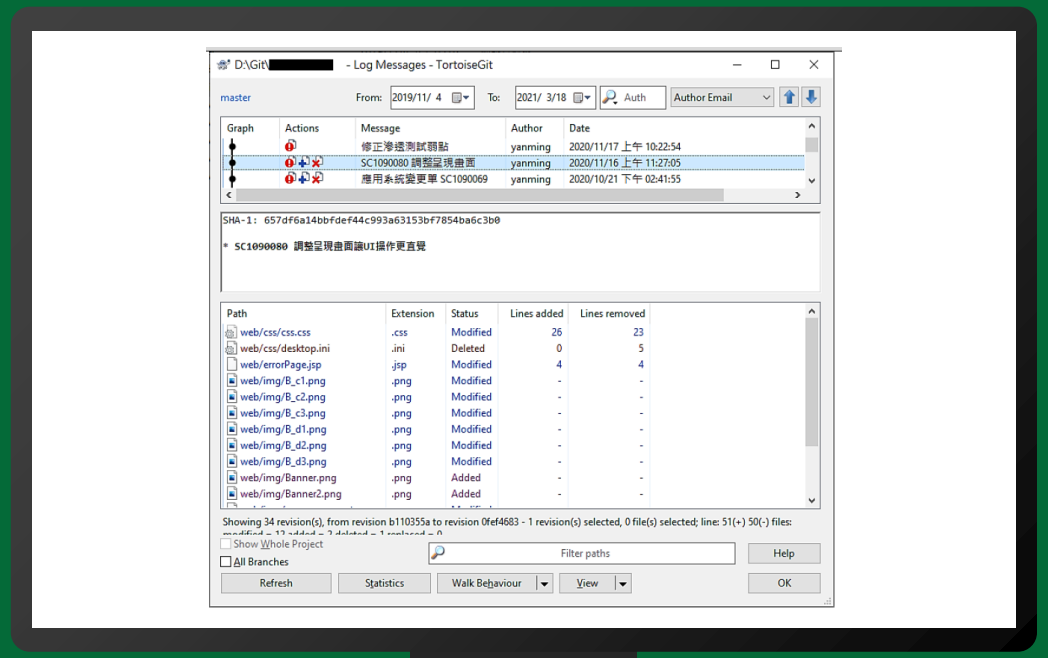
- 資通系統相關軟體(如資料庫與資通系統伺服器等軟體元件)若內建並啟用預設帳號密碼，很可能被惡意攻擊者透過搜尋引擎而輕易取得並加以利用，故應停用預設帳號與密碼，另外建立新的帳號登入使用。在預設帳號無法停用條件下，則應儘速變更密碼。

- 目前多數軟體元件會基於故障安全(Fail-Safe)原則，預設未啟用內建帳號密碼，但仍可能因系統管理者操作上失誤，在不經意啟用預設密碼而不自知，尤其若使用較舊版本的元件，操作風險又更高。以Apache Tomcat為例，新版本如Apache Tomcat 9已從組態設定檔案內移除預設帳號密碼，管理人員必須自行新增帳號密碼，故可降低操作失誤的風險；但若系統仍然使用舊版Apache Tomcat 7(官方已不再維護，建議更新版本)，此版本組態設定檔tomcat-users.xml中仍列出預設帳號密碼，雖已事先註解並未啟用，但管理人員仍可因為操作不當而啟用預設帳密，故風險較高，Tomcat 預設帳密設定範例詳見圖。

勤業眾信版權所有 保留一切權利

第二十條(系統發展生命週期部署、維運與委外階段)(1/2)

三、組織於資通系統發展生命週期之維運階段，應執行版本控制與變更管理。



佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統變更作業申請紀錄
- 資通系統版本變更紀錄

內容說明

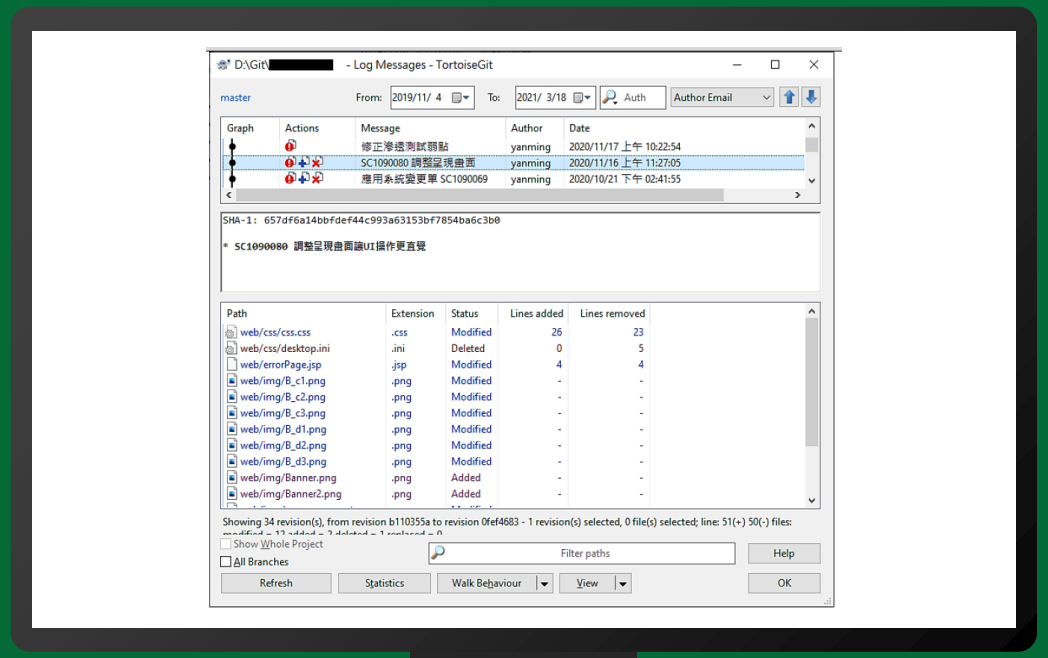
- 嚴謹的版本控制與變更管理可強化系統安全性與可用性。在維運階段可能因需求變更、系統除錯、功能精進等原因而需要變更系統組態，而版本控制目的為記錄系統組態在某段時間內的變更行為，使得使用者在需要時可取回特定版本，變更管理應予安全管制，須避免被惡意植入不當軟體、後門及電腦病毒等危害系統安全之元件。

- 實務上可建立程式館或使用版本控制軟體工具，以方便追蹤歷次的變更版本。知名的免費版本控制工具如CVS、Git及Subversion等，這些工具可將每次版本所有簽入檔案狀態儲存下來，並描述該版本的變更用途，如修正錯誤或新增功能等，這些描述可協助系統管理者理解各版本狀態差異，並在將來可視需求還原至先前特定版本。免費版本控制工具Git操作畫面範例詳見圖。

勤業眾信版權所有 保留一切權利

第二十條(系統發展生命週期部署、維運與委外階段)(2/2)

三、組織於資通系統發展生命週期之維運階段，應執行版本控制與變更管理。



內容說明

- 系統管理者進行系統變更作業，應符合組織規範，完成申請與審核程序後始可進行，如填寫資通系統變更作業申請單。執行變更作業前，宜先執行系統備份作業並訂定復原計畫，以保留原有系統作為異常時之衡量基準或復原準備。系統變更完成後，應更新相關系統操作文件及紀錄。
- 組織應以積極管理為原則，避免完全由委外廠商負責。若系統元件變更作業係委由廠商執行，應經過申請審核相關程序，並在組織人員監督下完成變更。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統變更作業申請紀錄
- 資通系統版本變更紀錄

勤業眾信版權所有 保留一切權利

系統與
服務獲得

第二十條(系統發展生命週期部署、維運與委外階段)

四、組織如委外辦理資通系統開發，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、可用性、完整性）納入委外契約

3. 需求說明

3.1 整體需求說明

詳細條列系統之各項功能要求及系統作業流程，並詳細說明之。

3.1.1 功能需求

3.1.2 系統作業流程說明

3.2 資安需求

委託機關應依據「資通安全責任等級分級辦法」之附表十「資通系統防護基準」，選取適用項目，包含 41 項技術面、13 項管理面之需求項目(詳附件 1)，以及 22 項資通系統防護基準之控制措施(詳附件 2、3)。

內容說明

- 應依據適用的法規命令與行政規則(含規範與指引等文件)及組織任務/營運需求，在資通系統、系統元件或資通系統服務合約納入安全相關要求，如可能包含安全功能要求、保護與安全相關文件要求、安全檢測活動要求及驗收標準等。
- 資通系統委外安全需求可參考技服中心「資通系統委外開發RFP資安需求範本(V2.0)」[6]，內容範例詳見圖。

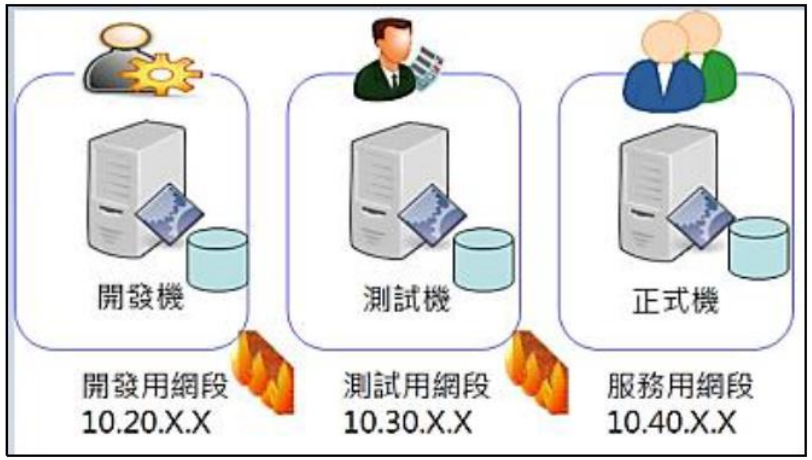
佐證資料

- 資通系統委外契約

勤業眾信版權所有 保留一切權利

第二十一條(獲得程序與系統文件)

一、資通系統正式作業環境應與開發、測試作業環境區隔。



佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統部署之防火牆規則

內容說明

- 應運用獨立的測試環境對資通系統變更進行分析，獨立的測試環境是指實體或邏輯上區隔、運作環境不同的環境，足以確保在測試環境中活動不會衝擊在正式作業環境中活動，正式作業環境中資訊不會無意中傳送給測試環境。應確保區隔環境時所需安全強度，如隔離相互間網路存取等，以網段區隔不同作業環境示意圖詳見圖。

- 開發環境、測試環境及正式作業環境區隔成不同的設備及網段，限制所能存取的應用程式及資料庫，以保護正式作業環境系統及資料。實務上開發人員常以本機電腦為開發環境，並連結使用本機端之資料庫進行應用程式開發。開發完畢再將應用程式部署至測試主機，並連結至測試用資料庫，供測試人員進行測試使用。俟測試完畢，再將應用程式部署至正式環境，並連結至正式資料庫提供上線服務。

勤業眾信版權所有 保留一切權利

第二十一條(獲得程序與系統文件)

二、組織應儲存與管理資通系統發展生命週期之相關文件。

文件/紀錄名稱	編號	保存年限
軟體發展計畫	依建構項目規範編碼	結案後2年
軟體需求規格書	依建構項目規範編碼	結案後2年
系統規格書	依建構項目規範編碼	結案後2年
軟體測試計畫	依建構項目規範編碼	結案後2年
維護手冊	依建構項目規範編碼	結案後2年
軟體使用手冊	依建構項目規範編碼	結案後2年
系統文件審查表	NCCST_FT_040	結案後2年
系統原始碼	依建構項目規範編碼	結案後2年
測試問題紀錄表	NCCST_FT_041 合併於軟體測試報告	結案後2年
軟體測試報告	依建構項目規範編碼	結案後2年
驗收紀錄表	NCCST_FT_042	結案後2年

內容說明

- 系統發展生命週期之相關文件應以書面或電子化形式保存，並被納入管理程序。

佐證資料

- 組織訂定之文件管理規範
- 資通系統相關文件

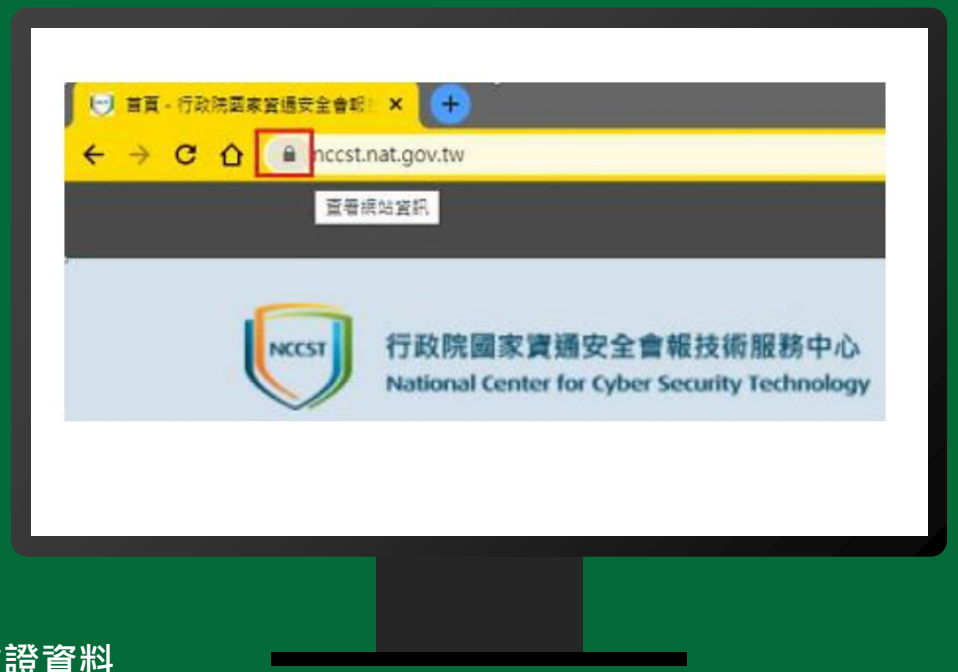
勤業眾信版權所有 保留一切權利

系統與
通訊保護

第二十二條(傳輸之機密性、完整性與資料儲存安全)

一、透過網際網路傳輸個人或機敏資料，核心系統應採用加密傳輸機制，以防止未授權之資訊揭露或偵測資訊之變更。

二、第一類組織於內部網路傳輸個人或機敏資料，核心系統宜採加密傳輸機制。傳輸過程中如有替代之實體保護措施者，則無需採加密傳輸機制。



內容說明

- 資通系統可實作加密機制，如HTTPS、SSH、SFTP及VPN等加密傳輸協定，或透過應用程式等適當方式，先行將資訊加密後再傳輸，以保護資料機密性與完整性。當站台啟用HTTPS，於瀏覽器網址列上會出現安全鎖頭圖示，範例詳見圖。

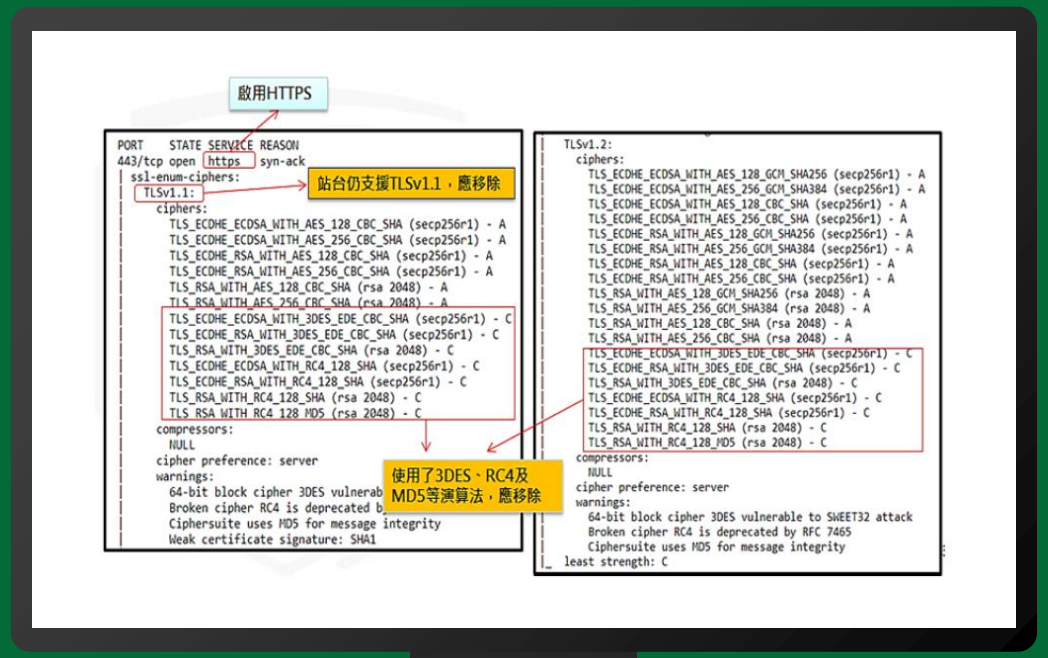
佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統加密連線之測試報告

勤業眾信版權所有 保留一切權利

第二十二條(傳輸之機密性、完整性與資料儲存安全)

五、加密機制應使用公開、國際機構驗證且未遭破解之演算法。



內容說明

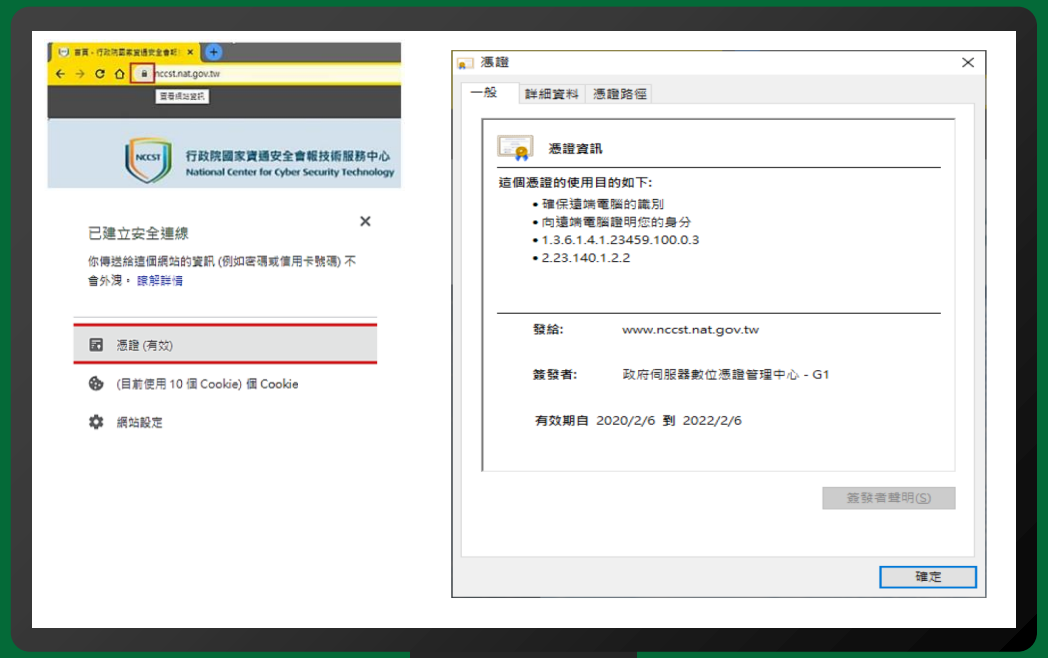
- SSL V3及TLS1.0皆已被視為安全性不足，若無相容性問題，建議停用。110年3月，RFC 8996標準[10]正式棄用TLS1.0及TLS 1.1。對IE、Edge、Chrome、Safari及Firefox而言，目前皆建議網站採用TLS 1.2，而網頁連線也以TLS 1.2為主。另外，加密協定所使用的演算法(Ciphers)亦有安全考量，如RC2、RC4、DES及3DES等加密演算法已遭破解，建議可改用AES與RSA等尚未遭破解之加密演算法。

佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統加密連線之測試報告，如Nmap檢測結果

勤業眾信版權所有 保留一切權利

第二十二條(傳輸之機密性、完整性與資料儲存安全)
六、加密機制之金鑰或憑證應定期更換。



內容說明

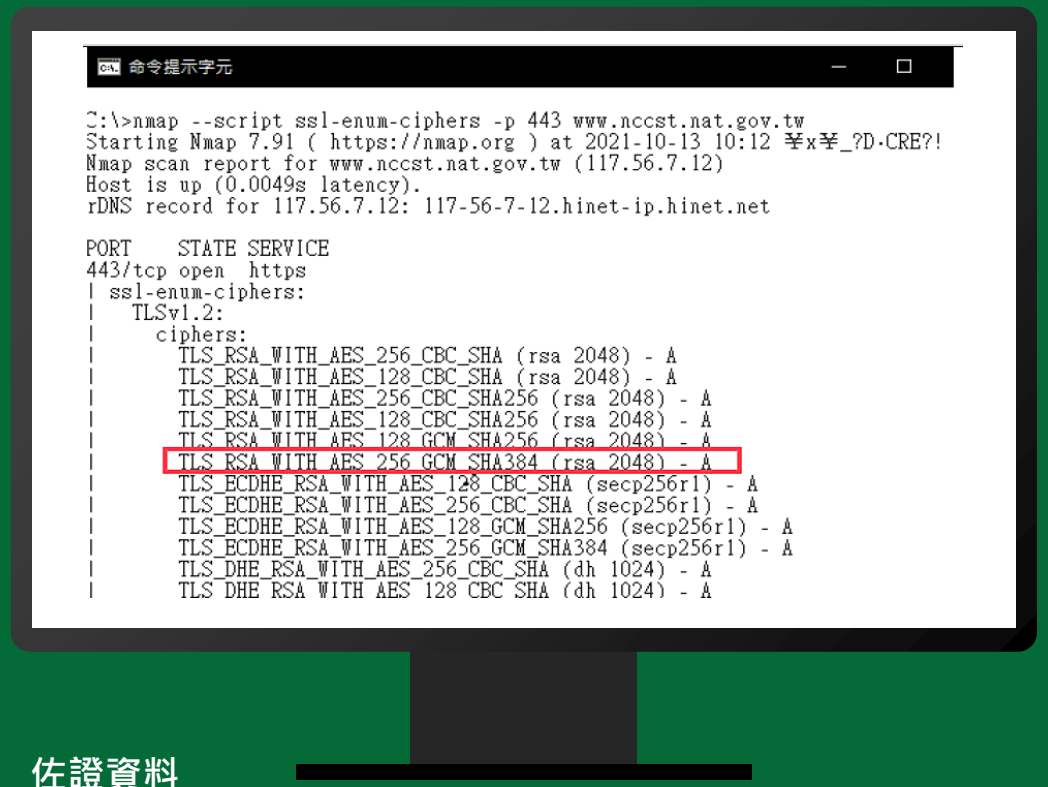
- TLS憑證(亦稱SSL憑證)服務，透過TLS加密傳輸協定建立瀏覽器與站台伺服器之間的安全通道。為避免TLS憑證被人惡意破解偽造，資通系統應設定憑證使用效期並定期更換。開對外服務站台應使用公正第三方所簽發之SSL憑證，以政府伺服器數位憑證管理中心(GTLSCA)為例，109年9月1日起所簽發之TLS憑證已調整為1年效期。組織內部使用之站台若使用自行簽發之TLS憑證，亦須避免使用萬年憑證，應評估資安風險及使用需求後，設定合理使用效期。

佐證資料

- 組織訂定之系統發展維護辦法
- 組織訂定之金鑰管理規範
- 資通系統憑證資訊

勤業眾信版權所有 保留一切權利

第二十二條(傳輸之機密性、完整性與資料儲存安全)
七、加密機制宜支援演算法最大長度金鑰。



內容說明

- 伺服器進行加密傳輸(如HTTPS等)時，可能因作業系統與資通系統伺服器元件版本等技術限制，僅能使用特定之加密演算法及金鑰長度範圍，此時宜設定資通系統可支援較長之金鑰長度，以降低金鑰被破解風險。

佐證資料

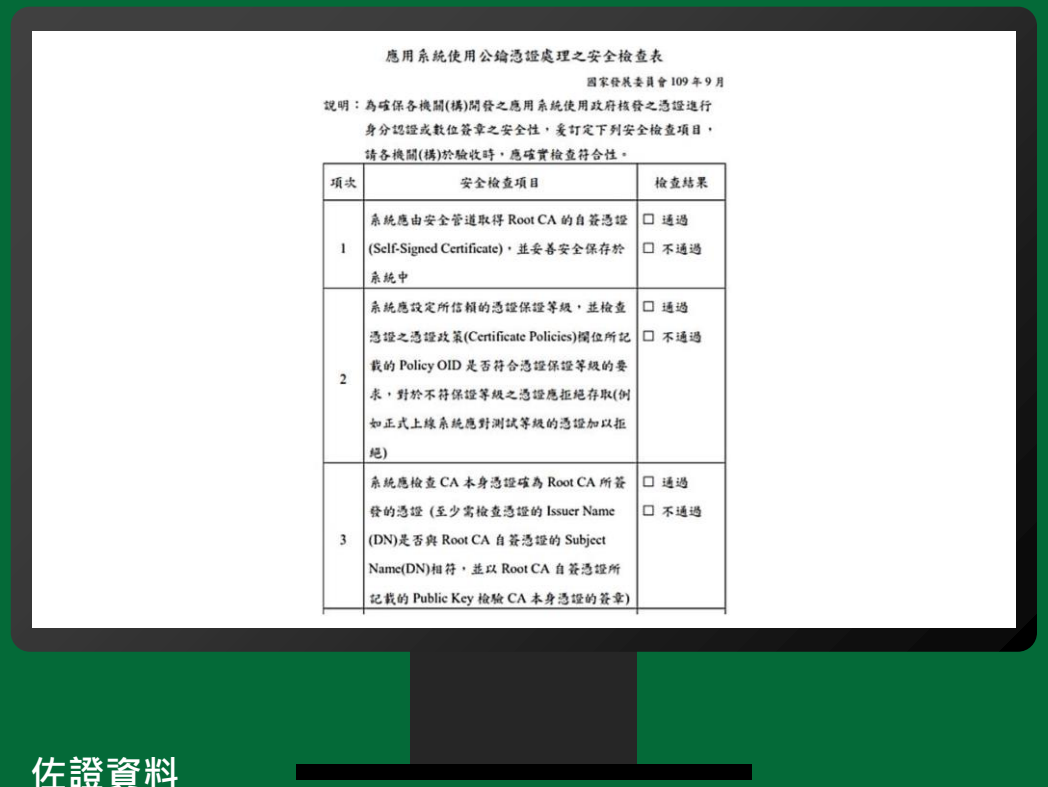
- 組織訂定之系統發展維護辦法
- 資通系統加密連線之測試報告，如Nmap檢測結果

勤業眾信版權所有 保留一切權利

系統與
通訊保護

第二十二條(傳輸之機密性、完整性與資料儲存安全)

八、加密機制於伺服器端之金鑰保管宜訂定管理規範及實施應有之安全防護措施。



應用系統使用公鑰憑證處理之安全檢查表

國家發展委員會 109 年 9 月

說明：為確保各機關(構)開發之應用系統使用政府核發之憑證進行身分認證或數位簽章之安全性，爰訂定下列安全檢查項目，請各機關(構)於驗收時，應確實檢查符合性。

項次	安全檢查項目	檢查結果
1	系統應由安全管道取得 Root CA 的自簽憑證(Self-Signed Certificate)，並妥善安全保存於系統中	☐ 通過 ☐ 不通過
2	系統應設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求，對於不符保證等級之憑證應拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)	☐ 通過 ☐ 不通過
3	系統應檢查 CA 本身憑證確為 Root CA 所簽發的憑證（至少需檢查憑證的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CA 本身憑證的簽章)	☐ 通過 ☐ 不通過

內容說明

- 伺服器端之金鑰一旦外洩，則加密機制視同無效，嚴重危害系統之機密性，故應訂定相關作業標準或管理規範，以妥善保護金鑰。應依據金鑰產生、分配、儲存、存取及銷毀之要求，實作應有之安全控制措施，確保金鑰機密性、完整性及可用性。
- 資通系統使用政府核發之憑證時，建議可依照GCP政府憑證入口網(https://gcp.nat.gov.tw)提供之「公鑰憑證安全性檢查表」，驗證各項目之檢查機制，以確保身分認證或數位簽章之安全性，使用範例詳見圖。

佐證資料

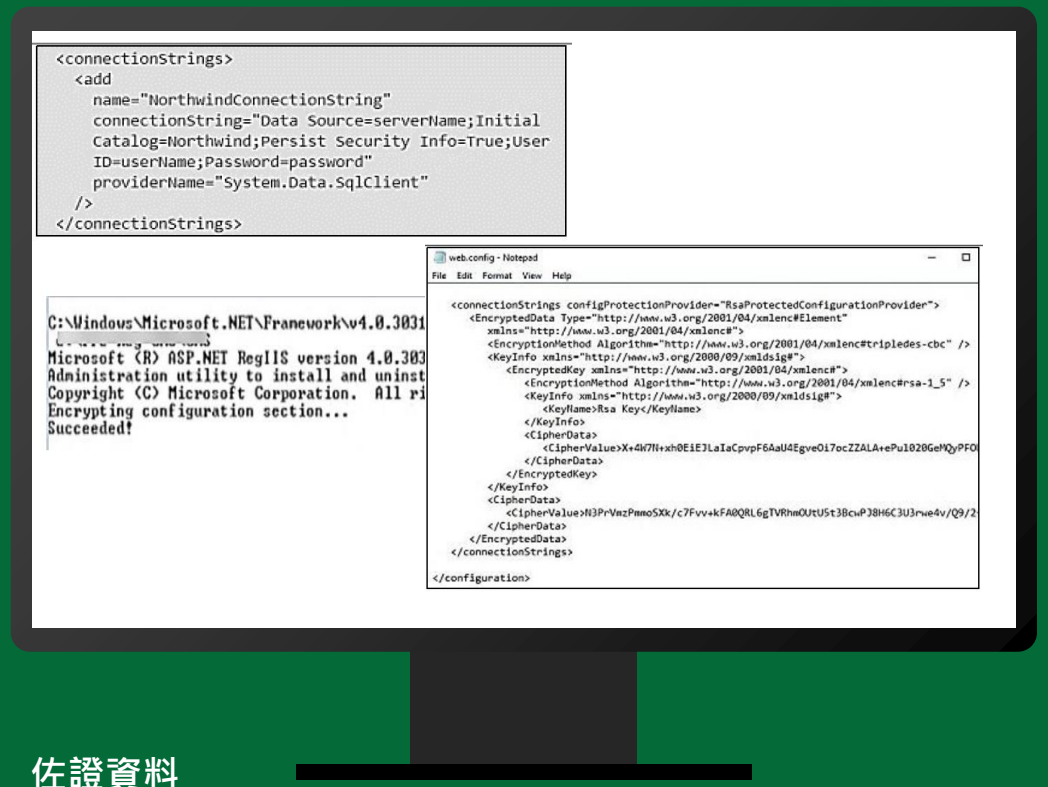
- 組織訂定之系統發展維護辦法
- 組織訂定之金鑰管理規範

勤業眾信版權所有 保留一切權利

系統與
通訊保護

第二十二條(傳輸之機密性、完整性與資料儲存安全)

九、第一類組織之核心系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。



佐證資料

- 組織訂定之系統發展維護辦法
- 資通系統組態設定檔

內容說明

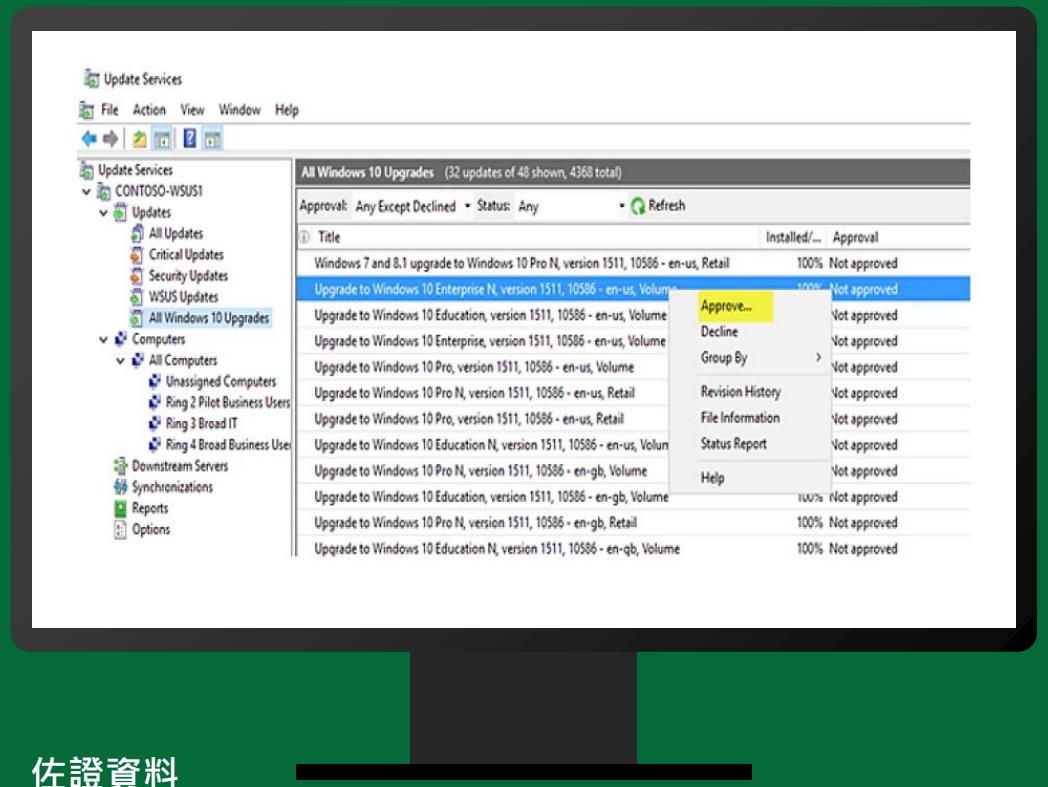
- 資通系統常利用組態設定檔案記錄一些於運作過程中會使用參數，這麼做可免除將參數值寫死於應用程式程式碼內，造成後續維護變更困難。惟其中可能包含資料庫連線位址資訊與連線帳號密碼等機密資訊，這些資訊若以明文形式保存，一旦外洩就有可能造成資通系統被惡意入侵，危害整個資通系統的安全性，而透過加密保護，則可有效降低機密資訊外洩風險。

- 實務上依照開發框架及軟體元件的不同，可能支援對整個組態設定檔案加密機制，或是針對其中特定參數進行加密保護，如僅加密資料庫連線字串等。以.NET應用程式為例，組態檔是標準 XML格式檔案，其資料庫連線字串會寫於web.config組態檔案內，並透過<connectionStrings>元素進行設定，範例詳見圖。

勤業眾信版權所有 保留一切權利

第二十三條(漏洞修復)

一、組織對於資通系統之漏洞檢測應以全部資訊資產為原則，漏洞修復應測試有效性及潛在影響，並定期更新。



佐證資料

- 組織訂定之系統發展維護辦法
- 弱點掃描、滲透測試及源碼掃描等安全檢測報告與修補紀錄

內容說明

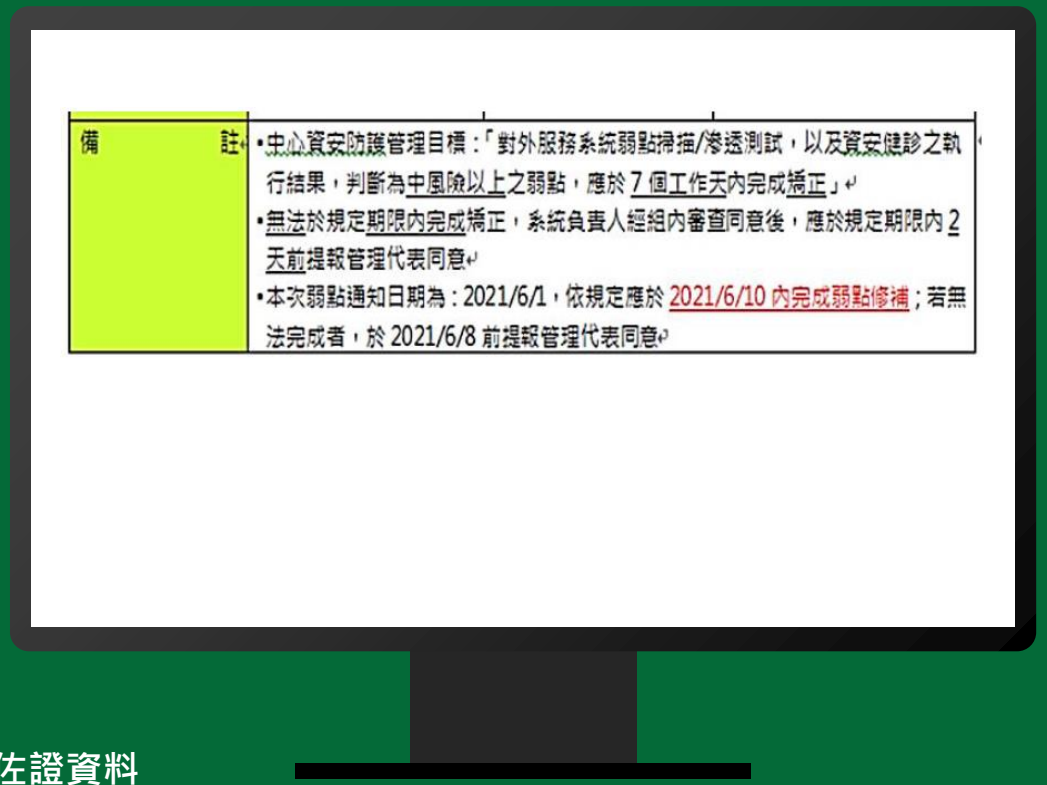
- 應定期進行軟體元件漏洞修復與更新，包含作業系統、資通系統伺服器、開發框架，以及第三方函式庫等軟體元件。例如，以WSUS管理派送安裝Windows作業系統更新，範例詳見圖。
- 系統管理者應確認作業系統等相關修正或更新程式對資通系統之影響，建立技術脆弱性資訊取得管道，評估可能帶來風險，以免貿然在正式環境套用修補程式或更新元件版本，可能因相容性問題而造成對系統服務運作產生預期外影響。例如，先於測試環境套用更新程式，確認不會對系統服務造成危害後，始於正式環境進行更新。惟當發生重大安全弱點，為爭取修補時效可能無法執行全面性測試，建議仍應測試主要功能流程未受影響後，再進行修補更新。

勤業眾信版權所有 保留一切權利

系統與
資訊完整性

第二十三條(漏洞修復)

二、組織應定期確認資通系統相關漏洞修復之狀態，應針對所發現漏洞之風險高低及是否對外提供服務，設定修補期限，未修補前應加強防護及異常偵測，以確保弱點管理之即時性及有效性。



備註	•中心資安防護管理目標：「對外服務系統弱點掃描/滲透測試，以及資安健診之執行結果，判斷為中風險以上之弱點，應於 7 個工作天內完成矯正」 •無法於規定期限內完成矯正，系統負責人經組內審查同意後，應於規定期限內 2 天前提報管理代表同意 •本次弱點通知日期為：2021/6/1，依規定應於 2021/6/10 內完成弱點修補；若無法完成者，於 2021/6/8 前提報管理代表同意

內容說明

- 注意相安全漏洞訊息(如透過CVE相關訊息網站、廠商安全通告等)，若發現採用之軟體或元件具有安全漏洞，或是由弱點掃描等安全性檢測所檢出之系統漏洞，皆應設法修復並定期追蹤修復進度，並配合定期之安全性檢測確認複測。定期確認資通系統相關漏洞修復之狀態範例詳見圖。

佐證資料

- 組織訂定之系統發展維護辦法
- 弱點掃描、滲透測試及源碼掃描等安全檢測報告
- 弱點修補紀錄

勤業眾信版權所有 保留一切權利

第二十四條(資通系統監控)

一、如發現資通系統有被入侵跡象時，應通報組織特定人員。

6.2 系統監看異常通報

由戰情室監控人員透過資安事件管理平台監控本中心資安設備事件日誌，包含網域主機、防火牆、入侵偵測系統及防毒系統等，若系統有異常事件發生，則依矯正及預防措施程序通報處理。

內容說明

- 應建立資通安全通報機制(如正式之通報程序及資安事件通報聯絡人等)，當發現資通系統遭不當存取、竄改、毀損等疑似入侵攻擊跡象時，可透過當面告知、電話、簡訊、電子郵件訊息等適當聯絡方式，通知相關人員進行適當處理，人員通知表列包含網路管理者、系統管理者、系統擁有者或各級資安人員等。監控通報作業規範範例詳見圖。

佐證資料

- 組織訂定之監控作業程序
- 組織訂定之通報應變作業程序

勤業眾信版權所有 保留一切權利

第二十四條(資通系統監控)

二、組織應監控核心系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用，非核心系統宜進行監控。

內容說明

- 資通系統之監控能力可透過各種工具與技術達成(如Web應用程式防火牆、入侵偵測系統、入侵防禦系統、惡意程式碼防護軟體、掃描工具，日誌監控軟體、網路監控軟體等)。系統連線監控工具使用範例詳見圖。

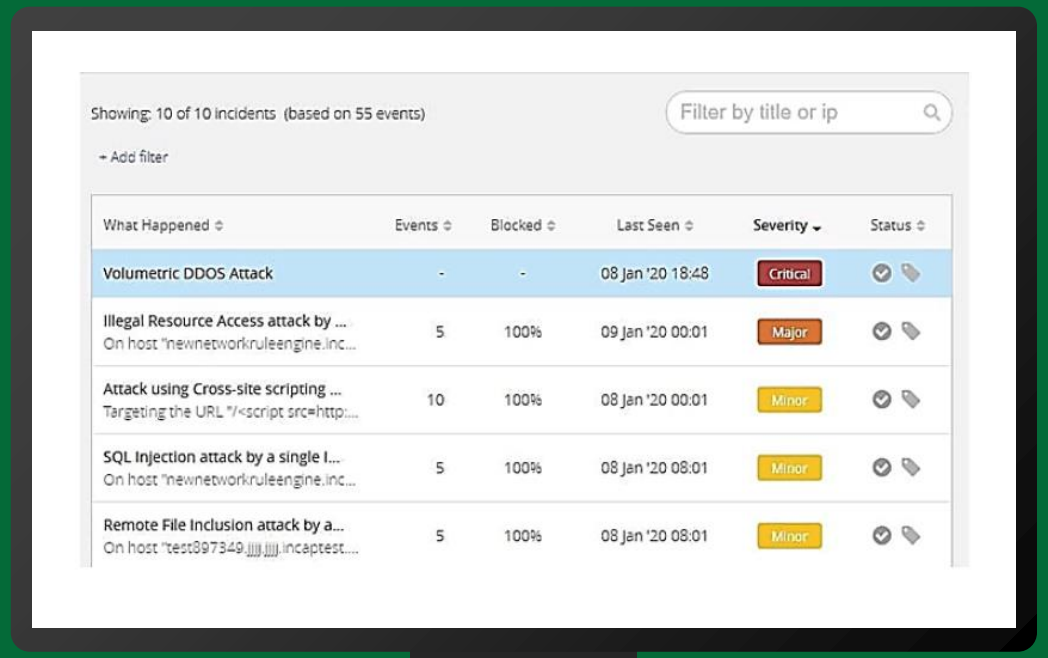
佐證資料

- 組織訂定之監控作業程序

勤業眾信版權所有 保留一切權利

第二十四條(資通系統監控)

三、核心系統宜採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。



內容說明

- 宜採用自動化工具，以支援近乎即時之事件分析。自動化工具包含基於主機、基於網路、基於傳輸，或基於儲存的事件監控工具或安全事件/資訊管理(SIEM)技術，提供即時分析警示或透過組織資通系統產生通知，如部署IPS、IDS、WAF及UTM防火牆等具備自動化監控能力之網路安全防護產品。以WAF偵測並分析資安事件範例詳見圖。

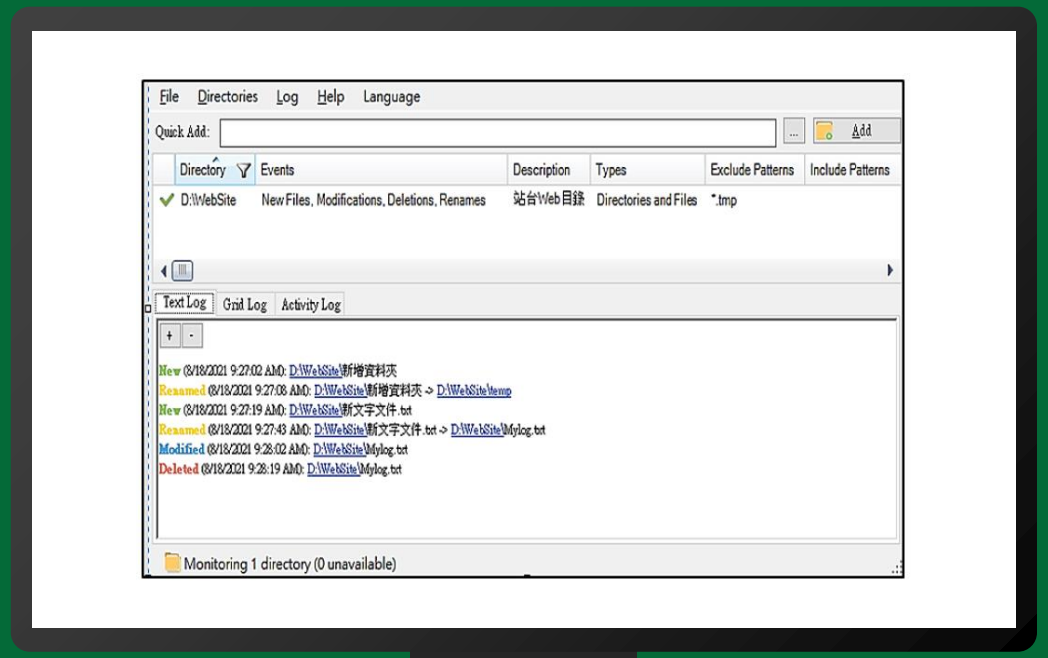
佐證資料

- 組織訂定之監控作業程序
- 資安事件分析紀錄

勤業眾信版權所有 保留一切權利

第二十五條(軟體及資訊完整性)

四、核心系統應使用完整性驗證工具，以偵測未授權變更特定軟體及資訊，非核心系統宜使用完整性驗證工具。



佐證資料

- 組織所使用之完整性驗證工具，如檔案雜湊值等

內容說明

- 資通系統軟體及資訊，包含應用程式、網站重要目錄與組態設定檔等，皆是惡意攻擊者最喜愛目標，如植入惡意檔案或竄改網頁內容等手法，破壞資通系統完整性。應使用適當技術與工具，檢查重要軟體及資訊內容是否被惡意竄改。
- 完整性檢查技術如使用密碼雜湊函數、同位元檢查及循環冗餘檢查等。亦可評估採用目錄檔案監控工具，可自動偵測應用程式與網站目錄或檔案的異動事件，當發現檔案異動時會留下相關日誌紀錄並提出示警。目錄檔案監控工具操作畫面範例詳見圖。

勤業眾信版權所有 保留一切權利

第二十五條(軟體及資訊完整性)

二、核心系統使用者輸入資料合法性檢查應置放於應用系統伺服器端。

```
<%@ language="C#" %>
<form id="form1" >
    <asp:TextBox ID="txtName" />
    <asp:Button ID="btnSubmit"  Text="Submit" />
    <asp:RegularExpressionValidator ID="regexpName"
                                    ErrorMessage="This expression does not validate."
                                    ControlToValidate="txtName"
                                    ValidationExpression="^[a-zA-Z'.\s]{1,40}$" />
</form>
```

內容說明

- 資通系統應檢查使用者輸入之有效語法與語義(如字元集、長度、數值範圍及可接受值等)，驗證輸入匹配指定之定義格式及內容。若資通系統接受惡意攻擊者提供之輸入而構成不正確編碼之結構化訊息，則該攻擊者可能插入惡意命令或特殊字元，導致資料被解釋為控制資訊或中繼資料。因此，模組或元件接收受污染輸出將會執行錯誤操作，或無法正確地解釋資料。傳遞到解譯器前預審輸入資料，可防止內容無意地被解釋為命令。

佐證資料

- 系統功能規格書
- 資通系統輸入合法性檢查之測試紀錄

勤業眾信版權所有 保留一切權利

第二十五條(軟體及資訊完整性)

三、資通系統發現於違反完整性時，應實施組織指定之安全保護措施。

內容說明

- 當發現資通系統完整性遭受破壞，如當發現資料庫或檔案被不當竄改、網站頁面被惡意置換、被植入惡意指令碼或元件等資安事件時，應依照我國資安法規及組織資安政策規範採取適當行動，如進行事件通報、緊急應變與災後復原等相關安全保護措施。例如，當組織業務承辦人員發現系統被植入惡意內容，破壞系統完整性，依規定進行資安通報，國家資通安全通報應變網站操作範例詳見圖。

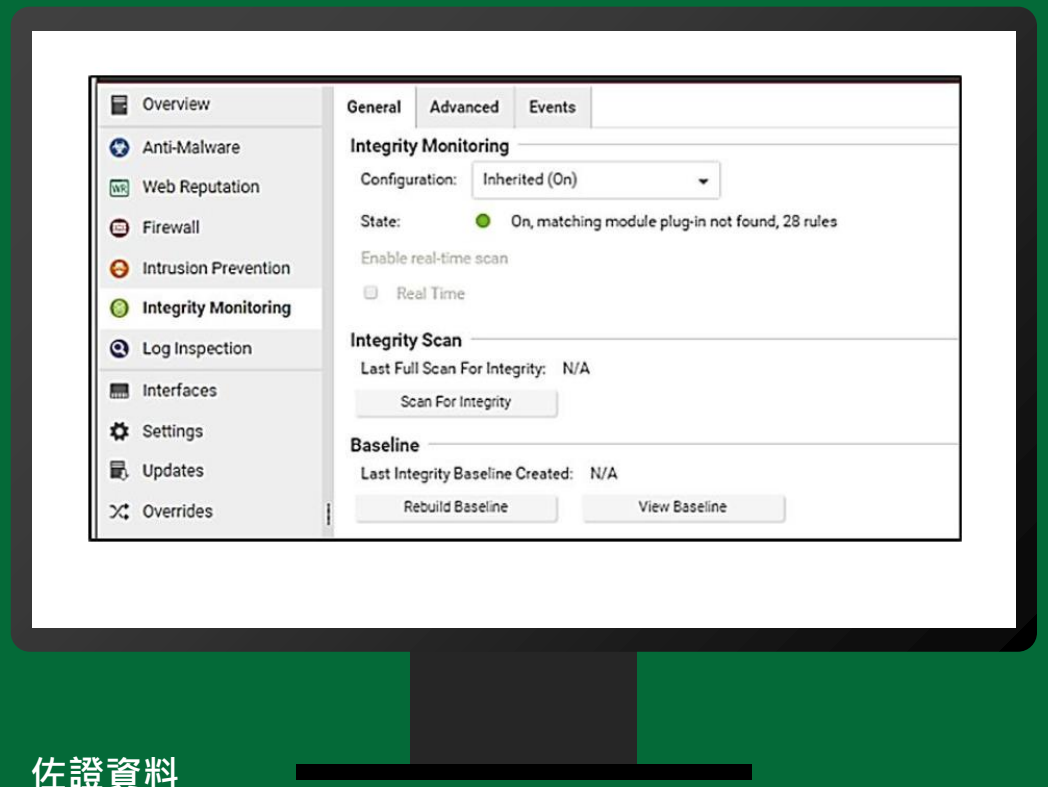
佐證資料

- 組織訂定之系統發展維護辦法
- 組織訂定之通報應變作業程序
- 組織訂定之監控作業程序

勤業眾信版權所有 保留一切權利

第二十五條(軟體及資訊完整性)

四、第一類組織之核心系統宜定期執行軟體與資訊完整性檢查。



內容說明

- 定期驗證軟體與資訊之完整性，以發現未經授權竄改行為，如透過即時偵測、進行雜湊值比對等方式，定期驗證內容是否遭到未授權之變更。實務上常先建立基準線(Baseline)，意即將軟體與資訊的初始狀態記錄下來，作為後續在進行完整性驗證檢查時比對依據。目前市面上存在多款完整性監視與驗證軟體，除可即時偵測檔案目錄異動行為，亦支援完整性掃描動作，比對檔案現況與基準線的落差，完整性掃描操作範例詳見圖。

佐證資料

- 組織訂定之系統發展維護辦法
- 完整性檢查執行紀錄

勤業眾信版權所有 保留一切權利

問題與討論

勤業眾信版權所有 保留一切權利

Deloitte.

勤業眾信

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the“Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2022 Deloitte Asia Pacific Services Limited.