

政風人員 資訊使用管理稽核作業指引



臺北市政府政風處
中華民國 111 年 5 月

第二版編輯說明

為落實資訊安全維護，提升資訊使用管理稽核執行效能，本處前於 109 年 9 月編印「政風人員資訊使用管理稽核指引手冊」。期間歷經資通安全管理法及其子法等法規修正、本府訂定資通安全相關作業指引，及近期行政院資通安全政策指示等變動。為使政風人員掌握最新資通安全資訊，提升機關資訊安全維護工作，爰修訂再版。

本次修訂部分包括：基本法規、資通安全責任等級、個人資料保護與管理、資訊資產管理等內容，另納入其他主管機關政風機構辦理資訊使用管理稽核發現問題，新增「資訊使用管理稽核常見違失態樣」，以豐富手冊內容並增進其實用性。

本指引手冊匯集行政院近期資安政策、中央法規、本府相關作業規範、各種資訊稽核常見缺失態樣及其改善措施，期能提供最新及貼近實務之資訊，成為機關辦理資訊機密維護業務之有利工具書。

臺北市政府政風處謹識

中華民國 111 年 5 月

目錄

壹、 稽核小知識	1
◆資訊稽核類型	2
一、 資訊安全稽核	2
二、 資訊使用管理稽核	2
三、 兩者區分	2
◆法規依據	3
一、 中央法規	3
二、 地方法規	4
◆稽核要領	5
一、 稽核流程	5
二、 稽核發現類型	5
三、 稽核手法	6
◆資安事件案例研析	7
一、 某機關電腦及公務信箱遭駭客入侵	7
二、 某機關伺服器主機遭駭客入侵案例	9
三、 機關網站公開機密文書	10
四、 透過某搜尋網站可下載本府員工薪資資料	11
五、 學生個資誤傳學校網站	12
◆資通安全責任等級	14
一、 等級核定	14
二、 分級標準	14
三、 應辦事項	16
貳、 資訊使用管理稽核	18
◆評估機關系統風險	19
◆擬定稽核計畫	20
◆建置系統查詢軌跡紀錄檔	22
◆界定異常存取情形及建立通報機制	23

◆權限管理情形	25
◆異常查詢自動化勾稽工具	26
◆召開研商會議及起始會議	27
◆稽核項目與稽核方法.....	28
參、 資訊安全稽核	44
◆稽核項目	45
◆導入資訊安全管理系統(ISMS)情形	46
◆資安專責人員與認知訓練	49
◆存取權限與人員管理.....	52
◆個人資料保護與管理.....	54
一、 資訊安全與個資保護之關係	54
二、 個資保護規範.....	55
三、 個資保護管理制度	56
◆資訊資產管理	58
一、 法規依據	60
二、 定義	60
三、 處理原則	61
四、 採購注意事項.....	61
五、 未來政策方向.....	62
◆資訊委外安全管理.....	63
肆、 資訊使用管理稽核常見違失態樣.....	66
◆權限管理未核實	67
一、 共用帳號	67
二、 未即時註銷或變更帳號.....	67
三、 未依職務內容設定系統使用權限	68
四、 帳號未即時登出.....	68
◆非授權查詢.....	69
一、 因好奇或便宜行事以姓名查詢個資	69
二、 以檢測系統等因素使用系統	69

三、 以查詢廠商資料等因素使用系統	70
◆查詢或登入次數異常.....	71
一、 查詢次數異常	71
二、 登入失敗次數異常	71
◆異常管控機制未建立或未落實	72
一、 未建置登入失敗鎖定功能	72
二、 未建置累積使用時間或查詢筆數限制功能	72
三、 未建置查詢事由登載功能	72
四、 通報機制未能有效發揮功能	73
◆稽核作業未落實	74
一、 系統管理單位未落實稽核作業.....	74
二、 系統管理單位未依規定辦理實地抽查作業	74
三、 僅廠商具調閱使用查詢紀錄檔權限	74
四、 系統使用單位未落實內部查核作業	75
◆文書作業未確實	76
一、 未經核准即先行查詢	76
二、 未落實登載查詢紀錄簿.....	76
三、 查詢紀錄簿未定期彙陳首長核閱	76
四、 未保存系統權限異動書面資料.....	77
◆其他違失情事	78
一、 系統環境未實體隔離	78
二、 未熟稔系統使用作業規範	78
三、 加班未辦理勤務刷卡作業	78

附錄

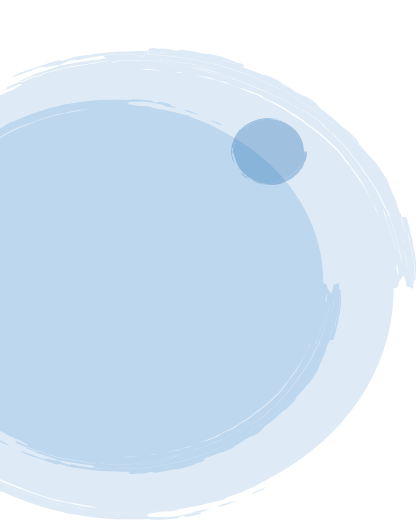
常用資安名詞.....	79
-------------	----

圖目錄

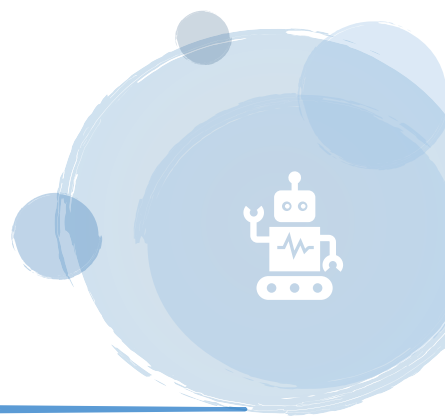
圖 1.警政日誌巨量資料分析系統介面圖	26
圖 2.系統查詢軌跡紀錄範例.....	30
圖 3.資訊系統登入紀錄查詢頁面範例	31
圖 4.資訊系統資料庫備份畫面範例.....	31
圖 5.磁帶存放紀錄表範例	32
圖 6.行政院資通安全處訂定新進人員資安宣導單(範本)	52

表目錄

表 1.資訊稽核比較表.....	2
表 2.系統風險評估指標表	19
表 3.政風機構協助機關 (構) 推動資訊使用管理稽核實施計畫.....	20
表 4.系統查詢軌跡紀錄檔工作項目表	22
表 5.異常存取情形項目表	23
表 6.權限管理情形項目表	25
表 7.系統取限管理項目表	25
表 8.事件日誌與可歸責性之措施內容	28
表 9.系統登入次數異常參考指標表.....	34
表 10.登入系統查詢時段異常指標表	36
表 11.系統使用時間異常指標表.....	39
表 12.查詢筆數異常指標表	40
表 13.第三方驗證機構清冊	46
表 14.資訊系統清冊	47
表 15.資訊系統安全等級評估表.....	48
表 16.各級機關資通教育訓練要求時數表.....	50
表 17.個資保護維護措施.....	56
表 18.ISO/IEC 27701 個人資訊管理系統不可排除適用事項	57



壹、稽核小知識



資訊稽核類型

一、資訊安全稽核

資訊安全稽核，係由各機關資訊單位主導，針對機關之資訊安全管理，包括資訊資產管理、人員安全、實體安全、網路安全及系統安全等環節，並結合資通安全管理系統 ISMS 認證項目，進行全方面檢視。依稽查方之不同，可分為第一方稽核（組織內部）、第二方稽核（客戶、委外廠商）及第三方稽核（外部組織）。

二、資訊使用管理稽核

資訊使用管理稽核，係由各機關政風室主導，資訊單位提供技術支援，關注的層面為系統存取，主要稽核項目為系統查詢軌跡紀錄檔保存情形、系統存取異常情形、建立異常狀況通報機制。辦理時機得併同前述資訊安全稽核作業，亦得由政風室自行簽報計畫辦理。

三、兩者區分

易言之，「資訊使用管理稽核」只是「資通安全稽核」的一個環節，卻是政風人員維護機關資訊安全的重要工作。

表 1. 資訊稽核比較表

項目 / 名稱	資訊安全稽核	資訊使用管理稽核
主責單位	資訊單位	政風單位
稽核重點	技術面	異常存取情形
辦理法源	資通安全管理法及本府相關資通安全規範	臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定

法規依據

一、中央法規

- (一)資通安全管理法
- (二)個人資料保護法
- (三)資通安全管理法施行細則
- (四)個人資料保護法施行細則
- (五)資通安全責任等級分級辦法
- (六)附表九資通系統防護需求分級原則
- (七)附表十資通系統防護基準
- (八)資通安全事件通報及應變辦法
- (九)資通安全管理法及子法彙編(110年9月版)
- (十)資通安全管理法FAQ(111年5月23日版)
- (十一)政風機構人員設置管理條例
- (十二)政風機構維護公務機密作業要點
- (十三)政風機構協助機關(構)推動資訊使用管理稽核實施計畫

二、地方法規

- (一)臺北市政府及所屬各機關辦理資訊使用管理稽核作業規定
- (二)臺北市政府資通安全管理規定
- (三)臺北市政府網路管理規範
- (四)臺北市政府員工使用資通訊裝置應注意事項
- (五)臺北市政府資通系統安全作業指引(111年2月24日施行)
- (六)臺北市政府資通訊資產及電子資料安全作業指引(111年2月24日施行)
- (七)臺北市政府資通安全事件通報及應變作業指引(111年2月24日施行)
- (八)臺北市政府使用物聯網安全作業指引(111年2月24日施行)
- (九)臺北市政府資通訊業務委外作業指引(111年2月24日施行)

稽核要領

一、稽核流程



二、稽核發現類型

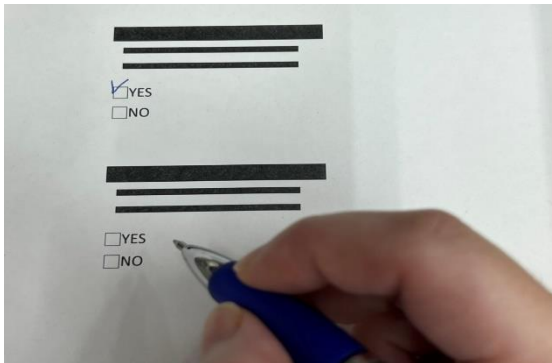
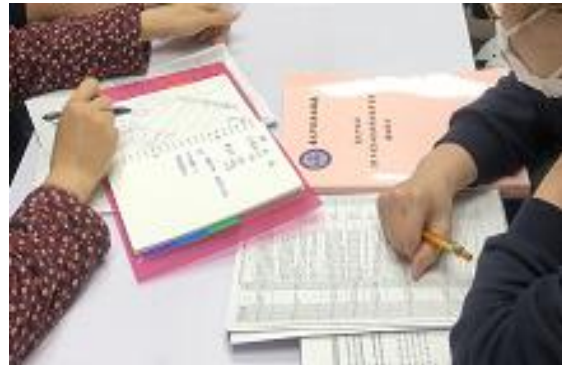
主要不符合事項 (Major Nonconformity)	<ol style="list-style-type: none">1.管理制度、程序或控制措施的完全失效或未執行2.極高數量缺失事項集中某一控管點或單位3.重大資訊安全風險並未被鑑別及檢討改善4.存在明顯立即資訊安全損失的風險
次要不符合事項 (Minor Nonconformity)	<ol style="list-style-type: none">1.管理制度中某一特定的要求並未被履行2.違反管理安全政策、規範、管理要點、程序之要求3.違反系統程序或工作程序指示
觀察事項 (Observation)	<ol style="list-style-type: none">1.較輕微之缺失事項2.欲查核但目前無紀錄可進行查核之事項3.無直接證據指出為次要不符合事項，但予以記錄，於半年或一年後持續觀察
改善機會 (Opportunity for Improvement)	<ol style="list-style-type: none">1.建議未來可持續改進之事項2.改善管理系統有效性之建議措施

三、稽核手法

(一) 人員訪談

有效溝通++

5W1H 原則



(二) 問卷

適合量化

結合訪談

(三) 文件紀錄查核

事前提供

風險控制



(四) 自動化工具

簡化稽核

e 化管理

資安事件案例研析

一、某機關電腦及公務信箱遭駭客入侵

(一) 案例大要

某縣市政府於 108 年間，疑似遭駭客利用 AD 派送客製化惡意程式到特定單位，進行資料竊取，並為躲避追查，抹除受駭系統稽核紀錄。

(二) 手法分析

1. 某機關透過防毒軟體偵測到多台電腦存在 APT(進階持續攻擊) 惡意程式，將使用者所「開啟」的文件上傳到 google drive。
2. 同仁電腦遭植入惡意程式，駭客掌握電子郵件信箱的帳號密碼，並利用網頁郵件 (WebMail) 登入使用者帳號，設定郵件轉寄，藉以取得相關郵件往來資訊。
3. 機關在伺服器的系統記憶體中發現惡意程式以注入記憶體之攻擊方式，使各家防毒軟體幾乎無法掃描發現，並更改防毒軟體等主機之路由設定表 (Routing Table)，將連主機的路由器指向主機自己，導致掃描結果無法回傳，增加比對難度。
4. 駭客入侵維運系統主機，掌握系統管理者帳號及密碼，以帳號連線市府 VPN 主機，將廠商帳號預設通知信箱竄改，再以管理者帳號遠端登入備用防毒

主機。

- 5.本案發現共同特徵是無線路由器遭駭客開啟 VPN 功能，建立 VPN 帳號及虛擬伺服器，駭客使用工具掃描有漏洞之無線路由器，利用國人並無更新無線路由器韌體之習慣，進行攻擊。

(三)機關防處作為

- 1.依契約約定裁罰維運廠商，修訂維運工作標準作業程序，改善維運工作檢核表，導入特權帳號管理系統，強化密碼管理及側錄操作紀錄。
- 2.針對重要核心主機，全面盤點網路連線，並導入 GCB 安全組態。
- 3.針對維運人員工作站進行實體隔離，將遠端管理改為跳板主機方式管理。
- 4.按月依監控數據、情資及架構等資訊調整 SOC 規則，並將核心設備相關安全日誌納入 SOC 監控機制與日誌系統。
- 5.補強骨幹或機敏網路區域偵測設備，將曾出現的惡意程式更新至防毒系統病毒碼。
- 6.持續強化公務電子信箱，增加 APT 惡意程式防護阻擋機制，關閉自動轉寄功能並提升加密傳輸方式。
- 7.收容全部公務電子郵件系統，集中執行資安防護與監控管理。
- 8.辦理紅隊演練(Red Team Assessment ; 在不影響

營運前提下進行模擬入侵攻擊)。

(四)結語

目前許多駭客中繼站之上層攻擊來源 IP 多來自中國網軍駭客組織所為，主要蒐集我國政府之人事、政策規劃、科研計畫及智庫資料，請各政風機構協調機關相關單位落實管理者帳號保管及強化密碼管理，確實掌握維運廠商的管理及資安狀況，持續檢視機關資安作為之執行情形，以有效防範駭客以公務電子郵件進行社交工程攻擊等情事。

二、某機關伺服器主機遭駭客入侵案例

(一)案例大要

某機關伺服器於 109 年間遭駭客入侵，下載惡意工具並插入資料表，嘗試以持續性連線及漏洞工具進行後續攻擊。

(二)手法分析

- 1.駭客利用 SQL 注入攻擊伺服器中舊網站語法漏洞並開啟 XP_CMDSHELL 功能取得控制權。
- 2.主機資料庫帳號之密碼為弱密碼，駭客取得帳號權限後下載惡意工具，藉此進行進一步攻擊。
- 3.駭客於資料庫插入資料表，內容皆為系統錯誤訊息。

(三)機關防處作為

- 1.重新檢視並移除該伺服器網站資料夾內無使用之

- 檔案，防止駭客利用舊網頁之漏洞進行攻擊。
- 2.以讀取資料庫權限最小之帳號執行對外連線，避免資料庫遭竄改或破壞。
 - 3.每季變更所有資料庫密碼，且須符合複雜度及資安規範，並留存紙本紀錄備查。
 - 4.要求系統維護廠商每季提供各系統弱點掃描報告，如有發現中、高級以上問題，即時完成修補作業。
 - 5.開啟 SQL 稽核紀錄功能，以利未來資安事件調查使用。

(四)結語

機關所屬閒置或不再使用之資訊系統、網站，資安措施或維護管理可能未盡完善，進而成為資安漏洞及攻擊目標，提醒各機關確實依資通安全責任等級分級辦法第 11 條第 2 項規定清查機關所使用網站與系統，並落實相關資安防護措施。

三、機關網站公開機密文書

(一)案情摘要

某機關承辦人認所承辦之機密文書內容僅係函釋法令說明，實質上未涉及機敏性，逕行將該機密文書公告於機關網站，惟查該機密文書解密條件尚未成就，亦未辦理解密程序，爰依臺北市政府文書處理實施要點規定，仍應辦理保密措施。

(二)涉及法規

- 1.刑法第 132 條第 1 項。
- 2.臺北市政府文書處理實施要點第 69 點、第 70 點、第 83 點第 1 項第 3 款及第 5 款。

(三)改進措施及建議作法

- 1.機關應加強宣導機密文書保密概念及洩漏公務機密責任，避免因法治概念認知不足，致罹刑章。
- 2.機密文書受文機關如認該機密文書無保密之必要，仍應依臺北市政府文書處理實施要點第 83 點第 1 項第 3 款及第 5 款規定完成解密程序。
- 3.機關網站資料公告應有審核機制或公告作業程序進行把關，以免影響機關形象。

四、透過某搜尋網站可下載本府員工薪資資料

(一)案情摘要

某機關人員於入口網站搜尋機關新聞，發現可查詢本府員工薪資資料，經查該系統建置年代較久，資安防護較弱，且系統主機置於 DMZ 區，雖有設置使用者帳號密碼登入機制，且系統查詢資料連結原僅有系統使用者可得知，卻因為該搜尋網站將個人搜尋紀錄與公開搜尋結果混合，使外界可透過該搜尋網站連結至表單。

(二)涉及法規

- 1.刑法第 318 之 1 條、第 359 條。
- 2.個人資料保護法第 16 條、第 18 條、第 28 條。

(三)改進措施及建議作法：

- 1.設置系統防火牆及存取控制白名單。
- 2.下載報表資料程序，設置帳號密碼機制或防止螢幕輸出等安全控管機制。
- 3.老舊系統資安防護不足，重新盤點機關老舊系統並進行健診，檢測是否存有資安風險；針對具大量個資之系統進行滲透測試，依檢測結果進行改善修補。

五、學生個資誤傳學校網站

(一)案情摘要

透過搜尋引擎，可下載某校學生個資(姓名、班級、身分證字號、生日、聯絡方式等個人資料)，查係該校於網站之最新消息公告中，不慎夾帶含有學生個資之檔案，另該網頁目錄瀏覽功能未關閉，任何人均可透過瀏覽目錄取得機敏資料。

(二)涉及法規

- 1.個人資料保護法第 18 條、第 28 條。
- 2.臺北市政府資通系統安全作業指引。

(三)改進措施及建議作法：

- 1.機關網站資料公告應有審核機制或訂定作業程序進行把關，以免影響機關形象。
- 2.檢視機關網站之網頁瀏覽目錄權限是否為關閉狀態，避免公務機密或民眾個資外洩。
- 3.將機關伺服器移至上級機關或本府資訊局集中統一管理，提升資安防護措施，擷節資安相關經費。

資通安全責任等級

行政院衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級，相關實施辦法依據「資通安全責任等級分級辦法」辦理¹。

一、等級核定

公務機關及特定非公務機關之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級²，原則上每二年提交主管機關核定³。

若因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經其等級提交機關或核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。⁴

二、分級標準

等級	內容事項	資通安全責任等級分級辦法
A 級	1. 業務涉及國家機密。	第 4 條

¹ 依資通安全管理法第 7 條第 1 項。

² 依資通安全責任等級分級辦法第 2 條。

³ 資通安全責任等級分級辦法第 3 條參照。

⁴ 依資通安全責任等級分級辦法第 11 條第 3 項。

等級	內容事項	資通安全責任等級分級辦法
	<ol style="list-style-type: none"> 2. 業務涉及外交、國防或國土安全事項。 3. 業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。 4. 業務涉及全國性民眾或公務員個人資料檔案之持有。 5. 屬公務機關，且業務涉及全國性之關鍵基礎設施事項。 6. 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。 7. 屬公立醫學中心。 	
B 級	<ol style="list-style-type: none"> 1. 業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。 2. 業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。 3. 業務涉及區域性或地區性民眾個人資料檔案之持有。 4. 業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。 5. 屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。 6. 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、 	第 5 條

等級	內容事項	資通安全責任等級分級辦法
	區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。 7. 屬公立區域醫院或地區醫院。	
C 級	各機關維運自行或委外設置、開發之資通系統者。	第 6 條
D 級	各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者。	第 7 條
E 級	<ol style="list-style-type: none"> 1. 無資通系統且未提供資通服務。 2. 屬公務機關，且其全部資通業務由其上級機關、監督機關或上開機關指定之公務機關兼辦或代管。 3. 屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關或出資之公務機關兼辦或代管。 	第 8 條

三、應辦事項

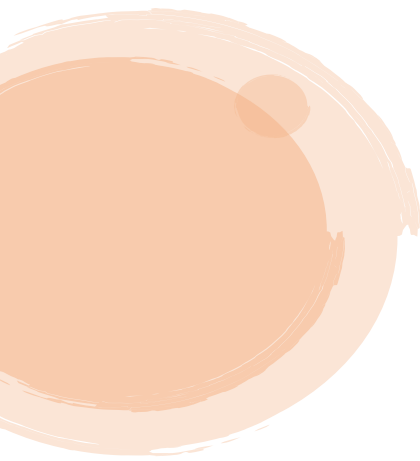
各機關應依其資通安全責任等級，辦理資通安全責任等級分級辦法附表一至附表八之事項⁵，詳細內容請參閱資訊安全防護基準檢核表。

各機關自行或委外開發之資通系統應依資通安全責任

⁵ 依資通安全責任等級分級辦法第 11 條第 1 項。

等級分級辦法附表九所定資通系統防護需求分級原則完成資通系統分級，並依同辦法附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理⁶。

⁶ 依資通安全責任等級分級辦法第 11 條第 2 項。



貳、資訊使用管理稽核



評估機關系統風險

為協助機關強化資通安全管理機制，防範公務機密外洩，建議先審視機關主要業務項目，確認機關之核心業務資訊系統標的及其使用情形、作業管理規定是否有相關稽核規範等，茲提供幾項要點供分析判斷：

表 2.系統風險評估指標表

要點	範例說明
資訊系統有無涉及機敏資料	涉及公務機密資料系統之使用查詢情形，應有適當之審查或稽核機制。
資訊系統有無涉及全國性、區域性或地區性之關鍵基礎設施事項	水費水表營收系統、水庫水文監測系統、交通監控系統。
資訊系統有無涉及民眾個人資訊之資料庫	地方稅務系統、戶役政系統、不動產地籍系統。
是否每年有中央目的事業主管機關定期考核系統使用情形	警政署 - 警政知識聯網、財政部 - 稅務系統、內政部 - 戶役政及地籍系統。
調閱 系統盤點清冊 加以瞭解機關使用系統概況	資訊系統安全等級、是否為共用性系統、承辦（管理）單位及維運廠商。
調閱系統之 安全等級評估表	瞭解系統之影響構面、等級評估及原因說明。
調閱系統資訊安全稽核規定(或資訊安全政策、系統作業手冊等)	瞭解稽核頻率、範圍及方法等。

擬定稽核計畫

依法務部廉政署 108 年 2 月 23 日廉政字第 10807003420 號函附「政風機構協助機關(構)推動資訊使用管理稽核實施計畫」執行原則，各政風機構得依實際情形訂定執行內容如下：

表 3.政風機構協助機關(構)推動資訊使用管理稽核實施計畫

機關全銜 ○○年度資訊使用管理稽核實施計畫	
項目	內容說明
壹、依據	一、政風機構人員設置管理條例第 4 條第 7 款。 二、政風機構人員設置管理條例施行細則第 10 條第 3 款。 三、政風機構維護公務機密作業要點第 14 點、第 15 點規定。 四、各資訊系統作業規定。
貳、目的	為協助各機關(構)強化資通安全管理機制，防範公務機密外洩，確保資料、系統、設備及網路安全，特訂定本計畫。
參、任務編組	由各政風機構結合機關(構)資訊單位按本機關(構)實際分工與職掌，辦理資訊使用管理稽核作業。
肆、稽核時機	結合各機關(構)依資通安全責任等級分級辦法規定之次數，辦理內部資通安全稽核。
伍、稽核範圍	某區間之系統查詢相關紀錄。
陸、受稽核單位及人員	系統管理者、使用單位及人員。

機關全銜
〇〇年度資訊使用管理稽核實施計畫

項目	內容說明
柒、稽核方式（作業程序）	依系統使用特性，調閱系統查詢紀錄檔及相關比對資料，並得運用文書審核、人員訪談、量化統計、自動化工具等方式進行稽核。
捌、工作內容及要領	本項說明詳如後述。
玖、結果處理	<p>一、各項稽核未盡事宜、改善意見，於稽核後彙整簽報機關(構)首長或其授權人員，並將建議事項移請相關單位檢討改善或參處，另藉由機關安全維護會報或相關會議，主動追蹤管考專案稽核所見缺失事項之改善情形。</p> <p>二、發現重大事件恐肇生資安事件之虞者，簽報機關(構)首長或其授權人員核定後，追究相關責任，通知限期改善，並於機關安全維護會報或相關會議適時報告。</p>
拾、行政支援事項	<p>一、各政風機構協助辦理稽核作業得調閱有關資料、實地測試或檢查資訊軟、硬體設備使用情形，並請各受稽核單位相關人員提供說明。</p> <p>二、受稽核單位、個人對於稽核人員實施稽核時，應充分配合執行。</p>
拾壹、保留條款	本計畫如有未盡事宜，得隨時修正。

建置系統查詢軌跡紀錄檔

在電腦領域，系統查詢軌跡紀錄檔 (Log file) 是一個記錄了發生在執行中的作業系統或其他軟體中事件的檔案，許多作業系統、軟體框架和程式都包含紀錄檔系統。

依「政風機構協助機關(構)推動資訊使用管理稽核實施計畫」第 5 條第 1 項，相關工作內容如下：

表 4.系統查詢軌跡紀錄檔工作項目表

項次	工作內容
1	系統應建置、啟動、處理及保留使用者紀錄檔，如紀錄檔資料不足以作為稽核管理使用，得協調另行開發或購置進階之管理工具。
2	系統查詢軌跡紀錄檔應處於啟動狀態，並應定期備份轉出檔案後保存，使其具有連貫性，以作為日後調查及監督之用。
3	系統查詢軌跡紀錄檔應指定專人定期及日常檢視，並做成書面紀錄備查。
4	應依規定確保使用者紀錄檔之建置與保存，俾利查察違規使用、越權查閱、下載資訊等異常情事，並就資通安全漏洞研採補救與防範措施，以及追究相關法律或行政責任，以有效防止公務機密資訊外洩。

界定異常存取情形及建立通報機制

界定異常存取情形及建立異常通報機制之目的，是為篩選可能存有缺失之查詢情形，以提升抽樣及實地稽核之效率，即時掌握異常事件，並即時處理；**列為異常存取情形並非即屬缺失**，仍需請使用者說明、提供查詢依據佐證等資料綜合判斷。

依政風機構協助機關(構)推動資訊使用管理稽核實施計畫第 5 條第 2 項、第 4 項、第 5 項第 1 款，得就機關(構)現有資通系統特性及運作現況，界定以下例示之系統存取異常狀況及建構相關通報機制，並協調資訊單位即時或按月彙送系統存取異常狀況報表供政風機構進行瞭解：

表 5.異常存取情形項目表

項目	內容
系統登入	1.登入失敗次數異常頻繁。 2.非勤務時間登入系統。 3.IP 位址異常。 4.使用他人或離職員工帳號。
使用時間	1.單次使用系統時間異常。 2.累計使用系統時間異常。
查詢異常	1.查詢筆數異常頻繁。 2.未於系統登載「案號」或「查詢事由」，或未設置「電腦查詢登記簿」。 3.查詢內容與登載之「案號」或「查詢事由」不符。 4.具系統存取特別權限者查詢筆數異常頻繁。 5.以機關首長、時事名人或公眾人物之姓名為查詢條件。

其他系統存取異常狀況	<ol style="list-style-type: none"> 1.查調三親等親屬資料。 2.假日進行資料主檔或資料庫內容異動。
將政風機構納入通報機制	將政風機構納入系統存取異常狀況之受通報單位。
落實通報機制	<ol style="list-style-type: none"> 1.前揭系統存取狀況各項管制作為是否落實。 2.系統存取異常個案是否確實通報政風機構。

權限管理情形

除針對系統使用存取行為進行稽核外，檢視系統權限開通時機及正當性，限縮使用者於必要權限之管控原則下，從源頭減少不當查詢行為。依政風機構協助機關(構)推動資訊使用管理稽核實施計畫第 5 條第 5 項第 2 款、第 3 款，權限相關稽核重點如下：

表 6.權限管理情形項目表

項目	內容
權限異動管理	退(離)職、職務異動及具特別存取權限等人員之權限之管理，檢視其申請或核准文件是否完整，及是否依規定取消或調整相關存取權限。
委外人員管理	委外廠商人員於系統存取權限辦理情形。

各政風機構得就機關現行權限管理相關規範，含新增、修改、刪除權限之作業規定及辦理情形，稽核人員得就下列項目進行查核：

表 7.系統取限管理項目表

稽核項目	內容
使用者名單	使用者權限帳號管控檢視依據，並得於名單中通盤檢視所屬人員帳號開通情形。
即時異動	新增、調動、註銷使用者帳號是否與人員實際異動時間相符。
權限之適當性	審視各使用者帳號權限開通內容之適當性。
定期清查	檢視未使用系統之使用者帳號，檢討是否有續留之必要。

異常查詢自動化勾稽工具

系統異常查詢勾稽、通報機制，可依系統使用特性、異常界定情形、稽核人力、查詢軌跡紀錄量、預算規劃等條件，審酌由系統自動化處理或整合人工審核方式辦理。

以臺北市政府警察局為例，該局使用警政知識聯網查詢數量巨大，自行研發「警政日誌巨量資料分析系統」，依系統使用特性，界定異常查詢條件及稽核範圍，可更有效率地篩選疑似異常情形，並提供資料予政風室辦理定期稽核。

圖 1.警政日誌巨量資料分析系統介面圖

召開研商會議及起始會議

各機關(構)政風室應會同使用、管理單位或稽核單位，針對前述機關風險評估、稽核計畫擬定及異常存取項目之界定等，集思廣益召開**研商會議**，共同磋商尋求共識。

至於先簽會資訊使用管理稽核計畫，或是先召開研商會議，得視機關慣例由政風室自行衡酌考量。如簽會計畫在前可讓首長及機關同仁事前透過書面資料瞭解相關資訊，幫助研商會議快速達成共識，更可適時運用機關內部會議、安全維護會報時機，提高機關首長及同仁對稽核的重視度。

起始會議(行前會議)則係於內、外部實地稽核前辦理，著重於稽核當日執行之流程與操作，就稽核人員及受稽對象，確認細部稽核範圍、稽核方法與項目、稽核所需文件與工作分配等，提升實地稽核的效率。



稽核項目與稽核方法

依法務部廉政署 108 年 2 月 23 日廉政字第 10807003420 號書函檢送「政風機構協助機關(構)推動資訊使用管理稽核項目表」，各政風機構得視機關(構)實際狀況增刪稽核項目，並結合各機關(構)現有之資通安全稽核表併同辦理，茲以範本項目進行說明：

(一)系統查詢軌跡紀錄檔(Log)

1.1 資訊單位是否有建立及啟動系統查詢軌跡紀錄檔(Log)，並保存一段時間(保存多久?)，以作為日後調查及監督之用。

因應資訊安全與法規要求，現行各機關使用之資訊系統多已建立及啟動系統查詢軌跡紀錄，然而紀錄內容是否具完整性且依相關作業規定期限妥善保存，亦需確認。依資通安全責任等級分級辦法附表十資通系統防護基準修正規定，有關控制措施構面之「事件日誌與可歸責性」規範內容如下：

表 8.事件日誌與可歸責性之措施內容

措施內容	說明
記錄事件	1.訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 2.確保資通系統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。 3.應記錄資通系統管理者帳號所執行之各項功能。 4.應定期審查機關所保留資通系統產生之日誌。
日誌紀錄內容	資通系統產生之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，採用單一日誌機制，確保輸出格式之一致性，

	並應依資通安全政策及法規要求納入其他相關資訊。
日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。
日誌處理失效之回應	<ol style="list-style-type: none"> 1.資通系統於日誌處理失效時，應採取適當之行動。 2.機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。
時戳及校時	<ol style="list-style-type: none"> 1.資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 2.系統內部時鐘應定期與基準時間源進行同步。
日誌資訊之保護	<ol style="list-style-type: none"> 1.對日誌之存取管理，僅限於有權限之使用者。 2.應運用雜湊或其他適當方式之完整性確保機制。 3.定期備份日誌至原系統外之其他實體系統。

參考文件：系統作業手冊或內部規定、系統軌跡紀錄查詢及管理頁面

編號	啟始時間	結束時間	連線時間	來源IP	流量	結束原因
1	2020-07-17 09:25:58		0秒	114	10 _IN: 0 B OUT: 0 B	
2	2020-07-16 18:00:01	2020-07-17 05:44:11	42252秒	114	10 _IN: 89.91 MB OUT: 13.77 MB	Lost-Carrier
3	2020-07-16 14:37:07	2020-07-16 17:14:30	9445秒	114	10 _IN: 76.12 KB OUT: 10.92 KB	Lost-Carrier
4	2020-07-16 14:29:06	2020-07-16 14:35:10	366秒	114	91 _IN: 15.45 KB OUT: 1.14 KB	Lost-Service
5	2020-07-15 21:18:15	2020-07-16 14:23:45	61532秒	125	216 _IN: 4.92 MB OUT: 19.62 MB	Lost-Service
6	2020-07-15 18:37:24	2020-07-15 21:17:52	9630秒	125	216 _IN: 2.77 MB OUT: 9.58 MB	Lost-Carrier
7	2020-07-15 10:14:36	2020-07-15 18:37:13	30159秒	125	216 _IN: 11.52 MB OUT: 58.33 MB	Lost-Carrier
8	2020-07-15 09:54:39	2020-07-15 10:13:50	1153秒	125	216 _IN: 299.09 KB OUT: 1.28 MB	Lost-Carrier
9	2020-07-14 18:16:28	2020-07-15 09:20:00	54215秒	125	216 _IN: 499.55 KB OUT: 1 MB	Lost-Carrier
10	2020-07-14 15:19:53	2020-07-14 16:17:44	3473秒	612	6 _IN: 3.09 MB OUT: 6.29 MB	Lost-Carrier
11	2020-07-14 11:58:07	2020-07-14 15:19:11	12066秒	612	6 _IN: 4.01 MB OUT: 7.78 MB	Lost-Carrier
12	2020-07-14 09:47:35	2020-07-14 11:57:25	7792秒	612	6 _IN: 4.15 MB OUT: 12.19 MB	Lost-Carrier
13	2020-07-14 09:23:39	2020-07-14 09:47:03	1406秒	612	6 _IN: 861.65 KB OUT: 6.67 MB	Lost-Carrier
14	2020-07-14 05:27:14	2020-07-14 09:23:13	14162秒	612	6 _IN: 100.63 KB OUT: 13.86 KB	Lost-Carrier

圖 2.系統查詢軌跡紀錄範例



圖 3.資訊系統登入紀錄查詢頁面範例

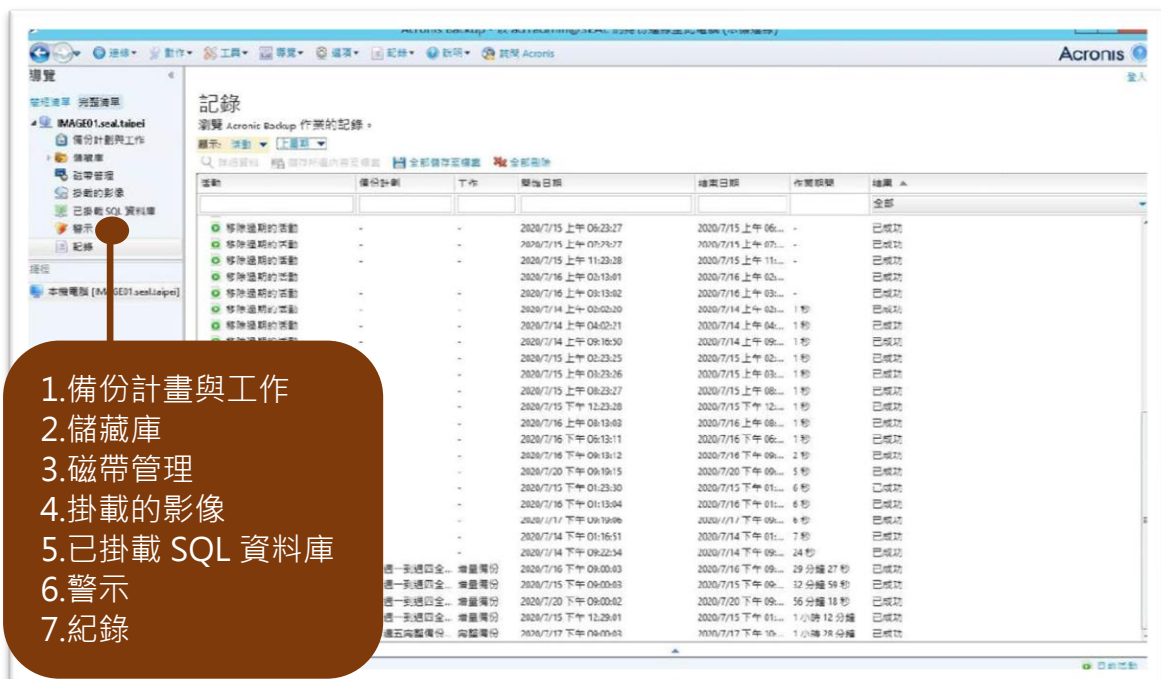


圖 4.資訊系統資料庫備份畫面範例

1.2

資訊單位系統紀錄檔，是否有定期備份轉出檔案後保存。

為避免系統查詢軌跡紀錄檔未被新資料覆蓋，確保事後得以追溯可疑異常查詢行為，應確實將系統查詢軌跡紀錄檔定期備份，並妥善保存。

參考文件：磁帶存放紀錄表(如下圖)、備份紀錄

文件類別	內部使用	磁帶存放紀錄表	文件編號	ISMS-4-007-05-1-109002
版次	V1.0			

填寫月份：2月

備份磁帶資料日期	存放日期	捲數	簽名	備份磁帶資料日期	存放日期	捲數	簽名
1	2	1	楊	16	17	1	楊
2	3	1	吳	17	18	1	楊
3	4	1	吳	18	19	1	吳
4	5	1	楊	19	20	1	吳
5	6	1	楊	20	21	1	楊
6	7	1	吳	21	22	1	楊
7	8	1	吳	22	23	1	吳
8	9	1	楊	23	24	1	吳
9	10	1	楊	24	25	1	楊
10	11	1	吳	25	26	1	胡
11	12	1	吳	26	27	1	吳
12	13	1	楊	27	28	1	吳
13	14	1	楊	28	29	1	楊
14	15	1	吳	29	31	1	楊
15	16	1	吳				

管理人員 [Redacted] 股長 [Redacted]

圖 3.磁帶存放紀錄表範例

1.3 資訊單位是否有專人隨時(經常)檢視。

此處專人非指資通安全專職人員（詳如後述），而係指特定人員之職務內容包含管理及檢視系統查詢軌跡紀錄檔者。

建議此處專人應儘量避免由系統使用者擔任，以免發生球員兼裁判之情事。

參考文件：資訊室業務職掌表、系統紀錄檔查檢紀錄與相關簽呈、實際存檔情形

(二)系統存取異常狀況情形

2.1 系統登入次數是否正常(相較一般使用習慣，系統登入次數小於____次)。

本項異常情形之界定，須審酌系統使用現況認定，與相關單位共同研商，謹就同仁職務差異、業務屬性、系統使用特性等常見指標供參考，說明如下：

表 9.系統登入次數異常參考指標表

指標	說明
同仁職務差異	如為後台承辦作業人員，同仁登入系統查詢完資料即可登出，登入次數較多；又如受理民眾洽公櫃台人員，上班時段同仁會維持系統上線以提高服務速度，登入次數較少。
業務屬性	如該業務具淡旺季性質，則不同時期登入次數可能有相當程度之差異，均屬正常情形。
系統穩定度	如果系統負載量較低（如伺服器頻寬、記憶體容量、硬體設備等因素），時常斷線易造成系統登入次數較高。
有無設定閒置時間自動下線機制	如系統設置閒置特定期間自動下線機制，則登入次數較多。
系統設定情形	簡易查詢資料之系統，登入次數較多；須線上作業之系統，登入次數較少。

2.2

系統登入失敗次數是否正常(相較一般使用習慣，連續失敗次數小於____次)。

依資通安全責任等級分級辦法附表十資通系統防護基準修正規定，有關控制措施「識別與鑑別」構面之「身分驗證管理」措施內容規定，具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。

本項異常之界定，可參考上開規定或依系統特性訂定較嚴格登入異常情形，為防止有心人士以惡意重複登入程式猜測密碼，系統應具備帳戶鎖定機制，若資訊系統未設定帳戶鎖定機制者，政風機構可依據上開規定，於稽核時機與相關單位研議設置。

參考文件：資訊系統作業規範、帳號認證及鎖定機制

2.3 登入系統查詢時段是否正常(例如於正常勤務時間登入系統)。

本項異常情形之界定，可審酌系統使用現況，與相關單位共同研商，謹就業務屬性、同仁職務差異、機關輪班需求等常見指標供參考，說明如下：

表 10.登入系統查詢時段異常指標表

指標	說明
業務屬性	適逢業務旺季，如地方稅稽徵月份，或單位人力短缺增加現有人力作業量，均會增加同仁加班機率，容易出現異常時段查詢情形。
同仁職務差異	如後台承辦作業人員，較易有加班情形；又如受理民眾洽公櫃台人員，於正常洽公時間才會登入系統。
機關輪班需求	如警察、消防機關等業務性質，同仁須全天候 24 小時輪值者，則需透過勤務分配表確認是否正常公務時間。

參考文件：系統使用查詢時段分析、查詢人員差勤紀錄

2.4 使用者系統連線電腦設備網際網路協定(IP)位址，是否正常(例如 IP 位址為使用者公務慣用之位址)。

為確認登入系統者均經授權使用者，若有非公務 IP 登入情形，均屬異常情形。

若系統已設定使用者 IP 位址白名單，並使用 IP 管理與網路存取控制工具（例如 Arpro）進行管控，則該系統僅接受白名單內之 IP 位址登入系統，已具備過濾異常 IP 位址功能。

參考文件：系統開放網域清單、機關 IP 位址清冊

2.5 使用者之帳號密碼是否沒有共用或交由他人使用情形。

資訊系統每一個帳號應具備唯一識別功能，以利該帳號使用者之查詢行為具有可歸責性，禁止使用共用帳號。

若機關有特別准許使用者共用帳號者，使用同仁應提出正當理由申請經主管核准，且管理者應定期清查共用帳號使用情形，查看有無未授權使用者登入情事。

稽核方法參考：調閱系統登入軌跡紀錄檔以清查同一帳號登入 IP 位址有無異動，並交叉比對同仁差勤紀錄、輪值表、簽到使用紀錄，是否登入情形與勤務時間相符，若登入次數較多者，亦可瞭解其原因。

參考文件：系統登入軌跡紀錄檔、機關 IP 位址清冊、差勤紀錄(或輪值表、簽到使用紀錄)、共用帳號清冊

2.6 是否沒有以離(休)職員工帳號登入使用之情形。

應落實系統使用者權限管理，系統管理者應於同仁離職或職務異動時，即時辦理系統帳號權限註銷或異動作業。

系統管理單位應定期辦理帳號清查作業，檢視有無離職同仁帳號尚未刪除或長期未使用之帳號，請使用單位檢視該帳號有無繼續保留需要。

稽核方法參考：得向人事室調閱離退職紀錄，比對統離職權限刪除異動紀錄表冊，檢視系統管理單位是否即時辦理帳號異動作業。

參考文件：人員離職異動名冊、系統帳號權限異動記錄、使用者帳號及權限管理規定、系統存取控制管理程序書

2.7	單次使用系統時間是否正常 (相較一般使用習慣，單次使用系統時間小於____小時)。
2.8	累計使用系統時間是否正常(相較一般使用習慣，每月使用系統累計時間小於____小時)。

本項異常情形之界定，須審酌系統使用現況認定，與相關單位共同研商，謹就同仁職務差異、業務屬性、系統使用特性等常見指標供參考，說明如下：

表 11.系統使用時間異常指標表

指標	說明
同仁職務差異	如為後台承辦作業人員，同仁登入系統查詢完資料即可登出，單次登入使用時間較短；又如為受理民眾洽公櫃台人員，上班時段同仁會維持系統上線以提高服務速度，登入單次登入使用時間較長。
業務屬性	如該業務具淡旺季性質，則不同時期單次或累計登入使用時間可能有相當程度之差異。
系統穩定度	如果系統負載量較低（如伺服器頻寬、記憶體容量、硬體設備等因素），時常斷線造成登入系統使用時間被切割，可能因此使用時間較短。
有無設定閒置時間自動下線機制	如系統設置閒置特定期間自動下線機制，可能因此使用時間較短。
系統設定情形	簡易查詢資料之系統，登入使用時間較短；須線上作業之系統，登入使用時間較長。

2.9

使用者查詢筆數是否正常(相較一般使用習慣，每月查詢筆數小於____筆)。

透過檢視查詢筆數異常情事，可瞭解有無同仁蒐集個資作不法用途，亦或是外界有心人士利用系統漏洞滲入擷取資料，本項異常情形之界定，須審酌系統使用現況認定，與相關單位共同研商，謹就同仁職務差異、業務屬性等常見指標供參考，說明如下：

表 12.查詢筆數異常指標表

指標	說明
同仁職務差異	如後台承辦作業人員與受理民眾洽公櫃台人員，因處理業務不同查詢筆數具有差異。
業務屬性	如該業務具淡旺季性質，則不同時期使用系統查詢次數可能有相當程度之差異。

2.10	使用者是否依規定於查詢系統登載「案號」或「查詢事由」。
2.11	系統雖無法登載「案號」或「查詢事由」，是否另設置「電腦查詢資料登記簿」管制使用情形。

系統是否須設置登載「案號」或「查詢事由」機制，應視系統主管機關法規、業務性質是否單純及機關首長權責決定。

本項雖非強行規定，但要求登記案號或查詢事由能有效減少同仁恣意查詢之動機，也利於事後追查管理，另有部分機關要求同仁查詢資料前需逐筆經主管陳核在案，更能強化查調前審查作業。

針對民眾、民代電話或現場查詢、臨時交辦案件、未立案或誤查案件等無相關申請單或公文可資證明者，建議至少可設置「系統查詢登記簿」俾利事後追蹤。

參考文件：資訊系統作業規範、系統查詢紀錄清冊、系統查詢登記簿、查詢依據佐證資料

2.12	使用者「查詢內容」與登載之「案號」(如收文號)或「查詢事由」是否相符。
------	-------------------------------------

調閱系統使用查詢軌跡紀錄檔與查詢依據佐證資料勾稽比對，確認同仁查詢目的係屬公務查詢用途，並釐清有無誤載誤查案件。

政風機構可推動使用單位自檢作業，由單位管理人員定期先行檢視，最後再由稽核人員依比率抽查或全面清查，提高實地稽核之效率，若自檢作業時發現異常情形，亦可立即通報政風機構深入調查，建立異常通報機制。

2.13 系統存取特別權限者查詢筆數是否正常(例如每月查詢筆數小於____筆)。

特權使用者係相較一般使用者擁有更多系統權限者，如系統管理者、網管、資料庫管理者、應用程式開發人員。可透過稽核時機，檢視該等使用者使用系統查詢情形，是否有濫用權限查詢情事。

對於特別權限者難以訂定通用稽核項目，惟建議稽核人員可先鎖定對象，再依其業務職掌擬定本項異常狀況。

2.14 是否沒有以機關首長、時事名人或公眾人物之姓名為查詢條件情事(亦即確認查詢作業係基於公務需要)。

可先建立機關首長、時事名人或公眾人物之名單，再據以檢視查詢條件是否有名單內人員。

2.15 是否有指派專人定期查核機關內使用者正常查詢機敏性資料系統，並留存查核紀錄備查。

可依資訊系統作業規範，檢視機關內部是否依規定頻率及執行方式辦理稽核或查核，有無定期彙整相關紀錄檢陳主管核章備查。

參考文件：資訊系統作業規範、稽核紀錄文件

(三)系統存取異常狀況通報情形

3.1 是否符合機關需求界定或修訂系統存取異常狀況。

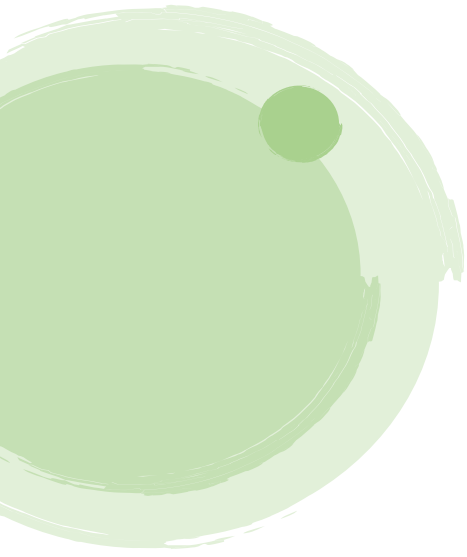
本項目係機關是否針對資訊系統使用現況，界定異常情形，可列入資訊系統作業規範中，或於定期稽核、查核時滾動式修訂。

除前揭稽核項目外，各機關另可依機關業務性質系統使用特性，設定其他異常情形列入稽核項目，例如：規費收據補發且作廢異常、稅籍主檔異動未於備註欄未註明原因等。

3.2 是否建立系統存取異常狀況通報機制且定期通報政風單位。

針對前述異常狀況項目，當使用單位或資訊室發現有異常情事時，有無即時通報或定期簽會政風室之機制，如建置系統自動示警機制、使用單位定期自檢後簽會政風機構，或會同政風機構定期辦理稽核等方式。

參考文件：事件通報與應變管理程序書、資訊系統作業規範、
資訊系統示警畫面、稽核紀錄文件



參、資訊安全稽核



稽核項目

資通安全管理法及其子法屬原則性規範，未詳細敘明資通安全稽核需含括哪些必要稽核項目，各機關可依資通安全責任等級分級辦法第 11 條第 1 項規定，各機關應依其資通安全責任等級辦理附表一至附表八之事項，自訂稽核項目表，並視每年度行政院資安會報政策重點作適時調整。

導入資訊安全管理系統(ISMS)情形

1.1 資訊安全管理系統之導入及通過公正第三方之驗證情形?

依資通安全責任等級分級辦法附表一至附表八之辦理事項規定，資通安全責任等級為 A、B、C 級機關，應於初次受核定或等級變更後之二年內，將全部核心資通系統導入 CNS 27001 或 ISO 27001 等**資訊安全管理系統標準**、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。

資通安全責任等級為 A、B 級機關需完成公正**第三方驗證**作業，另 D、E 級機關無自行或委外開發之資通系統，故無需導入 ISMS。所謂公正第三方係指通過我國標準法主管機關經濟部委託財團法人全國認證基金會(TAF)認證之機構，名單如下：

表 13. 第三方驗證機構清冊

認證編號	第三方驗證機構-認可公司清冊
MS001	臺灣檢驗科技股份有限公司 (SGS)
MS004	香港商英國標準協會太平洋有限公司台灣分公司 (BSI)
MS012	艾法諾國際股份有限公司 (Afnor)
MS013	環奧國際驗證有限公司 (TCIC)
MS014	香港商漢德技術監督服務亞太有限公司台灣分公司 (TUV NORD)

1.2

核心資訊系統是否依資安責任等級分級應辦事項納入資訊安全管理系統(ISMS)適用範圍？

依資通安全管理法施行細則第 7 條第 2 項規定之核心資通系統，係指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

各機關自行或委外開發之資通系統應依資通安全責任等級分級辦法附表九及附表十所定資通系統防護需求分級原則完成資通系統分級，並依資通系統防護基準執行控制措施，產製**資訊系統清冊**。

表 14.資訊系統清冊

臺北市政府○○局資訊系統清冊							填寫日期： 年 月 日				
編號	資訊系統名稱	業務屬性	資訊系統安全等級	共同性系統()	承辦管理單位	系統承辦人	系統廠商	連絡電話	輔導時間	安全等級評估表狀態	資通系統防護基準自評表狀態
承辦人：			復核主管：			資安長：					

表 15.資訊系統安全等級評估表

○○○系統安全等級評估表

功能說明： _____ 業務屬性：業務類 行政類

影響構面				資通系統安全等級
1.機密性	2.完整性	3.可行性	4.法律遵循性	

步驟一：設定影響構面等級

影響構面		安全等級	原因說明
1.機密性	初估		
	異動		
2.完整性	初估		
	異動		
3.可用性	初估		
	異動		
4.法律遵循性	初估		
	異動		

步驟二：識別業務屬性

項目		業務屬性	原因說明
1.識別業務屬性	初估		
	異動		
2.是否為共用性系統	初估		
	異動		

系統承辦人： _____ 資安承辦人： _____ 承辦單位主管： _____

資安專責人員與認知訓練

2.1	是否遵循資安責任等級分級應辦事項相關規定，指定專責人員負責資訊安全管理系統之維護與檢討，並有適切分工？
2.2	是否指定專人或專責單位負責資訊服務請求/事件處理、維運及檢討，並有適切分工？

資通安全專職人員，指應全職執行資通安全業務，意即渠業務職掌及工作內容不可辦理一般行政庶務，且具有登入國家資通安全通報應變網站帳號權限者。

依資通安全責任等級分級辦法，資通安全專責人員，各級機關應設置人數：A 級機關 4 人，B 級機關 2 人，C 級機關 1 人，D、E 級機關未規定，細部職務執掌工作項目則視資訊室分工情形辦理。

參考文件：資訊安全組織名冊、資訊室工作分配表、維運廠商契約等

2.3	人員是否瞭解機關之資訊安全政策，以及應負之資安責任？是否依職務層級辦理適當之資訊安全認知教育與訓練？
2.4	人員是否遵循資安責任等級分級應辦事項相關規定，接受資安專業課程訓練、資安職能訓練及資安宣導？

依資通安全責任等級分級辦法應辦事項，各級機關資通安全專職人員、資訊人員、一般使用者及主管，均有一定資通安全專業課程訓練或資通安全職能訓練時數之要求規定：

表 16.各級機關資通教育訓練要求時數表

認知與訓練構面要求					
人員區分/ 機關分級	A 級機關	B 級機關	C 級機關	D 級 機關	E 級 機關
資通安全專職人員	資通安全 教育訓練	每人每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練			未規定
	資通安全 專業證照	初次受核定或等級變更後之一年內，至少 4 名資通安全專職人員分別持有證照 1 張以上。	初次受核定或等級變更後之一年內，至少 2 名資通安全專職人員分別持有證照 1 張以上。	初次受核定或等級變更後之一年內，至少 1 名資通安全專職人員分別持有證照 1 張以上。	
	資通安全 職能評量 證書	初次受核定或等級變更後之一年內，至少 4 名資通安全專職人員分別持有證照 1 張以上。	初次受核定或等級變更後之一年內，至少 2 名資通安全專職人員分別持有證照 1 張以上。	初次受核定或等級變更後之一年內，至少 1 名資通安全專職人員分別持有證照 1 張以上。	
其他資訊人員	每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練。				
一般使用者及 主管	每人每年接受 3 小時以上之資通安全通識教育訓練				

一般使用者及主管，係指除包含機關組織編制表內人員外，尚包含得接觸或使用機關資通系統或服務之各類人員(院臺護字第 1090003579 號函)。

資通安全專業課程訓練或資通安全職能訓練相關時數，可透過以下方式取得：

- 1.參加經行政院資通安全處認證之資安訓練機構舉辦之資安職能訓練⁷。
- 2.參加技服中心舉辦之政府資通安全防護巡迴研討會，或所開設之資通安全策略、管理、技術相關課程。
- 3.參加資通安全專業證照清單⁸上所列之訓練課程。
- 4.參加國內外之公私營訓練機構所開設或受委託辦理之資通安全策略、管理、技術訓練課程。

參考文件：人力資訊安全管理程序書、新進同仁系統使用須知、共通性系統權限申請表、網路資源保密及使用切結書



⁷ 相關內容詳見行政院國家資通安全會報技術服務中心-資安人才培訓服務網
<https://ctts.nccst.nat.gov.tw/>

⁸ 清單按季更新，詳見行政院國家資通安全會報網站 - 資安法專區 - 資安管理法，
<https://nicst ey.gov.tw/Page/EB237763A1535D65>

存取權限與人員管理

3.1 是否訂定人員之資訊安全作業程序與權責？是否明確告知保密事項，且簽署保密協議？

依公務員服務法第 4 條保密義務規定，各機關多要求新進同仁於報到當日簽署保密協議，填妥系統權限開通申請書等文件，機關並應儘速辦理新人訓練，俾利新進同仁瞭解機關資訊安全規定，內容可參考下圖 6。

新進人員資安宣導單(範本)

1. 資安宣導：密碼換新、程式更新、下載要當心。(機關可自行填寫資安宣導)
2. 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，不得使用個人私有設備及中國廠牌產品，公務設備亦不得連結個人私有手機上網。若有業務上的需求，必須經資安長同意後，列冊管理並定期檢討。
3. 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知資安窗口。
4. 不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。
5. 公務資料傳遞及聯繫必須使用公務電子郵件帳號，不得使用非公務電子郵件傳送或討論公務訊息。
6. 即時通訊軟體使用應注意不得傳送公務敏感資料。
7. 傳送公務資訊應有適當保護，例如加密傳送。
8. 帳號密碼必須妥善保存，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口。
9. 主動通報資安事件或可能資安風險者，依規定獎勵。
10. 未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。
11. 有資安疑慮或異常時，應即時通報資安窗口。
12. 應遵守個人資料保護法及資通安全管理法。
13. 資安訊息網址：(機關資安宣導及規範網址)
14. 資安窗口：
 - 姓名：
 - 電話：
 - 電子郵件：

宣導人：
新進人員簽名：
中華民國 年 月 日

本宣導單1式2份，由新進人員及宣導人各執1份

圖 4.行政院資通安全處訂定新進人員資安宣導單(範本)

3.2 是否遵循存取權限最小化原則，僅授權因職務所需之存取權限，且定期審查其適當性與正確性？

最小權限原則是要求每一個合法動作最小的權限，就是為了保護系統資料以及功能避免受到錯誤或者惡意行為的破壞。

機關權限帳號管理者，應針對使用者業務性質，賦予不同存取權限且分別管理，避免共用帳號之情形，並定期辦理特殊權限及一般權限帳號清查，作成紀錄表單。

參考文件：帳號權限控管作業說明書、存取控制管理程序書、帳號清冊

3.3 是否針對人員(包含正式人員、臨時人員、派遣人員等)之離職或調職，訂定作業管理程序，且落實執行(如：帳號存取權限回收、停用或移除之處理等)？

帳號權限管理者應確實依員工離職報告單、帳號申請異動註銷單，註銷各項資訊資源及使用權限，若涉及單一簽入系統或人事系統聯動他系統者，並應注意有無一併刪除成功，帳號權限管理者並應按季辦理清查作業。

參考文件：權限帳號管理系統資訊作業規定、網域帳號清單、帳號申請異動註銷單

個人資料保護與管理

4.1	是否明確界定個人資料範圍？是否針對個人資料檔案進行內/外部環境與作業流程分析，以鑑別與個資有關之流程或應用系統，且落實執行個資盤點？
4.2	檢視蒐集、處理或利用個人資料之流程中，是否依照法律規定以及內部管理程序進行？
4.3	是否建立個人資料安全管理安控機制？機制內容是否包含存取權限、資料安全、人員管理及設備安全管理等(如：個人資料之傳送是否採取加密等保護機密性、是否確保個人資料之完整性等)？
4.4	是否針對所屬人員進行認知宣導與教育訓練，並確實記錄？
4.5	是否針對個人資料相關設備進行安全管理(如：相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等)？
4.6	是否建立個人資料安全稽核機制(包含對委外供應商之稽核，確保委外作業建立必要的個資管理流程、程序及安全控制措施等)？
4.7	是否建立個人資料使用紀錄、軌跡資料及證據保存相關管理機制(如新增、修改、刪除、資料匯出、列印等操作紀錄)？
4.8	具個人資料之系統是否有建立稽核機制？是否進行安全檢測作業(如滲透測試)？
4.9	於事故發生時，是否依規定通報，並作出應變處置及預防等措施？

一、資訊安全與個資保護之關係

資訊安全著重組織資訊資產之保護，係為確保資訊及其處理設備之機密性、完整性與可用性，針對組織、人員、場

所、系統及軟硬體設備等層面進行有效管理之措施。

個資保護係為防免人民隱私權及人格權遭受侵害，並促進個資合理使用，針對蒐集、處理及利用訂有規範，強調法令之遵循，其保護客體包括各種形式含有個資之檔案。

有別於非公務機關落實資訊安全維護，係基於維持組織正常營運與保護商業機密等私人目的；公務機關為公權力行使及行政管理目的必要，保存管理民眾個人資料，包含戶籍、財產所得、刑事紀錄、病歷等，此即為機關之資訊資產，爰公務機關之資訊安全維護常與個人資料保護相結合。然不啻於此，部分公務機關資訊業務涉及民生基礎設施（台電、台水、中油、核能等）及國家經濟重要制度（中央銀行及證交所等），此處資訊資產之重要性即高於個資保護，資訊安全範圍即有所擴張。

二、個資保護規範

本法第 2 條第 1 款定義**個人資料之類型**，第 6 條規定**特種個人資料**之限制，第 8、9 條明示**當事人告知義務**；公務機關對個人資料之**蒐集、處理及利用**，規定於個人資料保護法第 15 條至 18 條及施行細則第 23 至 25 條規定，其中本法第 18 條規定，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項；又同法施行細則第 12 條規定，本法所稱**安全維護措施**，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，包含下述事項：

表 17.個資保護維護措施

個人資料保護法施行細則第 12 條之安全維護措施	
1.配置管理之人員及相當資源	2.界定個人資料之範圍
3.個人資料之風險評估及管理機制	4.事故之預防、通報及應變機制
5.個人資料蒐集、處理及利用之內部管理程序	6.資料安全管理及人員管理
7.認知宣導及教育訓練	8.設備安全管理
9.資料安全稽核機制	10.使用紀錄、軌跡資料及證據保存
11.個人資料安全維護之整體持續改善	

除個人資料範圍之界定及處理程序外，其他事項經常會併同資通安全管理法之公務機關應辦事項辦理。

三、個資保護管理制度

個人資訊管理系統(PIMS)為評估組織是否有效進行個人資料保護之管理制度，我國於非公務機關主要以「臺灣個人資料保護與管理制度規範 (TPIPAS)」作為認證制度，於公務機關則以「ISO/IEC 27001 資訊安全管理系統」、「ISO/IEC 27701 個人資訊管理系統」、「ISO/IEC 29100 隱私權框架」、「ISO/IEC 29151 個人可識別資訊保護實務」及「BS 10012 英國標準個人資料管理系統」等作為驗證標準。

「ISO/IEC 27701 : 2019 個人資訊管理系統」驗證標準具體化個資保護管理制度辦理事項，其中不可排除適用事項如下表：

表 18.ISO/IEC 27701 個人資訊管理系統不可排除適用事項

主標題	相關內容
5.2 組織全景	5.2.1 瞭解組織及其全景 5.2.2 瞭解關注方之需要及期望 5.2.3 決定資訊安全管理系統範圍 5.2.4 資訊安全管理系統
5.3 領導作為	5.3.1 領導及承諾 5.3.2 政策 5.3.3 組織角色、責任及權限
5.4 規劃	5.4.1 因應風險及機會之行動 5.4.1.1 一般要求 5.4.1.2 資訊安全風險評鑑 5.4.1.3 資訊安全風險處理 5.4.2 資訊安全目標及其達成之規範
5.5 支援	5.5.1 資源 5.5.2 能力 5.5.3 認知 5.5.4 溝通或傳達 5.5.5 文件化資訊 5.5.5.1 一般要求 5.5.5.2 制定及更新 5.5.5.3 文件化資訊之控制
5.6 運作	5.6.1 運作之規劃及控制 5.6.2 資訊安全風險評鑑 5.6.3 資訊安全風險處理
5.7 績效評估	5.7.1 監督、測量、分析及評估 5.7.2 內部稽核 5.7.3 管理審查
5.8 改善	5.8.1 不符合項目及矯正措施 5.8.2 持續改善

資訊資產管理

5.1	是否確實盤點資訊資產並建立清冊(如：識別擁有者與使用者等)？是否訂定資訊分級規則(如：區分機密性、敏感性及一般性等)、授權處理層級及處理規範，且落實執行？
5.2	是否建立資訊資產異動管理程序，即時更新資訊資產清冊，且落實執行？
5.3	是否訂定資訊設備汰除管控程序，以確保清除資訊設備或儲存媒體內所存放之機敏資料，或將其實體破壞？

一般資訊資產管理內容如下：資訊資產採購、驗收、盤點、保管與使用、分類、價值等級評估、編號及標示、歸還及報廢處置。

各機關應每年定期執行資通訊資產盤點及風險評估⁹，依臺北市政府資通安全維護計畫製作資訊及資通系統資產清冊等相關文件；應視業務性質及機密等級，依資通訊資產與電子資料受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他等六大影響構面進行資料分級，並於蒐集、處理及利用三階段採行適當之安全機制及作法。

有關資訊設備汰除管控程序，依臺北市市有財產報廢處理原則，針對使用年限屆滿之資訊設備或儲存媒體，常以格式化作業、物理實體破壞等方式移除內建公務資料後，視其殘餘價值，選擇以轉贈或洽一般廠商價購或交回收清除機構價購，或無償交由環保局資源回收車回收。

資通訊資產報廢或不再使用時，應依資通訊資產類別循

⁹ 依臺北市政府資通訊資產及電子資料安全作業指引參、資通訊資產管理。

相關財產或物品報廢程序辦理後，再進行報廢、銷毀或其他處置，如轉贈社會福利機構等。

參考文件：臺北市政府資通訊資產及電子資料安全作業指引、資訊資產清冊、資產管理程序書、資產分類與控管程序書、個人電腦暨可攜式儲存媒體作業說明書、實體與環境安全管理程序書、資訊設備報廢管理作業說明書、財產異動/報廢單

5.4 機關是否尚有使用危害國家資通安全疑慮之產品？ 是否有造冊列管並評估汰換事宜？

各機關購置或使用資通訊產品，應依「各機關對危害國家資通安全產品限制使用原則」辦理，並禁用主管機關公告之資通訊產品，依現行法令規定、定義及處理原則等事項說明如下：

一、法規依據

- (一)政府採購法第 17、37 條。
- (二)機關辦理涉及國家安全採購之廠商資格限制條件及審查作業辦法。
- (三)各機關對危害國家資通安全產品限制使用原則。

二、定義

危害國家資通安全產品¹⁰：指對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務，且不定限於中國生產或陸資企業製造商品。

資通訊產品¹¹：參考資通安全管理法第 3 條用詞定義，包含軟體、硬體及服務等項，另具聯網能力、資料處理或控制功能者皆屬廣義之資通訊產品，如無人機、網路攝影機、印表機等。

受到規範的**產品範圍**則囊括：伺服器主機、網路攝影機、遙測定點設備、無人機、雲端服務、電信業的核心骨幹網路

¹⁰ 依行政院 108 年 4 月 18 日院臺護字第 1080171497 號函頒「各機關對危害國家資通安全產品限制使用原則」規範內容。

¹¹ 依行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函說明內容。

設備電腦軟體、防毒軟體、機關委外開發的軟體系統、委外通訊設備顧問，以及委外企業開發資訊系統等。

大陸廠牌認定方式：由機關「從嚴認定」，所有屬大陸廠牌者，無論其原產地於我國、大陸地區或第三地區等，渠等產品均須納入填報範圍。如無法判斷是否屬於大陸廠牌，建議可先行請原廠提供相關證明。

具敏感性或國安(含資安)疑慮之業務範疇¹²：由經濟部投資審議委員會於網站上不定時更新，如能源、水資源、通訊傳播、交通、金融及政府機關資通訊系統等。

三、處理原則

公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體；個人資通訊設備不得處理公務事務，亦不得與公務環境介接。

各機關除因業務需求且無其他替代方案外，不得採購及使用前述產品。必須採購或使用時，應具體敘明理由，經主管機關核可後，以專案方式購置，並列冊管理及遵守下列規定：指定特定區域及特定人員使用、不得與公務網路環境介接、不得處理或儲存機關公務資訊、測試或檢驗結果應產出報告，且購置理由消失，或使用年限屆滿應立即銷毀。

四、採購注意事項

有關機關辦理涉及國家安全採購業務，行政院公共工程委員會 109 年 8 月 17 日「機關辦理涉及國家安全採購之防

¹² 依經濟部投資審議委員會公告「具敏感性或國安(含資安)疑慮之業務範疇」規範內容。

範機制座談會」紀錄針對相關法律規範、廠商資格限制條件審查、投標須知範本勾選作法及陸資廠商界定範疇等，均有詳細說明。

五、未來政策方向

(一)限期汰換

限期完成全面汰換大陸廠牌資通訊產品，汰換前不得與公務環境介接，各機關應依「國有公共財產管理手冊」及「各機關財務報廢分級核定金額表」等規定辦理財物報廢。

(二)研議白名單

適用政府採購法之對象，原則以共同供應契約之品項為基準，未來並持續擴充增加共契中資通訊產品之品項。倘經機關評估需採購非共契品項者，應敘明理由及其必要性，簽報機關首長或其授權人員核准。

資訊委外安全管理

6.1 辦理涉及資通訊系統、設備、服務委外採購應注意事項？

辦理涉及資通訊系統設備服務相關採購案，除應注意是否符合資安相關規範外，可參考「臺北市政府財物採購契約範本」、「臺北市政府勞務採購契約範本」及「臺北市政府公共工程技術服務契約範本」(臺北市政府 111 年 4 月 6 日府授工採字第 1113007988 號函)內容辦理。

6.2 是否訂定廠商之資訊安全責任與保密規定？是否要求執行資安稽核，並請廠商提供異常報告，以利後續追蹤與管理？

鑑於時常有資安事件肇因於委外廠商而起，對於委外廠商之規範必須嚴格落實，委外業務包含資訊服務¹³(指提供與電腦軟體或硬體有關之服務)及雲端服務(指利用網路連結遠端伺服器所提供之服務)，且機關辦理統包工程契約、工程契約、財物契約、勞務契約、無償所提供或複委託者之委外作業履約項目若涉及資通訊產品、系統或服務者，即應注意資安相關規範。

依臺北市政府資通安全管理規定、臺北市政府資通訊業務委外作業指引規定，資訊業務委外時，各機關與受託者簽訂契約，應將受託者應遵循之資通安全、保密條款及作業相關法規要求、本府得保留對受託者進行資通安全稽核之權利等事項納入契約，並應於執行業務前簽署保密切結書及保密

¹³ 依據臺北市政府資通訊業務委外作業指引貳、使用範圍。

同意書，受託者應自行辦理資安稽核作業，各機關定期對受託者稽核表進行稽核。

參考文件：臺北市政府資通安全管理規定、臺北市政府資通訊業務委外作業指引、資訊作業委外服務安全作業要點、資訊委外業務派駐人員管理規範、資訊作業委外服務資訊安全需求、委外管理程序書、第三方管理程序書、系統建置/維護案契約、應用程式獲取開發及維護管理程序書、供應商關係管理程序書、保密切結同意書

6.3

委外廠商專案成員進出機關範圍是否被限制？對於委外廠商駐點人員使用之資訊設備(例如：個人、筆記型、平板電腦、行動電話及智慧卡等)是否建立相關安全管控措施？設備攜入/出有無填寫申請表？

關於門禁及人員管制部分，委外廠商派駐人員應列冊管理，並依臺北市政府資通安全管理規定，支援或維護服務人員應由機關承辦同仁陪同並經登記後，始得進出管制區域。

有關設備管理部份，人員攜帶資訊設備進出資訊機房時，須於「資訊機房人員進出管制紀錄」註明，若業務需要申請對外網路需依規定申請並經權責主管核准，並確認連線設備已安裝防毒軟體，其病毒碼更新狀態至最新，單純為儲存媒體應先經過安全掃瞄，確認無安全風險後始得攜入使用。

參考文件：臺北市政府資通安全管理規定、廠商資訊業務委外服務團隊成員名冊、機關提供硬體設備一覽表、人員進出電腦機房管制簿、實體與環境安全管理程序書、可攜式電腦或媒體使用申請註銷單、資

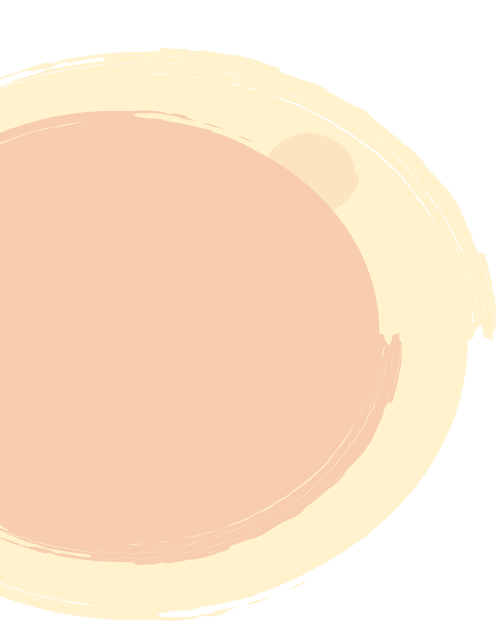
產分類與控管程序書。

6.4

是否訂定委外廠商系統存取程序與授權規定(例如：限制其可接觸之系統、檔案及資料範圍)？委外廠商專案人員調整與異動，是否依系統存取授權規定，調整其權限？

委外駐點廠商原則依帳號權限控管暨存取控制作業辦理，注意帳號權限開通之必要性、適當性，人員調整及異動應即時變更帳號權限。如遇業務上有遠端連線需要時，依臺北市政府資通安全管理規定第 17 點，本府禁止受託者遠端連線管理伺服器，如有遠端管理需求，應以 MDVPN 或 SSL VPN 等加密連線，一人一帳號且採取多因子認證，並僅得連線至受託者管理之主機範圍，降低重要主機可能攻擊範圍；連線及登入之相關紀錄應納入監控，有異常行為應停用帳號並進行調查。

參考文件：臺北市政府資通安全管理規定、系統委外開發或維護專案契約、系統存取控制管理程序書



肆、資訊使用管理稽核常見違失態樣



權限管理未核實

一、共用帳號

說明	1.不同使用者共用同一帳號登入系統查詢使用。 2.將帳號密碼交業務代理人使用。 3.原無系統帳號權限之使用者便宜行事，逕向同仁借用帳號使用。
改善措施	1.使用者帳號應具唯一性與識別性，且各該系統涉及民眾個資，應加強宣導同仁禁止帳號共用，確保查詢行為均得以回溯特定使用者，減少有心人士投機查詢之風險。 2.定期檢查勾稽比對使用者查詢紀錄及出勤情形(或業務內容)，確認查詢行為是否確為本人所為。

二、未即時註銷或變更帳號

說明	離退職人員之帳號權限未註銷或因系統管理者未能即時取得人事異動資訊，致未能即時註銷或變更帳號權限。
改善措施	1.將系統管理者納入人事異動訊息通知流程，以利即時註銷或變更異動人員之帳號權限。 2.定期盤點系統帳號使用情形，主動檢討取消閒置帳號，維護查詢帳號使用安全。

三、未依職務內容設定系統使用權限

說明	未依業務內容或職位等級之差異配發帳號權限，或未確實依各申請單位業務範圍，核定查調項目做最小範圍授權。
改善措施	<ol style="list-style-type: none">1.系統帳號權限申請範圍應經使用者主管審核後辦理，系統管理單位應確實審核使用者申請之權限，是否符合其職務範圍。2.定期檢查系統帳號授權內容及其實際使用情形，確認帳號授權情形是否妥適，並適時調整。

四、帳號未即時登出

說明	使用者登入系統用畢後，未即時登出。
改善措施	<ol style="list-style-type: none">1.使用者未即時登出，且若使用行動資訊設備登入系統後不慎遺失，恐遭有心人士不當利用之風險，應宣導同仁系統使用查詢後應立即登出之重要性。2.建議依系統使用特性，新增自動登出功能。3.定期檢查勾稽比對使用者查詢紀錄及出勤情形(或業務內容)，確認查詢行為是否確為本人所為。

非授權查詢

一、因好奇或便宜行事以姓名查詢個資

說明	系統使用者因好奇心查詢時事名人、親友或便宜行事等因素，利用姓名查詢民眾個人資料。
改善措施	<ol style="list-style-type: none">1.建議於系統適時新增彈跳視窗或於查詢頁面加註個人資料保護法相關規範警語，協助使用者檢視查詢行為。2.建立使用規範，請同仁盡量避免使用姓名查詢，若有使用姓名查詢之必要，應確實填寫因公查詢事由。3.建立稽查機制，將以姓名查詢紀錄列入特殊查詢項目，並經主管覆核機制，降低同仁不當查詢之風險。

二、以檢測系統等因素使用系統

說明	系統使用者以系統檢測、教學等因素，輸入自身或同仁資料作為測試。
改善措施	<ol style="list-style-type: none">1.雖查詢行為係為執行公務，惟查詢原因與系統應用目的無關，且難以查證查詢理由之真實性，建議系統管理單位針對使用系統可能遭遇困難狀況，訂定排解方式，避免逕以系統查詢個資。2.授權同仁系統使用權限時，應確認同仁對系統使用作業規範有充分認識，並加強宣導個人資料保護意識。

三、以查詢廠商資料等因素使用系統

說明	系統使用者為辦理會計結報作業或人事休假獎金作業，查詢廠商身分證字號或同仁出入境資料。
改善措施	<ol style="list-style-type: none">1.雖屬執行公務需要進行查詢，惟查詢目的與系統應用目的無關，並非授權查詢行為，應建立稽核機制，審視查詢目的，避免濫用系統查詢。2.授權同仁系統使用權限時，應確認同仁對系統使用作業規範有充分認識，並加強宣導個人資料保護意識。

查詢或登入次數異常

一、查詢次數異常

說明	因系統使用者受理案件後，於各處理階段有反覆查詢系統習慣。
改善	提醒使用者更改使用系統習慣，避免不必要之查詢，以降低反覆查詢之風險。

二、登入失敗次數異常

說明	系統使用者轉換使用系統時，疏未注意輸入大寫帳號，導致登入失敗次數異常。
改善措施	<ol style="list-style-type: none">1.提醒使用者於輸入帳號密碼時多加留意。2.建議系統管理者建置登入錯誤達一定次數即鎖定及異常通報機制，以阻斷不法人士嘗試登入系統。

異常管控機制未建立或未落實

一、未建置登入失敗鎖定功能

說明	系統未有登入失敗鎖定功能。
改善措施	建議依系統使用特性，新增登入失敗達一定次數之自動鎖定及異常通報功能，阻斷非授權使用者嘗試登入之機會，系統管理者、使用者主管或政風單位亦得以即時檢視及因應。

二、未建置累積使用時間或查詢筆數限制功能

說明	未限制單次(或固定週期)累計使用時間或查詢筆數功能。
改善措施	建議依系統使用特性，新增使用達一定使用時間、查詢筆數之自動示警或強制登出機制及異常通報功能，從使用端減少異常查詢行為，系統管理者、使用者主管或政風單位(或稽核單位)亦得以即時檢視是否有異常查詢之情事。

三、未建置查詢事由登載功能

說明	系統查詢介面無「查詢事由」或相類似欄位供點選或填列，亦無設置查詢登記簿等管制作為。
改善措施	建議於系統查詢頁面新增「查詢事由」之欄位或視窗，且點選(或填列)後使得進入查詢之強制措施，若未能即時建置系統功能，亦應設置查詢登記簿，俾利事後稽核比對查詢依據外，亦能對違規查詢者產生一定程度之嚇阻效果。

四、通報機制未能有效發揮功能

說明	系統以電子郵件將異常事件通知系統使用者及其主管，惟該郵件發送後未有備份資料。
改善措施	應將系統管理者納入系統異常通報機制，得適時納入政風單位即時掌握狀況及因應，並應完整記錄及保存使用查詢異常內容，以利辦理稽核作業。

稽核作業未落實

一、系統管理單位未落實稽核作業

說明	系統管理單位未依規定辦理使用者查詢稽核作業並留存相關稽核紀錄。
改善措施	系統管理單位應定期辦理稽核作業並保存相關紀錄，確實掌握系統使用者使用情形，並訂定系統使用作業規範，要求系統使用單位據以辦理內部查核作業，落實督導責任。

二、系統管理單位未依規定辦理實地抽查作業

說明	系統管理單位多以線上稽核或系統使用單位自行檢查，未依規定辦理實地稽核。
改善措施	系統管理單位應落實執行年度實地抽查稽核作業，或檢討修正「實地抽查稽核」規定，增加彈性稽核方式，以維護督導紀律。

三、僅廠商具調閱使用查詢紀錄檔權限

說明	僅系統維護廠商具有調閱使用查詢紀錄之權限，系統管理單位無法調閱紀錄，亦未辦理稽核作業。
改善措施	系統管理單位應具有調閱系統使用查詢紀錄之權限，檢討廠商調閱紀錄檔之必要性，並應定期辦理稽核作業。

四、系統使用單位未落實內部查核作業

說明	系統使用單位未依系統使用作業規定指派專人辦理內部查核作業及保管記錄，或由系統使用者辦理查調作業及保管記錄。
改善措施	建議將政風單位納入內部查核制度，落實審查機制，並由專人專責卷檔保管工作。

文書作業未確實

一、未經核准即先行查詢

說明	系統使用者未經業務主管核准，即先行查詢系統資料。
改善措施	應強化業務主管審核(查)功能，落實「先報後查」之作業程序。

二、未落實登載查詢紀錄簿

說明	系統查詢紀錄簿僅留存特定時點起相關資料，未依規定保存年限留存紀錄。
改善措施	應落實專人專責之卷檔管理工作，並依規定年限加以保存。

三、查詢紀錄簿未定期彙陳首長核閱

說明	部分系統查詢紀錄簿未依規定送陳機關首長核閱。
改善措施	應落實專人專責之卷檔管理工作，由專人按時陳報首長核閱。

四、未保存系統權限異動書面資料

說明	職務異動退(離)職人員權限取消或調整未留下書面資料。
改善措施	系統使用權限新增、修改、註銷等作業均須經使用單位主管及相關單位核可後據以辦理，並依系統使用查詢作業規定保存年限妥善收存相關紀錄，以利追蹤管理。

其他違失情事

一、系統環境未實體隔離

說明	系統使用者於可連結外部網路之個人電腦中使用系統，未符實體隔離之規定。
改善措施	建議系統管理單位協助使用單位建置實體隔離操作環境，或適時檢討修正「運用資料應實體隔離」規定之合宜性。

二、未熟稔系統使用作業規範

說明	系統使用者對系統使用作業規範及程序之認識，大多透過前手經驗傳承教導，未實際瞭解規範內容，易生違規情形。
改善措施	系統管理單位應落實系統權限管理及教育訓練，應於授權系統使用權限時，併同確認使用者對系統使用作業規範之認識。

三、加班未辦理勤務刷卡作業

說明	系統使用者非公務時間加班未辦理勤務刷卡及加班申請作業。
改善措施	加強宣導同仁應核實辦理勤務刷卡及加班申請作業，以利勾稽比對非公務時間使用查詢系統紀錄。

附錄

常用資安名詞

名詞	說明
系統存取控制	定義是「對於資訊系統的存取保護，防止任何未經授權的系統存取、破壞。」於 ISO 27001:2013 中的項目包括：存取控制政策、網路與網路服務的存取、使用者存取管理、機密授權資訊的使用、系統與應用系統的存取控制。
CIA 資安鐵三角	Confidentiality(機密性)-避免資料未經授權之存取或披露。 Integrity(完整性)-確保資訊之正確性及完整性。 Availability(可用性)-授權的使用者可以正常、可靠的使用資訊。
防毒軟體 (Anti-virus Program)	防毒軟體用於偵測、移除電腦病毒、電腦蠕蟲、和特洛伊木馬程式，通常含有即時程式監控辨識、惡意程式掃描和清除和自動更新病毒資料庫等功能。
管理者 (Admin)	為 administrator 的縮寫，指對特定系統或應用程式有最高權限者，得使用新增、刪除或修改等功能。
黑名單 (Blacklist)	黑名單是電腦應用中常使用的存取控制方式之一，被列入黑名單的用戶無法進入系統。如電郵過濾透過黑名單，阻擋某些電郵地址或伺服器發出的電郵，達到過濾垃圾郵件的目的。
白名單 (Whitelist)	與黑名單相對的是，即「除名列於上者外一律不准進入」的信任許可名單。
使用者記錄文檔	指某些網站為了辨別用戶身分而儲存在用戶端 (Client Side) 上的資料，通

名詞	說明
(Cookies)	常經過加密處理。
虛擬私人網路 (VPN)	虛擬私人網路 (VPN) 是一種常用於連接中、大型企業或團體與團體間的私人網路的通訊方法。它利用隧道協定 (Tunneling Protocol) 在使用者電腦和 VPN 閘道器之間建立加密通道，來達到傳送端認證、訊息保密與準確性等功能。
防火牆 (Firewall)	在計算機科學領域中是一個架設在網際網路與企業內網之間的資安系統，根據企業預定的策略來監控往來的傳輸。主要功能為隔離網路，透過將網路劃分成不同的區域，制定出不同區域之間的存取控制策略來控制不同信任程度區域間傳送的資料流。
靜態應用軟體安全檢測 (Static Application Security Testing)	屬於「應用系統網站弱點掃描」的一種，亦常稱為靜態應用系統安全測試、白箱測試、源碼檢測，用不同角度檢查應用系統的原始碼(source code)程式流中可能被攻擊者所發現的漏洞，優點：在在開發階段及早修復問題，比起事後修補容易。
政府組態基準 (Government Configuration Baseline，簡稱 GCB)	目的在於規範資通訊設備(如個人電腦、伺服器主機及網通設備等) 的一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險。
資訊安全管理系統 (Information security management system，簡稱	是一套有系統地分析和管理的資訊安全風險的方法，有助於從法遵的合規性、技術及管理的有效性來對資訊安全進行評估。

名詞	說明
ISMS)	
ISO 27001:2013 資訊安全管理國際標準	目前國際上最廣泛採用之資訊安全管理規範，可提供建立、實作、運作、監視、審查、維持及改進資訊安全管理系統之模型，並可透過公正獨立的第三方組織，進行稽核與驗證。
ISO 27701:2019 個人資訊管理系統 國際標準	為保護個人隱私資訊提供指引，藉由補充額外的管控要求，以建立、實施、維護和持續改善在 ISMS 範圍內的隱私資訊管理 (Privacy Information Management)，降低隱私資訊所面臨的風險。
金鑰 (KEY)	在電腦技術中，是指一種與加密演算法搭配使用的符號序列，用於資料加/解密。
對等式網路 (peer-to-peer，簡稱 P2P)	又稱對等技術，是無中心伺服器、依靠用戶群 (peers) 交換資訊的網際網路體系。透過減少網路傳輸節點，能降低資料遺失的風險，卻也相對造成監控的難度，且為病毒媒介、駭客入侵與洩密管道，形成資安破口。
滲透測試 (Penetration testing)	伺服器 / 主機作業系統、應用軟體、網路服務、物聯網設備等，類比駭客的手法進行滲透或穿透跳躍主機之入侵測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竊改或竊取之可能性。 「滲透測試」是由具備極高技術水準的資安顧問以人工方式模擬駭客的思維，針對系統做攻擊測試。國際常用的測試規範有 OWASP Checklist、OWASP

名詞	說明
	ASVS、CWE/SANS Top 25 等。
紅隊演練 (Red Teaming)	係用以補足傳統滲透測試容易忽略之邊界防禦，以及基於人為疏失之佈署盲點，利用公開資訊、社交網路、暗網等蒐集目標情資，結合資訊安全專家之專業知識、攻防技術及駭客工具資料庫，對於雙方所約定之攻擊目標與組織，採取無所不用其極的方法進行入侵演練，同時可驗證防守方(藍隊)的偵測與回應能力。
伺服器 (Server)	對使用者端提供特定服務的硬體 (Hardware) 和軟體 (Software) 整合起來稱為「伺服器 (Server)」。可區分為管理資源並為用戶提供服務的電腦軟體，通常分為檔案伺服器 (能使用戶在其它電腦存取檔案)，資料庫伺服器和應用程式伺服器。或執行以上軟體的電腦，又稱為網路主機 (host)。
社交工程 (Social Engineering)	係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破資通安全防護，遂行其非法的存取、破壞行為。
資訊安全監控中心 (Security Operation Center，簡稱 SOC)	資訊安全監控中心 SOC 管理組織的資安產品、網路設備、使用者設備，以及系統中任何可能違反資訊安全 CIA 的內容，提供 24*7 的服務負責監看，偵測與處理資安事故。
SQL 注入 (SQL injection)	SQL 是一種資料庫系統常用的程式語言。若駭客在輸入的字串之中夾帶錯誤 SQL 指令，且程式忽略字元檢查，夾帶進去的惡意指令就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因

名詞	說明
	此遭到破壞或是入侵，是發生於應用程式與資料庫層的安全漏洞。
SSL 加密通訊協定 (Secure Socket Layer)	為 TLS 傳輸層安全性協定 (Transport Layer Security) 之前身，係一種安全協定，目的是為網際網路通訊提供安全及資料完整性保障。
雙因素認證 (two-factor authentication，簡稱 2FA)	<p>認證，為確認是由本人所發出的，所以認證必須要有唯一性，不會重複。目前認證方式為：What you know ? (密碼或 PIN)、What you have ? (Token 或 Smart card)、What you are ? (生物特徵，如指紋)。雙因素認證，就是結合了兩種不同的認證方式，亦稱雙因子認證。</p> <p>兩階段驗證(two-step verification)，則是純粹的驗證過程有兩次，可以使用同一種認證方式驗證兩次，或是不同的認證方式。</p>
弱點掃描 (Vulnerability Assessment)	<p>「弱點掃描」是使用自動化工具對系統進行檢測，找出所有已知的風險。</p> <p>弱點掃描分為系統弱點掃描與網站弱點掃描：</p> <p>「系統弱點掃描」係針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目須符合 Common Vulnerabilities and Exposures (CVE) 發布的弱點內容(最新版)。</p> <p>「網站弱點掃描」係針對網頁安全弱點進行掃描，檢測項目須符合最新版 OWASP TOP 10。</p>

名詞	說明
	這種測試比較依賴程式本身的品質，不同廠牌、不同種類的規則，都會有不同的結果。
不斷電系統 (Uninterruptible Power System，簡稱 UPS)	是在電網異常（如停電、欠壓、干擾或浪湧「也稱：湧浪電流」）的情況下不間斷的為電器負載設備提供後備交流電源，維持電器正常運作的設備。
網站應用程式防火牆 (Web Application Firewall，簡稱 WAF)	WAF 主要是用於保護網站應用程式，透過監控網站傳輸的 HTTP 流量，比對病毒與惡意程式資料庫，過濾出可疑流量並拒絕惡意流量進入，保護網站免受駭客攻擊。
縱深防禦 (Defense-in-Depth)	指利用多層次的防禦技術來減緩不同類型的攻擊，常見項目有：防火牆、Web 應用程式防火牆、入侵偵測防禦系統、病毒與垃圾郵件過濾閘道系統、虛擬私有網路、存取控制、資安事件監控等。
邊界網路 (DeMilitarized Zone，簡稱 DMZ)	係屬網路架構布置方案之一種，常被使用的架設方案，是在不信任的外部網路和可信任的企業網路外，建立一個面向外部網路的邏輯子網路，在受保護網路與外部網路之間，新增的網路，用於對外部網路的伺服器主機，可提供額外保護內部網路的安全層，有時亦稱為週邊網路。
Windows 更新服務 (Windows Server Update Services)	是微軟公司開發的一個電腦程式，它允許管理員管理已為微軟產品發布的更新和熱修復修補程式分發到企業環境中的電腦。WSUS 從微軟更新網站下載這些更新，然後分發它們到網路上的電

名詞	說明
	腦。
目錄列舉功能 (Directory Listing)	瀏覽網站未指定瀏覽內容時，會根據網站伺服器所提供的選項搜尋該目錄中的啟始頁面(如：index.html)。若應用程式開啟目錄列舉功能，當應用程式未找到設定檔所指定的啟始頁面，便會列出該目錄下的所有檔案和目錄。駭客可藉此得知目錄中的檔案與結構，並取得儲存資料庫連線等網站相關設定。
資安健診	<p>資安健診服務係透過整合各項資通安全項目的檢視服務作業，提供受檢單位資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資訊系統安全防護能力。</p> <p>包括網路架構檢視(檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠)、有線網路惡意活動檢視(封包監聽與分析、網路設備紀錄檔分析)、使用者端電腦檢視(更新檢視、組態設定檢視、電腦惡意程式或檔案檢視)、伺服器主機檢視(更新檢視、組態設定檢視、惡意程式或檔案檢視)及安全設定檢視(目錄伺服器(如 MS AD) 組態設定檢視、防火牆連線設定)等。</p>
ISO 四階文件	<p>第一階文件：主要包括全範圍之資安整體實行政策及原則，如：資安政策、管理手冊、適用性聲明等。</p> <p>第二階文件：主要包括各領域之執行方向及原則，如：資訊資產、實體環境、人員安全、網路安全、風險評鑑、營運</p>

名詞	說明
	<p>管理、系統開發、事件通報、內部稽核等程序書。</p> <p>第三階文件：主要為包括相關業務流程及處理程序之詳細描述，如：人員職權、帳號及通行碼管理、備份、營運計畫、資料庫管理、委外人員管理等作業程序或辦法。</p> <p>第四階文件：主要包括業務運作所採用之表單、合約及其產生之各項紀錄，如：文件記錄、衡量指標表、季報表、名冊、切結書等表單。</p>
<p>入侵偵測系統 (Intrusion Detection System，簡稱 IDS)</p>	<p>指通過對行為、安全日誌或稽核資料或其他網路上可以獲得的資訊，進行研判、比對，然後檢測出資料庫中入侵系統的異常行為或侵入的企圖。</p>
<p>入侵預防系統 (Intrusion Prevention System，簡稱 IPS)</p>	<p>是一部能夠監視網路或網路裝置的網路資料傳輸行為的計算機網路安全裝置，能夠即時的中斷、調整或隔離一些不正常或是具有傷害性的網路資料傳輸行為。比較簡單的解釋是入侵預防系統=入侵偵測系統+防火牆。</p>