資通安全法律案例彙編

第 18 輯

行政院國家資通安全會報技術服務中心

中華民國 110 年 12 月

凡例

壹、本彙編案例依其內容及相關法律觀點之重要內容，分為以下類別：

一、資訊保護(Security)

二、資訊公開(Disclosure)

三、資訊監察(Monitors)

四、資訊應用(Application)

貳、本案例編碼共 5 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年分三碼及案例流水編碼兩碼；以利讀者在案例與評量間對照參考。

壹、資訊保護(SECURITY)---------- 1

美國人口統計局 IT 管控遭糾舉多項疏失---------- 3

國內基金系統遭駭 企業機密恐嚴重外洩 ---------- 8

Google 將加強對未滿 18 歲用戶的隱私保護---------- 12

房仲神器違法蒐集與販售個人資料---------- 16

Android 新木馬病毒藏身免費 App 挾持數千個 Facebook 帳號 ---------- 20

上士入侵軍用電腦竊取少校前夫兵資 從重判刑 ---------- 25

美國 FCC 禁華為、中興等中企產品 ---------- 28

假網站釣個資銀行用戶遭詐---------- 31

中國駭客疑似鎖定我國重要機關組織 須嚴加防範---------- 36

美國 NASCIO 發布採購指引整合資安需求 ---------- 40

國內某基金會個資外洩，影響 2,000 名考生---------- 45

求職面試時雇主要求面試者提供疫苗接種證明，是否適法？ ---------- 49

高中生「學習歷程檔案」因委外廠商失誤而遺失---------- 54

外洩 5.33 億筆個資 Facebook 未通知受害人 ---------- 58

NCC 抽查台灣 15 款熱銷手機資安！ ---------- 62

美國警局成為受害者 駭客洩漏大量資料 ---------- 66

立委批員警洩漏個資懲戒標準輕 內政部：通盤檢討---------- 70

五倍券數位綁定相關資安議題 ---------- 75

GCP 服務完成金融雲端委外獨立第三方單位查核---------- 80

愛心協會大規模捐款個資外洩，關鍵在於資訊服務廠商---------- 85

聚焦資安專業人才培訓：美國的共同責任 vs.台灣的公私協力 ---------- 90

金融機構之資通安全長設置義務---------- 93

貳、資訊公開(DISCLOSURE)----------97

立院三讀 不當勞動行為裁決書原則應予公開---------- 98

落實公民參與 全台 22 地方議會均已公開議事資訊----------102

參、資訊監察(MONITORS) ---------- 106

簡訊實聯制使用爭議 前法官：應立法明定----------107

智慧型兒童手錶之後門資安漏洞----------111

肆、資訊應用(APPLICATION)---------- 115

歐盟執委會提出人工智慧法令，制定一致性規則草案----------116

衛福部官方「台灣社交距離」App 登場！ ----------120

微軟啟用「無密碼登入」新趨勢----------124

歐盟對抗假消息之實務準則與指引----------128

伍、自我評量---------- 133

是非題----------134

選擇題----------141

壹、資訊保護(Security)

類別：資訊保護【案號：S11001】

美國人口統計局 IT 管控遭糾舉多項疏失

【焦點話題】

美國商務部檢核長辦公室(Department of Commerce Office of Inspector General, OIG)於 2021 年 8 月 16 日發布一份調查報告[1]，內容為 2020 年 1 月美國人口統計局(Census Bureau)所管理的伺服器遭到公開可取得的弱點利用工具攻擊。這些伺服器主要是用於員工遠端存取以進行任務作業、開發及實驗之用。攻擊者企圖遠端執行程式碼，成功變更了系統上使用者帳號資料，但是未能在系統上植入後門程式，因此攻擊者未能成功駭入該單位網路。

但 OIG 認為人口統計局仍有下列缺失：未及時修補重大漏洞、未及時發現並報告該事件、未保存足夠的系統軌跡紀錄(Log)、未執行事故評估與改善的管理程序、持續使用供應商已不支援服務的伺服器等。

【參考資料來源：三立新聞，109/11/06】

【重點摘要】

1. 從資通安全風險管理的角度檢視本案可知，如遭駭客入侵，即使其未成功植入後門程式或造成其他損害，仍應即時進行通報並進行相關問題之發現、處理及改善。

2. 因應資安事件的有效做法包括：建立及時通知系統管理人員重大漏洞的程序、定期檢視更新漏洞掃描清單並進行掃描、檢視自動警示系統確保可發現相同類型的攻擊、確保能及時通報已查明之資安事件、定期檢視系統 Log 以確保 IT 資產正常、在資安政策中規定執行資安事件事後改善的時程要求、建立生命週期終止產品的優先除役計畫等。

[1]The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement(網址： https://www.oig.doc.gov/OIGPublications/OIG-21-034-A.pdf，最後瀏覽日：110 年 8 月 23 日)

【法律觀點】

為有效因應資通安全事件，從風險管理的角度出發，應包括事前安全防護、事中緊急應變及事後復原等程序。以公務機關為例，目前資通安全管理法、資通安全管理法施行細則與資通安全事件通報及應變辦法中，針對事前、事中與事後之管理均有相對應之規範。在事前，各公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫[2]，並應訂定通報及應變機制[3]，且應每年向上級或監督機關提出資通安全維護計畫實施情形[4]，並應就資通安全事件之通報與應變訂定作業規範[5]。

於事中，於知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關[6]。其通報時間應於知悉資通安全事件後，一小時內依主管機關指定之方式及對象，進行資通安全事件之通報[7]。如因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由[8]。除通報外，公務機關知悉資通安全事件後，第一級或第二級事件，應於知悉該事件 72 小時內，第三級或第四級事件，應於知悉該事件 36 小時內，完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜[9]。

而事後，應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關[10]。該報告除了事件的發生紀錄、影

[2] 資通安全管理法第 10 條。

[3] 資通安全管理法第 14 條第 1 項。

[4] 資通安全管理法第 12 條。

[5] 資通安全事件通報及應變辦法第 9 條、第 10 條。

[6] 資通安全管理法第 14 條第 2 項。

[7] 資通安全事件通報及應變辦法第 4 條第 1 項。

[8] 資通安全事件通報及應變辦法第 4 條第 3 項。

[9] 資通安全事件通報及應變辦法第 6 條第 1 項。

[10] 資通安全管理法第 14 條。

響評估、損害控制評估及調查處理之歷程外，更重要的是事件根因分析，與防範類似事件再次發生所採取之措施，與相關措施預定完成時程與成效追蹤機制[11]。相關調查、處理及改善報告，並應於完成損害控制或復原作業後一個月內，依主管機關指定之方式送交之[12]。

【管理 Tips】

根據 OIG 此次報告所給的建議，可知如機關遇到類似風險，亦可採取相關管理措施以處理風險，並可避免資安事件發生：

首先，儘管美國國家標準技術研究院(National Institute of Standards and Technology)已於事件發生前即召開相關會議，並針對該漏洞利用問題進行討論與提出相關因應措施，統計局並未能有效落實相關因應措施。且亦未利用定期漏洞掃描即時發現此一漏洞。因此建立及時通知系統管理人員重大漏洞的程序、並定期檢視更新漏洞掃描清單並進行掃描，可有效降低事件發生的機率。

其次，統計局的防火牆於 1 月 13 日即成功阻擋駭客的攻擊，但直到 1 月 28 日統計局才意識到伺服器已遭受攻擊，究其原因，是統計局未能利用資安資訊與事件管理工具(Security Information and Event Management Tool, SIEM)，對有可疑的網路活動進行主動警示。且亦未能及時將相關受侵害資訊進行內外部通報，故檢視自動警示系統確保可發現相同類型的攻擊、而及時通報已查明之資安事件方能結合各方資源以有效因應相關攻擊。

另外，統計局僅透過供應商預設的 Log 規模儲存 Log，因此所存之 Log 不足以分析此次事件，因此應定期檢視系統 Log 儲存設定，以確保 IT 資產正常。

而檢視統計局的資安事件應變政策，並未規定執行資安事件事後分析改善的時程要求，應於政策納入此一部分，方能透過事件後所得之經驗改善其作業流程。

最後，本報告調查中發現統計局至 2021 年 2 月仍在使用此次事件中受攻擊之伺

[11] 資通安全管理法施行細則第 8 條。

[12] 資通安全事件通報及應變辦法第 6 條第 2 項。

服器，而這些伺服器已過使用期限，服務供應商不會再更新安全修補程式，也不會提供維護服務，持續使用這樣的系統會產生漏洞被利用的持續性風險，因此應建立生命週期終止產品的優先除役計畫以降低此一風險。

另外，針對本事件，亦可參考最新修正資通安全責任等級分級辦法附表十資統系統防護基準中相關防護做法，如依據日誌儲存需求，配置所需之儲存容量；定期確認資通系統相關漏洞修復之狀態，並測試其有效性及潛在影響；監控資通系統以偵測攻擊與未授權之連線，而採用自動化工具監控進出之流量並進行分析，則可管理更高之風險。

【相關標準】

ISO 27001:2013(CNS 27001)

- A.8.3.2 媒體之汰除

  (1) 標準內容： 當不再需要媒體時，應使用正式程序加以安全汰除。

  (2) 適用說明： 本案中統計局應建立生命週期終止產品的優先除役計畫淘汰已過期的伺服器以降低漏洞被利用的風險。

ISO27001:2013(CNS27001)

- A. 12.2.1 防範惡意軟體之控制措施

  (1) 標準內容： 應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。

  (2) 適用說明： 利用 SIEM，對有可疑的網路活動進行主動警示，以確保可發現相同類型的攻擊。

ISO27001:2013(CNS27001)

- A.12.4.3 管理者及操作者日誌

(1) 標準內容： 應存錄系統管理者及操作者之活動，且應保護及定期審查該日誌。

(2) 適用說明： 定期檢視 Log 系統的規模與運作狀態，方可提供資安事件調查之有效資訊。

ISO27001:2013(CNS27001)

- A.12.6.1 技術脆弱性管理

(1) 標準內容： 應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

(2) 適用說明： 建立及時通知系統管理人員重大漏洞的程序、並定期檢視更新漏洞掃描清單並進行掃描，可有效降低資安事件發生的機率。

關鍵字	資通安全事件、資通安全事件通報應變、定期漏洞掃描、自動警示系統、日誌 Log 管理、資通系統、防護基準

類別：資訊保護【案號：S11002】

國內基金系統遭駭 企業機密恐嚴重外洩

【焦點話題】

國內某基金之創業投資電腦系統於 110 年 6 月底遭到大陸駭客惡意入侵，導致系統主機被植入病毒程式。遭到入侵的資料庫內存有企業投資與融資業務資料，包含轉投資事業基本資料、財務報表及會議記錄、貸款專案內容及執行情形等。同時遭到入侵的還有人事資料相關之資料庫，資料庫內包含委員、股權代表及員工的個資。因所涉包括個人資料等重要資料，已被通報為資通安全事件。該基金於知悉事件後，已立即阻斷不當連線並採取處理措施，且經初步盤點數位軌跡，並未發現有資料遭竄改或竊取之情事。

經調查後發現，該基金委託銀行建置之電腦系統，似有資安維護措施不足之情形；銀行則表示其歷年來協助進行相關資安管理並提供資安建議，包括：Windows Update、防毒更新、防火牆及入侵防禦系統維運、伺服器系統備份等資安維護措施。

【參考資料來源：中時新聞網，110/7/23；國家發展委員會新聞稿，110/7/23】

【重點摘要】

1. 當受託維運資通系統之機關發生資通安全事件時，應儘速通知委託機關，以利委託機關依照資通安全管理法所規定之時間，按照資通安全事件之等級，進行相關通報與應變作業。
2. 機關依據調查結果，應迅速採取降低或解除風險之措施，並進行復原，如封閉相關系統對外連線、重新設定存取控制措施、清查是否有資料遭受破壞或外洩。除此之外，亦應透過根因分析，逐步調整現有作法，如增加相關資安人力資源，或更新資料庫管理方式，以避免資通安全事件再次發生。

【法律觀點】

本案因受駭標的一創業投資電腦系統遭植入病毒程式，且資料庫遭入侵而導致有資料外洩之疑慮，已符合資通安全事件之認定。如屬資通安全管理法 為例進行介紹，除應依規定迅速向上級、監督機關及主管機關通報外，更重要的應該是能夠儘速控制或復原損害，依資通安全事件通報及應變辦法第 6 條規定，公務機關知悉資通安全事件後，關於第三級資通安全事件，應於知悉該事件後三十六小時內，完成損害控制或復原作業。本案之受託廠商亦已召開緊急會議，同時裝設網路監控系統進行偵測及側錄。第一時間封閉該系統及網域的對外連線，並將惡意程式的特徵碼回報給資安防毒公司，作為第一線的阻擋防護外，在系統防護未確保提升前，不對外提供連線。只允許特定人士可以存取該系統；透過重新設定網域和系統管理員的帳號、密碼，清查所有使用者身分，不僅釐清所有代理人之間的存取權限和關係，也暫停使用不必要的網路共用帳號、密碼，並進行系統的漏洞修補和主機重置，徹底清除惡意程式[1]，可在第一時間將系統被不當利用之風險降低與解除。

此外，由於本案涉及系統委外建置，該機關應依資通安全管理法第 9 條與資通安全管理法施行細則第 4 條，監督受託廠商對於該系統之資通安全維護情形，而應監督之要項包括：受託者應具備完善之資通安全管理措施或通過第三方驗證；受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員；對複委託之管理；涉及國家機密之受託人員之適任性查核；系統開發相關之安全性檢測與授權證明；受託者違反法令或知悉資通安全事件時之通知與補救義務；委託關係終止或解除時，確認受託者返還、移交、刪除或銷毀因履約所持有之資料；對受託者之稽核等[2]。

【管理 Tips】

除針對資通安全事件的通報與緊急應變外，為避免後續再次發生類似資安事件，

[1] 基金系統遭中國駭客入侵，通報為資安事件 (網址：https://www.ithome.com.tw/news/145842 ，最後瀏覽日：110 年 8 月 31 日)。

[2] 資通安全管理法施行細則第 4 條。

提出完整的資通安全事件調查、處理及改善報告，包括事件根因分析、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施等[3]。於本案中，所採取的相關分析與後續管理措施包括[4]：

- 在資通系統委外之情形下，可參考政府資訊作業委外資安參考指引中，對委外廠商服務之監視與審查之方式。除了通案要求委外廠商依循採購文件載明之資安要求事項辦理外，可透過書面審查，如取得委外廠商第三方審查報告、內部稽核報告、自動化工具掃描之報告或自我評估報告等，以進行監管。如評估委外系統風險更高時，亦可由委託機關自行召集適切之稽核人員至受託廠商地點進行稽核[5]。
- 回報發現到的惡意程式特徵碼給相關的資安防毒業者，未來只要有類似的惡意程式入侵系統，可提升防毒軟體攔阻的成功率。
- 因系統老舊，某些系統監控資料因為儲存空間不足而遭到資料覆寫，故應適當增加儲存空間以提升系統監控效率，並使系統監控資料可以適切保存，有利為未來查核。
- 加強組織本身資訊、資安人員的配置，搭配外部資安專業機構的協助，更能確保整體系統的安全性。

【相關標準】

ISO27001:2013(CNS27001)

- A.15.2.1 供應者服務之監視及審查

  (1) 標準內容： 組織應定期監視、審查及稽核供應者服務交付。

  (2) 適用說明： 於本案中，係因委外建置之系統遭駭客侵入，而有資訊

[3] 資通安全管理法施行細則第 8 條。

[4] 同註 2。

[5] 政府資訊作業委外資安參考指引：3.4.2.5.5 委外廠商服務交付管理。

外洩之風險，若有資訊服務或系統委外者，對於受託之單位仍應以稽核或其他適當方式，善盡監督之責任。

ISO27001:2013(CNS27001)

- A.16.1.2 通報資訊安全事件

(1) 標準內容： 應循適切之管理管道，儘速通報資訊安全事件。

(2) 適用說明： 於本案中，應由發現事件之單位儘速通報內部資安管理單位，其後再依據資通安全管理法之規定，通報管權責機關。至於通報之方式，公務機關為利用「主管機關指定之方式」，即利用國家資通安全通報應變網站(https：//www.ncert.nat.gov.tw/)辦理通報業務。

ISO27001:2013(CNS27001)

- A.16.1.6 由資訊安全事故中學習

(1) 標準內容： 應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。

(2) 適用說明： 如上所述，應提出完整的資通安全事件調查、處理及改善報告，透過事故根因分析，並採取防範類似事件再次發生之管理、技術、人力或資源等層面之措施。

關鍵字	資通安全事件通報應變、駭客攻擊、資料庫入侵、資訊委外、資通安全

類別：資訊保護【案號：S11003】

Google 將加強對未滿 18 歲用戶的隱私保護

【焦點話題】

科技進步與資訊量增多，影響了現代人的生活方式，兒童與青少年花更多時間上網，引起家長、社會團體關心兒童與青少年因網路活動而產生的隱私問題。為因應來自家長與社會團體的批評，Google 近來重新調整服務辦法與個人資料蒐集的內容與使用方式，以避免對兒童、青少年使用者造成不良影響。其修正包括：將 13 歲至 17 歲之 YouTube 使用者預設為最高等級隱私保護，這表示這些使用者所上傳之內容預設為私人影片，僅本人及指定分享對象才能看見，避免未成年使用者在未留意情況下，將個人影片公開於網路。此外，Google 將防止 18 歲以下的用戶接觸到針對其年齡、性別、興趣等所投放的精準廣告(targeting ads)，且允許 18 歲以下用戶及其父母或監護人要求從 Google 圖片搜尋結果中刪除未成年人的圖片。

【參考資料來源：UPI，110/08/10；DEADLINE，110/08/10】

【重點摘要】

1. 我國個資法就未成年人告知同意、權利行使並無特別規定，因此關於未成年人行使個資法上相關權利，應回歸適用民法有關行為能力之一般規定，何時須法定代理人同意，何時得由未成年人自行處理，於個案適用上難免有模糊空間。

2. 相較於我國法制，美國聯邦法針對 13 歲以下的兒童頒布兒童線上隱私保護法(Children's Online Privacy Protection Act, COPPA)，針對企業蒐集兒童個資所應踐行的告知同意，規定應取得父母同意，並且父母同意的過程必須是可以驗證的。此法案特別考量兒童於數位平台的使用上可能之隱私議題，並以父母介入監督作為必要條件，對未成年人的保護更加完善，可作為企業實踐或是未來修法的建議方向。

【法律觀點】

我國兒童及少年福利與權益保障法中，將未滿 12 歲之人稱為兒童、12 歲以上未滿 18 歲之人稱為少年[1]，針對兒童及少年的隱私保護，我國多聚焦於兒少案件的隱私[2]、或是新聞媒體播報兒少案件時，對其個人資訊之隱匿。但是對於一般兒童與少年使用數位媒體或平台的隱私保障，仍仰賴個人資料保護法(下稱個資法)對個資蒐集、處理、利用的規定，又個資法就未成年人告知同意、權利行使並無特別規定，是關於未成年人行使個資法上相關權利，應回歸適用民法有關行為能力之一般性規定。

過往實務案例中，有教材業者以贈品利誘學童提供個人資料，國家發展委員會(下稱國發會)依照個資法第 5 條[3]、第 7 條第 1 項[4]、第 8 條第 1 項[5]之規定，以及個資法施行細則第 16 條[6]之規定，認為若欲基於當事人同意蒐集個人資料，應明確告知應告知事項，使當事人充分瞭解後審慎為之，且告知之方式，應以足以使當事人知悉或可得知悉之方式為之。由於學童多為未成年人，教材業者之告知方式應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使該學童得以充分瞭解其個人資料之後續利用。倘教材業者未完整踐行

---

[1] 兒童及少年福利與權益保障法第 2 條。

[2] 兒童及少年福利與權益保障法第 61、66 條參照。

[3] 個人資料保護法第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」

[4] 個人資料保護法第 7 條第 1 項：「第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。」

[5] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

[6] 個人資料保護法施行細則第 16 條：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」

告知，或其告知對象無法充分瞭解其個人資料之後續利用，則未能符合個資法第 7 條告知後取得同意之規定[7]。

相較於我國法規定，美國之兒童線上隱私保護法(Children's Online Privacy Protection Act of 1998, COPPA)[8]係於 1998 年頒布、2000 年生效、針對美國公司於美國境內或境外蒐集 13 歲以下兒童個人資料所頒布之法案，其中規定網站營運商若欲蒐集 13 歲以下兒童之個人資料，應於網站上說明將蒐集兒童的哪些資訊、如何利用此類資訊等[9]、按照法令取得可驗證之父母同意(Verifiable parental consent)[10]、符合資料保留與刪除之規定，並禁止以參加遊戲、提供獎品或其他條件，讓兒童提供超過所需之個人資訊[11]。此法案特別考量兒童對於數位平台的使用，並直接加入父母監督要素做為告知同意之條件，不待回歸其他法律的適用，對未成年人保護更為完善，或可作為未來修法之參考方向。

【管理 Tips】

企業如從事跨國資料蒐集時，必須清楚盤點並知悉各國相關個人資料保護或是隱私之相關規定。例如美國企業在台灣營業、蒐集台灣人民之個資，必須要遵循台灣的個人資料保護法，同樣地，企業若在歐盟境內設有據點或是對歐盟境內的個人蒐集個資，則有歐盟一般資料保護規則(General Data Protection Regulation)之適用。

盤點個資暨隱私相關法令規定後，則進一步需於公司內部程序、產品與服務設計中加入法遵與隱私設計。尤其隱私設計上，對於可能使用產品或服務的受眾，應考量其年齡，對於未成年的使用者，宜拉高其隱私保護層級，例如上傳內容的預設保護、精準廣告的投放限制等均屬須注意之處，此外，產品設計上讓父母或監

[7] 有關教材業者以贈品利誘學童提供個人資料所涉個人資料保護法之合法性？ (網址: https://pipa.ndc.gov.tw/nc_11980_32426 ，最後瀏覽日：110 年 9 月 2 日)

[8] 15 U.S.C. §§ 6501–6506

[9] 5 USC 6502.

[10] 15 USC 6501(9).

[11] 15 USC 6502.

護權人得以監督未成年人的之使用，也是業界的良好實踐。

【相關標準】

ISO27001:2013(CNS27001)

- A. 18.1.4 個人可識別資訊之隱私及保護

  (1) 標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

  (2) 適用說明： 公司應定期盤點應適用的法令與法規，尤其需特別注意隱私與個人資料保護的相關規定，以美國公司為例，若其產品、服務或是營運上有蒐集兒童的個人資料，必須將兒童線上隱私保護法(COPPA)的規定納入法令遵循的範疇。

ISO 29100 :2011(CNS29100)

- 4.7 隱私控制措施

  (1) 標準內容： 組織宜發展隱私控制措施作為其「隱私設計」作法之一部分，亦即隱私遵循宜於 PII 處理之系統設計時期即納入考量而非於後續階段方納入。(摘錄)

  (2) 適用說明： 隱私設計是指產品或是服務在設計上必須符合法律規定，且蒐集處理個人資料應具備適當性、關聯性以及與處理資料目的時的必要性。例如對兒童與青少年的隱私保護預設為私人影片，即為一種隱私設計的做法。

關鍵字	兒童線上隱私保護法(COPPA)、個人資料保護法、未成年人個資告知

類別：資訊保護【案號：S11004】

房仲神器違法蒐集與販售個人資料

【焦點話題】

前房仲業者編寫「People」查詢系統(俗稱房仲神器或小白機)，蒐羅全台民眾房產個資高達 1 億 8 千萬筆，內容包括全台人民持有房產、住址、工作經歷、聯絡手機及生日、身分證資料等，檢警所搜扣之查詢系統資料庫容量達 220G 並以一台數萬元的價格銷售給其他房仲業者謀利。

【參考資料來源：聯合新聞網，2021/08/18，自由時報，2021/08/18】

【重點摘要】

1. 我國個資法第 41 條規定，意圖營利而違法蒐集、處理、利用個人資料，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。
2. 企業應定期或不定期對其所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。尤其若有營利意圖而違法的行為，將會面臨民、刑事責任。

【法律觀點】

依據我國個人資料保護法(下稱個資法)之規定，若欲蒐集、處理、利用他人個資，應符合特定法定要件。該法第 19 條規定，除特種資料外，非公務機關對個人資料之蒐集或處理，應有特定目的，並符合 8 種法定情形[1]。同法第 41 條則規定：意圖營利而違法蒐集、處理、利用個人資料，足生損害於他人者，處五年以下有

[1] 個人資料保護法第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

期徒刑，得併科新臺幣一百萬元以下罰金[2]。另外，同法第 29 條亦規定其民事賠償責任：非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，應負損害賠償責任。

本案例中大批民眾個資，係先由該前房仲業者蒐集後，編寫系統並進一步向其他房仲業者銷售謀利；其他房仲業者向其購買後，再進行各自對個資的利用，因此在個資的蒐集階段即須依照屬於直接或間接之蒐集方式，而應符合相應要件。若係直接蒐集者，應於蒐集前為個資法第 8 條之告知並取得同意[3]；若係間接蒐集者，亦應依第 9 條第 1 項之規定於處理或利用前踐行告知義務[4]。另應特別注意者，係各產業的中央目的事業主管機關得依據個資法第 27 條指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。以本案的不動產經紀業為例，內政部訂有「不動產經紀業個人資料檔案安全維護管理辦法」，該辦法第 10 條明確指示不動產經紀業應區分直接蒐集與間接蒐集的個資的情形，並分別訂定告知方式、內容及注意事項，並要求所屬人員確實辦理。以下將針對案例中兩種不同主體進行討論：1. 蒐集個資並販賣的前房仲業者；2. 收受資料的其他房仲業者。

以蒐集個資並販賣的前房仲業者為例，其若未於蒐集前或處理與利用前踐行告知義務，亦無個資法第 19 條的法定情形，已屬於違法蒐集、處理個資的情況；又，其隨後將其違法蒐集所得之個資販賣給其他房仲業者，販售行為屬於個資法上的利用行為[5]，本應依個資法第 20 條之規定，於蒐集之特定目的必要範圍內為之，

---

[2] 個人資料保護法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

[3] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

[4] 個人資料保護法第 9 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。」

[5] 個人資料保護法第 2 條參照。

或需符合特定目的外利用情形，本案中的情節顯然並未遵守此一要求。

至於收受資料的其他房仲業者，其收受資料的行為屬於間接蒐集之情形，應於處理及利用前踐行告知、取得當事人同意，並於特定目的為利用，始為適法的行為。

【管理 Tips】

本案係屬於非公務機關對個資的違法蒐集、處理、利用。房仲屬於不動產經紀業，對於個人資料蒐集、處理及利用應符合個資法第 19 條及第 20 條規定，為防免員工因缺少法律意識而有觸法之可能，業者應定期或不定期對其所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

【相關標準】

ISO 27001:2013(CNS 27001)

- A.18.1.4 個人可識別資訊之隱私及保護

  (1) 標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

  (2) 適用說明： 個資保護法中有關於刑事、民事責任之規定，企業若涉及個人資料的蒐集、處理及利用，應特別注意規範內容，確認個人的隱私與資料均依循法律規範而有完善保護。

ISO 27001:2013(CNS 27001)

- A. 7.2.2 資訊安全認知、教育及訓練

  (1) 標準內容： 組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2) 適用說明： 對個人資料蒐集、處理及利用應符合個資法規定，企業應定期或不定期對其所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

關鍵字	個人資料保護法、不動產經紀業個人資料檔案安全維護管理辦法、認知宣導、教育訓練

類別：資訊保護【案號：S11005】

Android 新木馬病毒藏身免費 App　挾持數千個 Facebook 帳號

【焦點話題】

新的木馬程式 FlyTrap 從 2021 年 3 月開始席捲 140 個國家，透過社交媒體、第三方應用程式商店，入侵超過 10,000 名受害者的裝置，並利用社交工程挾持 Facebook 帳號。

FlyTrap 使用某些吸引人的主題，例如 Netflix 或 Google AdWords 的免費優惠券代碼、或是投票選出最佳足球員活動等，這類免費程式會搭配精美設計介面，並使用社交工程，引誘使用者下載。使用者不僅可透過 Google Play 或第三方 Android 市集下載，也可從一般網站直接下載。下載後，FlyTrap 會以投票、收集優惠卷代碼或累積積分等理由引導使用者登入 Facebook 帳戶，並蒐集受害者的 Facebook 名稱、位置、電子郵件、IP 位置及和 Facebook 帳號相關 Cookie 等個人資訊。隨後，FlyTrap 會再利用這些帳戶作為殭屍網路，用以進行惡意攻擊，如散布惡意程式、不實資訊等。

【參考資料來源：科技新報，110/8/11】

【重點摘要】

1. 木馬程式與社交工程已經成為資訊安全的最大威脅之一，除了政府單位、關鍵基礎設施之外，企業對於資料保護也相當重視。至於個人電腦、手機等終端裝置，因為很高機率與社交媒體帳戶、銀行應用程式、企業工具等綁定連結，資料含金量高，易成為惡意攻擊之對象。

2. 木馬程式 FlyTrap 挾持用戶 Facebook 帳戶，損害了機密性、完整性與可用性。可知全民資安意識的提升甚為重要，雖然 Google 已經將嵌入有 FlyTrap 的應用程式於 Google Play 商店下架，但類似之攻擊或威脅仍持續存在。用戶於下載免費應用程式應特別注意類似攻擊模式，也建議安裝防毒應用軟體，以偵測木馬或是惡意程式之威脅。至於企業則

應訂定相關行動裝置使用政策，使員工下載應用程式時應遵循公司之政策與程序，以確保資通安全。

【法律觀點】

資通安全管理法第 7 條第 1 項規定：「主管機關應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；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之。」而該條授權訂定之資通安全責任等級分級辦法中，附表一(資通安全責任等級 A 級之公務機關應辦事項修正規定)、附表三(資通安全責任等級 B 級之公務機關應辦事項修正規定)於今(民國 110 年)年增訂「端點偵測及應變機制」之應辦事項[1]，要求 A 級、B 級公務機關應於初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。

又所謂端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業[2]。若設備端有進行前述端點管理，則如 FlyTrap 等木馬程式侵入，或有大量蒐集個資的異常活動，端點偵測及應變機制將能掃描偵測並記錄惡意程式的行為，以進行分析，提高資安防護的能量。

此外，資通安全管理法第 3 條說明資通安全是指「防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。」機密性(Confidentiality)指的是資訊的存取須經過授權；完整性(Integrity)是確保資訊的內容正確且完整；可用性(Availability)則是確保經授權的使用者，能存取及使用資訊。若系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作時，

[1] 附表一、附表三中，同時新增者還包括「資通安全弱點通報機制」，要求被核定的 A 級和 B 級公務機關一年內，完成資安弱點通報機制導入作業。

[2] 參照資通安全責任等級分級辦法附表一、附表三的備註六。

即構成資通安全政策之威脅而形成資通安全事件。

本案例中，木馬程式 FlyTrap 挾持用戶 Facebook 帳戶，進而利用社交工程散播含有木馬程式的惡意連結、宣傳虛假消息與活動，影響用戶對帳戶的控制與使用，同時損害了機密性、完整性與可用性，可能已構成資通安全事件，如為資通安全管理法之公務機關或特定非公務機關時，則亦應資通安全管理法相關規定進行通報與後續處理。

【管理 Tips】

FlyTrap 以投票、收集優惠卷代碼或累積積分等理由引導使用者登入 Facebook 帳戶，並蒐集受害者的個人資訊。FlyTrap 使用了 JavaScript injection 的技術，在 WebView 中配置了注入 JavaScript 程式的功能，只要使用者用該 WebView 開啟 URL，就能夠注入惡意 JavaScript 程式並擷取所有必要的資訊，包括 Facebook 名稱、位置、電子郵件、IP 位置及和 Facebook 帳號相關 Cookie 等[3]。

行動裝置的使用與個人日常生活習習相關，為了居家工作或是移動方便，許多公司的資訊系統也會與行動裝置相連接，因此管理行動裝置的使用也成為組織保護資訊系統的重要環節。FlyTrap 等木馬程式或惡意威脅利用用戶對於手機等終端裝置的使用習慣，竊取大量個人資訊，且傳播容易，可以輕易挾持眾多社交媒體帳號，產生巨大的影響。又許多公司會請員工於私人手機中下載並使用企業工具，或配發公務手機、公務筆電供員工使用，為避免受到類似 FlyTrap 等木馬程式的攻擊，企業應訂定相關行動裝置使用政策，包括軟體下載與使用時，應僅安裝來自可信任來源之軟體、注意軟體安裝時所要求之權限是否合理、安裝資安防護軟體、定期進行軟體更新或修補作業等[4]，並更新常見的惡意攻擊資訊，提醒員工下

[3] Aazim Yaswant, FlyTrap Android Malware Compromises Thousands of Facebook Accounts, ZIMPERIUM, August 9, 2021. (網址：https://blog.zimperium.com/flytrap-android-malware-compromises-thousands-of-facebook-accounts/ ，最後瀏覽日：110 年 11 月 16 日).

[4] 有關行動裝置的資安防護，可以參考行政院國家資通安全會報網站上所公告之行動裝置資通安全注意事項(簡要版)(網址：https://nicst.ey.gov.tw/Page/16FFA138E66A0905/a91dad4c-11e6-43e7-a4bb-

載應用程式或軟體時應遵循公司政策與程序，以確保資訊安全。

FlyTrap 只是竊取網路平台帳號憑證的眾多威脅之一，雖然於收到通報之後，Google 已經立即將嵌入有 FlyTrap 的應用程式於 Google Play 商店下架。但第三方 Android 應用市集與各式提供免費應用程式下載的網路平台，則持續有其蹤跡。用戶於下載免費應用程式應特別注意是否有類似登入社交平台帳號取得優惠的吸引要素，也建議安裝防毒應用軟體偵測木馬或是惡意程式的威脅。

【相關標準】

ISO 27001:2013(CNS 27001)

- A.6.2.1　行動裝置政策

(1) 標準內容：　應採用政策及支援之安全措施，以管理使用行動裝置所導致之風險。

(2) 適用說明：　許多公司的資訊系統會與行動裝置相連接，因此管理行動裝置的使用也成為組織保護資訊系統的的重要環節。組織應頒布有關行動裝置的使用政策，例如針對公務機禁止下載與工作無關的應用程式。

ISO 27001:2013(CNS 27001)

- A.12.5.1　運作中軟體之控制

(1) 標準內容：　應實作各項程序，以控制對運作中系統之軟體安裝。

(2) 適用說明：　透過引誘下載、社交工程等方式進行帳號挾持或是裝置入侵，因此造成組織損害的情形逐年增加。組織應透過管理手段對於軟體安裝的行為加以控制，保護資訊系統。

23af28029988，最後瀏覽日：110 年 11 月 16 日)

關鍵字	木馬程式、惡意攻擊、資通安全管理法、行動裝置使用政策

類別：資訊保護【案號：S11006】

上士入侵軍用電腦竊取少校前夫兵資 從重判刑

【焦點話題】

陳姓少校發現其於部隊遭懲處之資料被邱姓男子公布於網路，軍方查知，陳姓少校前妻郭姓上士與陳男有婚姻紛爭，郭女利用陳男帳號密碼入侵軍用公務電腦，取得陳男受懲處之相關資料，交由邱男公布，檢方偵辦後，認為郭女有無故取得公務機關電腦電磁紀錄及洩漏國防以外應秘密消息犯意，依法起訴。地院則認為郭女行為恐造成軍方人員身分保密破口，對軍隊內部管理及國防秘密保護影響重大，從重以公務員利用職務上機會，無故取得公務機關電腦電磁紀錄罪論處。

【參考資料來源：自由時報，109/12/27】

【重點摘要】

1. 公務員因職務之便利，侵入電腦並洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，可能違反包括刑法洩漏國防以外之秘密罪，以及公務員利用職務上機會，無故取得公務機關電腦電磁紀錄罪等罪名，並應從重依無故取得公務機關電腦電磁紀錄罪論斷。

2. 資料儲存於資通系統內，於判斷資通系統所需之控制措施時，可依資通安全責任等級分級辦法附表九之資通系統防護需求分級原則，以機密性、完整性、可用性與法規遵循性作為判斷標準，區分其防護需求等級，再參考附表十之資通系統防護基準判斷所需進行之控制措施。

【法律觀點】

公務人員若利用職務之便利，未經授權進入公務機關電腦，取得電磁紀錄，或有洩漏、交付國防以外應秘密之文書、圖畫、消息或物品之情形者，可能違反刑法

第 358 條[1]、第 359 條[2]、第 132 條[3]等罪名，以處罰最重之第 359 條來說，最高可處 5 年以下有期徒刑，亦可併科 60 萬以下罰金；如一行為同時觸犯上述數罪名而從重處斷時，即應論以第 359 條之罪。

本案中，郭女利用其身分職務之便，利用陳男之帳號密碼無故入侵公務電腦後並取得其資料，即屬刑法第 358 條規定之「無故輸入他人帳號密碼...而入侵他人之電腦或其相關設備者」;其入侵後並洩漏陳男電子資料予他人，致生損害於陳男及公務機關對於資訊管控之機密安全性，則可能進一步構成刑法第 132 條之「公務員洩漏或交付關於中華民國國防以外應秘密之文書」，及第 359 條規定之「無故取得...他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人」之情形。

【管理 Tips】

公務人員或一般民眾因職務之便所導致之資料洩漏事件時有所聞，資通安全責任等級分級辦法對於系統之防護規定則可參考作為管理控制之手段。除資安法之納管對象以及具備自行或委外開發資通系統者外，組織亦可參照該辦法附表九之資通系統防護需求分級原則，以機密性、完整性、可用性與法規遵循性之防護需求等級作為判斷標準，區分系統防護需求等級，再依附表十之資通系統防護基準判斷所需進行之控制措施，藉以開列系統開發或採購時之需求。以身分驗證一項來說，採用多重認證技術，即可更有效降低假借他人密碼即可登入系統之情形。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.8.2.1　資訊之分級

---

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。」

[3] 刑法第 132 條第 1 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。」

(1) 標準內容：　資訊應依法律要求、價值、重要性急對未經授權揭露或修改之敏感性分級。

(2) 適用說明：　資訊分級應考量限制資訊之營運需要，而組織在考量資訊安全之資訊分級時，可參考資通安全責任等級分級辦法，透過機密性、完整性、可用性以及法規遵循性加以分級，並給予適當保護。

ISO 27001：2013(CNS 27001)

- A.9.4.1 資訊存取限制

(1) 標準內容：　應依存取控制政策，限制對資訊及應用系統功能之存取。

(2) 適用說明：　組織應規範並落實各資通系統之不同使用權限，就各該系統僅允許具使用權之使用者進行系統登入存取。

關鍵字	刑法、資通安全責任等級分級辦法、資料機密性

類別：資訊保護【案號：S11007】

美國 FCC 禁華為、中興等中企產品

【焦點話題】

美國聯邦傳播委員會(Federal Communications Commission, FCC)將 5 家中國企業列入國安威脅清單。FCC 於 2021 年 3 月列出「對國家安全構成威脅的通信設備和服務清單」，禁止接受聯邦政府補貼、資助之網路營運商購買該清單上公司生產之設備與器材，並呼籲未接受聯邦政府資金之營運商將所有不受信任電信設備排除在美國市場之外。當時該清單上有 5 家中國企業，包含：華為、中興通訊、海能達通信、杭州海康威視及浙江大華技術。FCC 代理主席羅森沃賽爾表示不安全的網路設備可能會破壞美國 5G 網絡發展，使外國行為者能夠獲取通訊內容、在網路植入病毒和惡意軟體、竊取私人資訊、從事智財權盜竊以及監視公司與政府機構等惡意活動。

【參考資料來源：新頭殼，110/06/18】

【重點摘要】

1. 政府或民間在採購資通訊設備時，應留意避免使用來自受敵意勢力控制之公司所生產之產品。

【法律觀點】

政府或民間企業之資通設備及服務，若由不受信任之供應商或敵意勢力所控制，該供應商或敵意勢力很可能藉以破壞我國網路安全、竊取個人資訊、進行間諜活動、網路攻擊破壞關鍵基礎設施等。因此美國於 2021 年 3 月 12 日所列出之「對國家安全構成威脅的通信設備和服務清單」，認定含華為、中興通訊、海康威視、海能達和浙江大華等五家中國企業[1]對於美國國家安全和公民安全構

[1] PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES PUBLICATION OF THE LIST OF EQUIPMENT AND SERVICES COVERED BY SECTION 2 OF THE SECURE NETWORKS ACT (網址：https://docs.fcc.gov/public/attachments/DA-21-309A1.pdf ，最後瀏覽日：110 年 8 月 25 日)

成不可接受之風險。

就我國而言，為達維護資通安全之目的，政府或民間在採購及使用資通訊技術設備及服務[2]時，為避免公務及機敏資料遭不當竊取，導致機關機敏資訊外洩或造成國家資通安全危害風險，組織應落實資產盤點、對供應商之可靠性進行評估。尤其受資通安全管理法所規範之機關，更應落實採購安全來源之資通產品，以維護機關資通安全。

【管理 TIPS】

在採購資通安全產品時，應對供應商之可靠性進行評估，落實採購安全來源之資通產品，以維護機關資通安全。

政府單位在採購資通安全產品時，可將下列事項納入考量範圍，以避免採購到具資安風險之非本國產品[3]：

1. 是否屬國內研發、設計或製造之產品(含硬體及軟體產品)。
2. 是否為具我國國籍之自然人或依我國法律設立登記之法人、機構或團體在國內提供之服務，且在臺附加價值率達百分之三十五者。
3. 是否為我國政府電子採購網共同供應契約中原產地標示為臺灣之資通安全產品。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.18.1.1 適用之法規及契約的要求事項之識別

[2] 資通安全管理法第 3 條第 1、2 款：「一、資通系統：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。二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務」

[3] 資通安全自主產品採購原則二。

(1) 標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有法律、法令、法規及契約要求事項，以及組織未符合此等要求之作法。

(2) 適用說明： 當組織屬於中央與地方機關(構)、公立學校、公營事業及行政法人時，應依照政府採購之相關規範進行選商，並進行後續管理。

ISO 27001：2013(CNS 27001)

- A. 15.1.3 資訊及通訊技術供應鏈

(1) 標準內容： 與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應相關聯之資訊安全風險的要求事項。

(2) 適用說明： 組織在進行外部採購時，除應以合約議定相關基礎事項外，協議亦應將資訊安全風險要求事項納入。且應對供應鏈是否具備滿足需求之必要條件且可信賴，進行相對應的背景調查，以降低其不適用之風險。

關鍵字	資通安全自主產品採購原則

類別：資訊保護【案號：S11008】

假網站釣個資銀行用戶遭詐

【焦點話題】

近期傳出數起假冒銀行簡訊之詐騙案件，在誘導民眾點入假頁面輸入帳戶資訊後，再持竊取之帳密資料登入真實銀行頁面，將款項轉出。

主管機關提醒，民眾使用網路銀行及行動銀行比率上升，對近期發生的新詐騙手法，提醒民眾務必注意資訊安全。

主管機關說明，近期傳出詐騙個案，銀行都已在第一時間做出相應處理，受害民眾已向警政單位報案，全案進入調查程序，主管機關並已提醒銀行在官網、網路銀行及行動銀行介面強化客戶交易安全宣導，並應主動提醒客戶不要點選不明簡訊連結，銀行若發現假冒網站，也應立刻通知警政單位。

【參考資料來源：中央通訊社，110/02/09】

【重點摘要】

1. 以詐術之不正手法，使第三人誤信簡訊內容為銀行所寄發之資料而輸入個人資料，並於取得受害人資料進而利用已取得受害人銀行帳戶之財產，可能觸犯刑法第 339-3 條第 1 項不正利用電腦或其相關設備取財罪。
2. 金融資安行動方案提出強化資安監理、深化資安治理、精實金融韌性及發揮資安聯防等四大予資安相關之策勵方向，並據此提列 36 項執行措施，並以此方向修訂資安自律規範，使金融機構有所遵循。

【法律觀點】

本案係民眾收到詐騙簡訊，對方假冒金融機構於簡訊中提供假網站之超連結，使民眾誤認所連結之網頁係銀行所有，進而主動輸入其銀行之帳號及密碼，當對方取得其銀行之帳號及密碼後，遂利用相關資訊侵入民眾銀行帳戶，此係犯

罪者利用社交工程攻擊藉以入侵他人電腦、帳戶等行為，已觸犯刑法第 358 條[1]無故入侵他人電腦罪。同時，犯罪者意圖為自己不法之所有，利用從民眾騙取而來之網路銀行帳號及密碼，轉出受害民眾帳戶內之財產，則觸犯刑法第 339 之 3 條第 1 項[2]不正利用電腦或其相關設備取財罪，上開二罪最重可處七年以下有期徒刑。

另，依個人資料保護法第 27 條之規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏[3]，且中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法[4]，非公務機關應予遵行。

今金融中央目的事業主管機關為金融監督管理委員會，其已針對：金融控股公司、銀行業、證券業、期貨業、保險業、電子票證業、電子支付機構、其他經金融監督管理委員會公告之金融服務業、金融監督管理委員會主管之財團法人等九類非公務機關[5]，規定應依其業務規模及特性，衡酌經營資源之合理分配，配置管理人員及資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法。

隨著資安威脅日益嚴峻，金融主管機關為各金融機構及公會之資安防護訂定金融資安行動方案，作為各金融機構及公會檢討資安策略、管理制度及防護技術等遵循之指引[6]。

---

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。」

[2]刑法第 339 之 3 條第 1 項：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更記錄，而取得他人財產者，處七年以下有期徒刑。」

[3] 個人資料保護法第 27 條第 1 項。

[4] 個人資料保護法第 27 條第 2 項。

[5] 金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第 2 條第 1 項。

[6] 金管會推動「金融資安行動方案」，追求安全便利不中斷的金融服務目標 （網址：https://www.fsc.gov.tw/ch/home.jspid=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202008060003&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News ，

金融資安行動方案中多項執行措施係參考資通安全管理法及其相關子法，包括就資通系統訂定防護基準分級管理；就資通訊環境訂定並要求政府機關導入組態基準，以及因應資訊系統委外風險於防護基準納入系統發展生命週期管理各階段控制措施[7]；委外辦理資通訊系統之建置、維運或資通服務之提供，於選任及監督受託者時應注意事項[8]；要求機關應導入資通安全管理標準，並透過第三方獨立機構驗證資安管理之有效性[9]；引導金融機構重視資安人員之資格能力等事項，均係參考資通安全管理法進行調整[10]。

除此之外，金融資安行動方案亦要求一定規模金融機構或純網銀設置資安長，並由副總經理兼任之[11]，並鼓勵金融機構建置資安監控機制，且透過資安攻防演練以實證其因應攻擊之防禦能量與應變能力[12]。更建立資安情資關聯分析平台[13]，提供金融機構早期預警與防護建議，另透過建立金融資安事件應變體系[14]，以有效因應資安事件，並發揮資安聯防的功能。

【管理 Tips】

面對社交工程可由兩種角度加以觀察，第一，就組織角度而言，組織應對權限加以分級控管，非屬各單位執掌之事務，不應掌握帳號、密碼等特殊權限；安裝防毒軟體，設定個人防火牆，並定期更新病毒碼；針對電腦系統及應用程式隨時更新修補程式；強制設定安全密碼；判定資料等級並予以加密，且可定期辦理社交工程演練[15]。第二，就個人角度而言，應隨時具備危機意識，對於不明

最後瀏覽日 110 年 11 月 1 日）

[7] 金融資安行動方案執行措施彙總表 2.1 說明。

[8] 金融資安行動方案執行措施彙總表 2.3 說明。

[9] 金融資安行動方案執行措施彙總表 5.1 說明。

[10] 金融資安行動方案執行措施彙總表 7.1 說明。

[11] 金融資安行動方案執行措施彙總表 1.1(1)，事實上，此部份亦參考資通安全管理法第 11 條規定，惟該法第 11 條係針對公務機關，對特定非公務機關並無強制要求設置資安長。

[12] 金融資安行動方案執行措施彙總表 9.1。

[13] 金融資安行動方案執行措施彙總表 11.1。

[14] 金融資安行動方案執行措施彙總表 12。

[15] 資通安全事件通報及應變辦法第 18 條：「公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容

來源之可疑電子郵件不予開啟；再次確認訊息來源確為可信任之通知人始可開啟點閱，檢視後仍須保持警覺並勿輕易點擊連結網址或下載檔案；如有下載檔案必要，先將附件檔案另存新檔並以防毒軟體掃描；如有疑似社交工程之行為，應立即回報相關管理單位，並進行事件記錄。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 6.1.3 與權責機關之聯繫

(1) 標準內容： 應維持與相關權責機關之適切聯繫。

(2) 適用說明： 組織針對與資安相關事項，均應有與權責主管機關聯繫之管道，透過積極溝通，或可得到包括資安情資分享，提供金融機構早期預警與防護建議。

ISO 27001：2013(CNS 27001)

- A. 16.1.1 責任及程序

(1) 標準內容： 應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。

(2) 適用說明： 組織應建立自身的對應程序，並以確保資通安全事故發生時，組織人員能依循該文件化的程序進行後續處理。

ISO 27001：2013(CNS 27001)

- A. 16.1.2 通報資訊安全事件

(1) 標準內容： 應循適切之管理管道，儘速通報資訊安全事件。

得包括下列項目：一、社交工程演練。二、資通安全事件通報及應變演練。三、網路攻防演練。四、情境演練。五、其他必要之演練。」

(2) 適用說明： 公務機關與特定非公務機關於資通安全事件發生時，負有通報主管機關或目的事業主管機關之義務，且該通報應依資通安全事件通報及應變辦法加以處理。

關鍵字	個資洩漏、金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法、金融資安行動方案

類別：資訊保護【案號：S11009】

中國駭客疑似鎖定我國重要機關組織 須嚴加防範

【焦點話題】

根據美國資安威脅資料分析公司 Recorded Future 在 7 月 8 日所發布之消息，疑似由中國政府資助之駭客攻擊組織(Threat Activity Group 22, TAG-22)利用 GlassFish 伺服器軟體的漏洞，部署 Cobalt Strike 類型滲透測試工具，後續再透過植入 ShadowPad、Spyder、Winnti 等惡意軟體來進行控管、攻擊。而 Recorded Future 公司旗下的 Insikt Group 團隊，基於網路流量資料分析結果，找到 TAG-22 入侵活動鎖定之具體目標，其中即包含我國某財團法人。依據該發布消息所揭露之部分，該財團法人尚未受到實質侵害，而其亦表示，其資安小組將持續關注此案發展，嚴密監控內部資安環境與資安控管，並持續滾動式調整，以保護重要資產資訊安全[1]。

【參考資料來源：iThome 新聞，110/7/11】

【重點摘要】

1. 境外駭客攻擊我國企業或法人團體網路或電腦系統的行為，可能構成刑法第 358 條與營業秘密法第 13-1 條等罪，而企業或法人團體得藉由依循或參考資通安全管理法第 17 條第 1 項、資通安全管理法施行細則第 6 條與資通安全責任等級分級辦法附表十之資通系統防護基準等相關防護及控制措施，防免該等攻擊行為。
2. 為防範境外駭客攻擊，應建立資通安全完整防護機制、定期進行各種惡意活動檢視、弱點檢測與滲透測試，以及相關社交工程演練。

【法律觀點】

關於本案境外駭客攻擊我國企業或法人團體網路或電腦系統之行為，可自下列幾

[1] 遭中國駭客鎖定？工研院：資安小組已嚴控資訊安全(網址：https://ec.ltn.com.tw/article/breakingnews/3599163 ，最後瀏覽日：110 年 9 月 1 日)

個部分判斷可能適用之法律為何。

本案利用 GlassFish 伺服器軟體的漏洞，部署 Cobalt Strike 類型滲透測試工具入侵的行為，雖尚未成功竊取資料，但仍有可能構成刑法第 358 條無故破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者之罪。

依據該分析消息指出，該攻擊活動很有可能是針對某財團法人所進行相關高科技研發之成果。如該等研發之成果，符合營業秘密之要件(即具有秘密性與經濟價值性並已採取合理保密措施)而可能為營業秘密時[2]，若遭駭客竊取，則該竊取行為將可能構成營業秘密法第 13-1 條竊取營業秘密罪[3]。且由於該駭客組織疑似來自於大陸地區，如後續將竊取所得之營業秘密用於大陸地區，另應適用營業秘密法第 13-2 條之加重處罰規定[4]。

而本案財團法人屬於政府捐助之財團法人，即為資安管理法所規範之特定非公務機關，因此在資安相關法令義務，除依據資通安全管理法第 17 條第 1 項[5]與資通安全管理法施行細則第 6 條[6]，訂定包括資通安全防護及控制措施，與資通安全事件應變機制在內之資通安全維護計畫外，尚應依據資通安全責任等級分級辦法附表十之資通系統防護基準，定期確認資通系統之相關漏洞並加以修復，或監控資通系統，以偵測相關攻擊與未授權之連線。透過相關安全防護措施的控管，降低遭到駭

---

[2] 營業秘密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」

[3] 營業秘密法第 13-1 條：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣一百萬元以上一千萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。」

[4] 營業秘密法第 13-2 條：「意圖在外國、大陸地區、香港或澳門使用，而犯前條第一項各款之罪者，處一年以上十年以下有期徒刑，得併科新臺幣三百萬元以上五千萬元以下之罰金。」

[5] 資通安全管理法第 17 條：「關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」

[6] 資通安全管理法施行細則第 6 條：「本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：…八、資通安全防護及控制措施。九、資通安全事件通報、應變及演練相關機制。…」

客成功攻擊之風險。

【管理 Tips】

本案除利用伺服器漏洞加以攻擊，並透過特製後門程式作為長期存取目標的手段，更進一步會透過假檔名的方式，將惡意程式的執行檔偽裝成履歷文件的 Office 文件檔案，引誘接收者開啟，進而滲透遭受攻擊的單位[7]。在管理上可採取下列方式，因應上述攻擊行為：

- 建置資通安全完整防護機制，包含防毒軟體、網路防火牆、應用程式防火牆、入侵偵測及防禦機制、進階持續性威脅攻擊防禦措施，持續防範可能的惡意程式攻擊。
- 為即時發現可能的攻擊行為，定期進行網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視等，如有對外網站或核心資通系統，並定期辦理網站安全弱點檢測與系統滲透測試。當發現高風險弱點時，應即時修復。
- 為避免遭到偽裝的檔案攻擊，應定期執行社交工程宣導、教育訓練及演練，分享最新社交工程案例。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.7.2.2 資訊安全認知、教育及訓練

(1) 標準內容： 組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

[7] Recorded Future, Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling(網址： https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/，最後瀏覽日：110 年 9 月 6 日)

(2) 適用說明： 機關或組織應提供適當的教育訓練，使同仁均了解常見的入侵手法，例如惡意程式可能偽裝於工作文件或信件內，避免因誤開啟而遭受攻擊。

ISO 27001：2013(CNS 27001)

- A. 12.2.1 防範惡意軟體之控制措施

(1) 標準內容： 應實作防範惡意軟體之偵測、預防及復原控制措施，並合併適切之使用者認知。

(2) 適用說明： 應部署惡意程式防護軟體，對於偽裝文件所包含的惡意程式可加強防護，即便偽裝文件被開啟，仍可即時攔截或避免重要系統被攻擊。

ISO 27001：2013(CNS 27001)

- A.12.6.1 技術脆弱性管理

(1) 標準內容： 應及時取得關於使用中之資訊系統的技術脆弱性資訊，並應評估組織對此等脆弱性之暴露，且應採取適當措施以因應相關風險。

(2) 適用說明： 對組織系統定期弱點偵測或透過流量監控，預防可能的攻擊，如本案中 Recorded Future 結合被動的 DNS 資料，以及敵對 C2 偵測手法，以此探查 Winnti、ShadowPad、Spyder 等後門程式動態。並基於網路流量資料分析結果，能找到 TAG-22 入侵活動鎖定的具體目標。

關鍵字	境外駭客攻擊、營業秘密、定期漏洞掃描、紅隊模擬測試工具

類別：資訊保護【案號：S11010】

美國 NASCIO 發布採購指引整合資安需求

【焦點話題】

美國州際資安長協會(National Association of State Chief Information Officers, NASCIO)於 2021 年 4 月發布了將資安整合於採購程序之指引[1]。考量多數的 IT 採購都在最後階段才讓資安部門加入評估，提供資安保護的程度十分有限，因此本指引強烈建議將從採購最初階段便應納入資安評估，使其成為整體採購程序之一環。本指引特別指出在 IT 環境中，設備或系統使用者需適當地使用與保護相關資源，而管理者必須妥善管理，資安團隊應定義並監控相關系統，最後採購部門負責人員應將安全性納入採購程序考量，並依此產出相關契約。

【參考資料來源：StateTech，110/5/21】

【重點摘要】

1. 進行資訊設備採購之機關，除得依政府採購法授權之辦法於招標文件內就廠商資格訂定限制條件以維護採購時之資安需求外，並應依據行政院相關函令，對於可能導致機敏公務資訊外洩或造成資通安全危害風險之資通訊產品進行妥善的評估與管理，包括不與公務環境介接，並進行汰換等。
2. 對於資訊設備或系統之採購，應於採購初期便納入資安考量，並由各個利害關係人組成共同團隊為之，以降低後續所產生之資安風險。可採用的優良實務做法如對採購過程之參與者，進行資安重要性與潛在的風險之教育、以契約要求供應商採用符合需求程度的資安措施、定期審核供應商之資安水準等。

【法律觀點】

[1] NASCIO, (網址: https://www.nascio.org/wp-content/uploads/2021/04/NASCIO_NASPO_CIS_CybersecurityAquisition_2021.pdf，最後瀏覽日：110 年 9 月 16 日)

目前各國已開始注意到供應鏈之安全性風險問題。為全面性掌握採購之風險，2021 年 2 月拜登總統簽署了 14017 號「保障美國的關鍵供應鏈」行政命令[2]，該行政命令要求聯邦政府各機關應對各該領域之關鍵產業提出風險識別報告與風險處理建議政策，以確保美國之供應鏈不受干擾。如商務部對應半導體製造與先進封裝供應鏈、能源部對應高容量電池與電動車電池供應鏈、衛生及公共服務部對應藥物與活性藥物成分供應鏈等。

而我國目前關於政府機關採購資訊產品之資安相關規定，首先，政府採購法第 17 條第 4 項規定：「機關辦理涉及國家安全之採購，有對我國或外國廠商資格訂定限制條件之必要者，其限制條件及審查相關作業事項之辦法，由主管機關會商相關目的事業主管機關定之。」行政院公共工程委員會基於此一授權，發布了「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」，使採購機關得於招標文件內就廠商資格訂定限制條件，限制投標廠商之國籍或其股東國籍或資金來源。又，依行政院臺護長字第 1090201804A 號函，要求公務機關使用資通訊產品之原則如下：(一)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。(二)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。(三)各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。此外，並應儘速完成汰換所使用或採購大陸廠牌資通訊產品(含硬體、軟體及服務)作業。因此為維護機關的供應鏈安全，從採購、使用與管理都有更多需要機關注意及落實的部分。

【管理 Tips】

除以法令明文禁止採購標的外，亦可參考前述美國相關指引中所述，成功的大規模科技採購，需要各部門的專業知識與共同投入，相關角色應包括：請購單位的代表人、資訊長辦公室、資安長辦公室、技術專家、風險管理專員(含隱私管理專

[2] White House Briefing Room, Executive Order on America’s Supply Chains, (網址: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/，最後瀏覽日：110 年 9 月 21 日)

員)、法律顧問與採購專員等。而此種類型採購應以專案管理方式為之，而非視為傳統單一採購案，並建立專案人員之角色與專案目標，以及應於專案中進行相關風險之評估與處理。

而具體作法方面，該指引建議各州政府在整合採購與資安時，可落實下列作法：

- 採購程序設計方面
  在採購程序初始即納入資安考量並規劃其預算，並確保採購程序與政府資安標準與架構的一致性。

- 採購合約規定方面
  在採購合約中要求供應商或承包商提供其符合政府資安實際措施的證明，透過契約條款與專案管理規劃與執行，建立嚴格的第三方(供應商)的評估與問責體系。並能建立相關流程可定期監督已在合約關係中之第三方所採取之安全措施。

- 風險管理方面
  密切注意供應鏈風險管理，實施採購目標供應鏈風險評估以辨識並減低供應鏈風險。透過市場調查以辨識風險、企業趨勢與採購最佳實務做法。基於風險考量來磋商契約條款，盡可能保持彈性。並應關注政府命令或指引已禁用之產品或軟體。

- 教育訓練方面
  教育各利害關係人確保其了解資安的概念、優先性與目標等，並教育採購單位與使用單位關於政府採行的風險評估與處理框架，此外也培育預算單位認知關於資安的重要性與潛藏之風險。

此外，技服中心所發布之「政府資訊作業委外資安參考指引」[3]，依照資訊委外生命週期，從計畫作業階段、招標階段、決標階段、履約管理階段、驗收階段、保固作業階段，亦有相關建議可供參考利用。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 7.2.2 資訊安全認知、教育及訓練

(1) 標準內容： 組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2) 適用說明： 應教育資訊設備或系統之採購、預算、使用單位與利害關係人，關於採購過程中資安之重要性，以及相關風險管理程序。

ISO 27001：2013(CNS 27001)

- A. 15.1.3 資訊及通訊技術供應鏈

(1) 標準內容： 與供應者之協議，應包含因應與資訊及通訊技術服務及產品供應鏈關聯之資訊安全風險。

(2) 適用說明： 在採購合約中，應要求供應商證明其安全性，並要求其接受管控或定期稽核，同時應納入風險考量訂定契約條款。

ISO 27001：2013(CNS 27001)

- A. 15.2.1 供應者服務之監視及審查

[3] 技服中心，網址：https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh(最後瀏覽日：110 年 10 月 29 日)

(1) 標準內容： 組織應定期監視、審查及稽核供應者服務交付。

(2) 適用說明： 應建立相關流程，以定期監督設備與服務供應商之資安措施或產品標準。

關鍵字	IT 採購、資訊採購、供應商監督、資安採購標準

類別：資訊保護【案號：S11011】

國內某基金會個資外洩，影響 2,000 名考生

【焦點話題】

國內某政府捐助成立之基金會(下簡稱該基金會)針對 111 年度之新式學測辦理試辦考試，該試辦考試系統自 110 年 4 月 1 日上線，並自 4 月 12 日開始正式報名。該基金會於 4 月 15 日自行查知，其試辦考試報名系統之資料庫，遭駭客入侵，約有 2,000 筆學生報名資料(占報名總數 2.67%)遭不明人士瀏覽，其發現後即通報權責機關，實施緊急應變措施，並進行系統調整與修補(系統邏輯之改善)，強化資通安全防護措施，亦已依個人資料保護法之規定通知相關當事人。全案並送司法機關調查中。該基金會另說明此試辦考試系統與 110 年度指定科目考試系統不同，並完全區隔，因此 110 年度指考報名系統並未受此次事件影響。

【參考資料來源：聯合報，110/6/2】

【重點摘要】

1. 資通安全管理法納管對象，除有資通安全責任等級分級辦法第 11 條第 3 項之情事外，依同辦法第 11 條第 1 項規定，應就其資通安全責任等級辦理應辦事項，若有自行或委外開發資通系統者，該等資通系統應依同辦法第 11 條第 2 項之規定，按該辦法附表九進行防護需求等級分級並落實該辦法附表十資通系統防護基準內對於使用者識別與鑑別以及身分驗證管理等措施，以強化系統之安全性。

2. 未經授權侵入他人系統瀏覽資料之行為，可能構成刑法第 358 條利用電腦系統漏洞入侵電腦或相關設備罪；若涉及個人資料之外洩，該系統受駭之單位亦須依個人資料保護法第 12 條，以及個人資料保護法施行細則第 22 條等規定，通知相關當事人。如其為資安法納管對象(此案例為特定非公務機關)，無論是否涉及個人資料外洩，應依資通安全

管理法第 18 條等規定，進行資通安全事件之通報及應變。

【法律觀點】

新聞稿雖未揭露駭客係如何入侵報名系統，但由該基金會事後之修補措施(修正系統邏輯判斷缺失等)觀之，駭客可能係利用該系統邏輯判斷缺失加以入侵，此舉將構成刑法第 358 條無故利用電腦系統之漏洞，入侵他人之電腦或其相關設備之罪。

而本案學生報名資料遭「瀏覽」一節，如駭客除瀏覽外亦對資料進行複製、拍照、截圖、下載、刪除、竄改等行為，則亦可能取得、刪除或變更他人電腦或其相關設備之電磁紀錄[1]，而不構成刑法第 359 條之罪[2]；如有蒐集或處理個人資料之行為，也可能違反個人資料保護法第 41 或 42 條之罪[3]。

依該基金會之組織性質，為政府捐助之財團法人，屬資通安全管理法所納管之特定非公務機關，而因試辦考試系統確有被入侵之事實，顯示其保護措施已失效，且相關情事對個資當事人有侵害之虞，此屬資通安全事件[4]，因此，該基金會應依照資通安全管理法第 18 條第 2 項[5]與資通安全事件通報及應變

[1] 台灣臺中地方法院 106 年重訴字第 405 號民事裁定。

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。」

[3] 個人資料保護法第 41 條：「意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」；第 42 條：「意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

[4] 資通安全管理法第 3 條第 4 款：「資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。」

[5] 資通安全管理法第 18 條第 2 項：「特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。」

辦法第 11 條[6]、第 13 條[7]之規定通報中央目的事業主管機關、完成損害控制或復原作業，並另應依個人資料保護法第 12 條[8]之規定，通知相關當事人。

【管理 Tips】

如上述，本案可能與系統邏輯判斷缺失與密碼管理措施有關，以資通安全管理法及其子法就資通系統開發應遵循之規定，可視資通安全責任等級分級辦法附表十資通系統防護基準相關之內容，按系統與服務獲得構面之系統發展生命週期需求階段，即應針對系統安全需求(含機密性、完整性、可用性)進行確認，若屬中、高等級之系統，並應於系統發展生命週期設計階段，識別可能影響系統之威脅，進行風險分析及評估，並將評估結果進行安全需求修正，以確保開發出之系統具備一定程度之安全性。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 14.1.1 資訊安全要求事項分析及規格

(1) 標準內容： 資訊安全相關要求事項，應納入新資訊系統或既有資訊系統之強化的要求事項中。

(2) 適用說明： 為強化機關組織之資通系統對於惡意入侵之防護能量，組織應於新系統之開發或既有系統更新、改版時，將缺乏安全性而可能面臨之潛在風險納入考量，並確

[6] 資通安全事件通報及應變辦法第 11 條第 1 項：「特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。」

[7] 資通安全事件通報及應變辦法第 13 條第 1 項：「特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：
一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。
二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。」

[8] 個人資料保護法第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

實落實資訊安全相關要求。

ISO 27001：2013(CNS 27001)

- A. 14.2.8 系統安全測試

(1) 標準內容： 於開發中，應實施安全功能性之測試。

(2) 適用說明： 考量新系統或既有系統更新、改版之安全性，組織應對該等系統進行測試及查證，以確保其得如期如質運作。

關鍵字	全國性系統、駭客入侵、系統資訊存取管理、通行碼管理

類別：資訊保護【案號：S11012】

求職面試時雇主要求面試者提供疫苗接種證明，是否適法？

【焦點話題】

目前國內民眾陸續施打 COVID-19 疫苗，有勞工面試時，被雇主要求提供疫苗接種證明，勞動部表示，接種證明屬於隱私資料，雇主若無正當理由即要求提供，將有違法問題。此外，國外求職網站 Indeed 之統計資料也顯示，新增的員工招募資訊中，有 90%的職位要求求職者應「接種疫苗」。

【參考資料來源：中央社，110/09/03; HSRM，110/08/23; HRDIVE，110/08/25】

【重點摘要】

1. 疫苗接種證明是疫情時代下產生的個人資料(下稱個資)，歐盟、國際衛生組織等國際組織，均將其定義為健康個資，具有敏感性。我國個人資料保護法(下稱個資法)亦將個資區分為一般與特種個資，醫療個資即屬於特種個資的一種。又依據我國個資法施行細則之規定，疫苗接種證明符合醫療個資之定義，而屬於特種個資，原則上不得蒐集、處理、利用，僅例外如取得個資當事人書面同意時，始得蒐集、處理、利用。

2. 就業服務法規定雇主不得要求求職者提供「非屬就業所需隱私資訊」。公司在招募資訊中欲要求疫苗接種證明者，應確認該證明是否屬於該招募職位所必須者。

【法律觀點】

我國個資法將 6 種個資定義為「特種個資」，包括病歷、醫療、基因、性生活、健康檢查、犯罪前科，原則上不得蒐集、處理或利用[1]。接種疫苗之證明，可能涉及醫療之個資類別。

[1] 個人資料保護法第 6 條。

依個資法施行細則之規定，醫療個資指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個資[2]。故判斷疫苗接種證明是否屬於醫療個資的認定上，應確認(1)是否由醫師或醫事人員進行；(2)目的是否為治療、矯正、預防人體疾病、傷害、殘缺；(3)是否有進行「診察及治療」；或基於以上之診察結果，所為處方、用藥、施術或處置。依據此標準，疫苗接種係由醫師或醫事人員，基於「預防人體疾病」之目的，並基於「可施打疫苗」之診察結果所為之「用藥」行為[3]，故解釋上可歸為特種個資的類別，僅於符合個資法第 6 條第 1 項所規定之情形下，例如取得當事人書面同意時，始得蒐集、處理及利用。惟即使得到當事人書面同意，應注意若其他法律另有限制，例如涉及我國就業服務法之就業隱私規定時，不得僅依當事人書面同意便蒐集、處理或利用。

有關疫苗接種證明性質之討論同樣出現在歐盟資料保護委員會(European Data Protection Board, EDPB)與歐盟資料保護監督機構(European Data Protection Supervisor, EDPS)於 2021 年 3 月提出有關「數位綠色證明(Digital Green Certification)」[4]法規提案之共同意見[5]。此共同意見中明確表示數位綠色證明中所顯示之資訊，包含疫苗接種證明，為敏感資訊。世界衛生組織則指出，個人疫苗接種狀態是健康隱私資訊，需要採取法律與技術

[2] 個人資料保護法施行細則第 4 條。

[3] 依據藥事法之規定，疫苗為生物藥品之一種，故施打疫苗之行為可定義為「用藥」行為。

[4] 數位綠色證明將包含以下資訊：疫苗接種證明(疫苗名稱與製造商、接種數量與接種日期)、檢測證明(檢測類型、檢測日期與時間、檢測中心與結果)、恢復證明(陽性檢驗結果日期、證明簽發者、簽發日期與有效日期)。

[5] EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)

上之保護措施[6]。

國際討論之焦點多集中於疫苗接種證明為個人健康隱私資訊、具有敏感性質，國家應恪遵保護人權與隱私的法律義務。至於特定行業或職務是否得要求求職者提供疫苗接種證明，於本案例撰寫之時，聯合國新冠肺炎危機處理小組強調航空業與航運業所屬從業人員，例如船員與空服員，在全球貿易、社會經濟復甦上佔有重要角色，尤其許多國家會要求船員或空服員入境時出示疫苗接種證明，故各國應將其列入疫苗之優先施打名單。至於雇主是否得於招募員工時要求提供此種證明，則為各國國內法之規範範圍[7]。

根據我國就業服務法之規定，雇主在招募或僱用員工時，不可以違反求職人或員工意思，留置其國民身分證、工作憑證或其他證明文件，或要求提供非屬就業所需隱私資料[8]。疫苗接種證明屬於隱私資料確實沒有疑義，但是不是屬於就業所需資料，必須看事業單位的工作屬性及場域狀況來判別。因此，雇主若要求求職者提供疫苗接種證明，必須提出正當理由，亦即必須證明其要求提供之隱私資料，係該應徵職務所必須具備者，否則等於是要求勞工提供非就業所需資料，有違法之疑慮。

【管理 Tips】

企業蒐集個資時，必須盤點並知悉個資保護或是隱私之相關規定，包括散落

---

[6] 世界衛生組織(WHO)於 2021 年 8 月 27 日發布以下文件，表示疫苗接種證明:Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, 27 August 2021. (Last updated: 2021.11.16)

[7] International Maritime Organization (IMO), UN organizations issue joint call for seafarers and aircrew to be prioritized for COVID-19 vaccination, 26 March 2021. (網址：https://www.imo.org/en/MediaCentre/PressBriefings/Pages/vaccination-UN-joint-statement.aspx ，最後瀏覽日：110 年 11 月 16 日)

[8] 就業服務法第 5 條第 2 項:「雇主招募或僱用員工，不得有下列情事：一、為不實之廣告或揭示。二、違反求職人或員工之意思，留置其國民身分證、工作憑證或其他證明文件，或要求提供非屬就業所需之隱私資料。三、扣留求職人或員工財物或收取保證金。四、指派求職人或員工從事違背公共秩序或善良風俗之工作。五、辦理聘僱外國人之申請許可、招募、引進或管理事項，提供不實資料或健康檢查檢體。六、提供職缺之經常性薪資未達新臺幣四萬元而未公開揭示或告知其薪資範圍。」。

於其他法律規範中的隱私規定。例如就業服務法屬於勞動法令，然其中關於就業隱私的規範，也是公司應審慎納入法遵管理的一環。

若公司想要求求職者提供疫苗接種證明，首先應確認請求的正當目的，包括疫苗接種證明是否與該職務內容相關，且公司也應制定相當程序，確保求職者面試時，每位負責面試的主管或同仁均瞭解是否可以詢問接種疫苗之相關資訊。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.18.1.4 個人可識別資訊之隱私及保護

(1) 標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2) 適用說明： 公司應定期盤點應適用的法令與法規，尤其需特別注意隱私與個資保護的相關規定，以招募新員工為例，就業服務法針對就業隱私資料之提供，規定應有「正當理由」，否則雇主不得要求提供。此種散落於勞動相關法規內、有關隱私之規定，公司應特別注意將其納入法遵的範疇。

ISO 27701：2019

- 6.4 .1.1 篩選(聘用前人力資源安全)

(1) 標準內容： 對所有可能被聘用者所進行之背景調查，宜依相關法律、規範及倫理，並宜相稱於營運要求及其將存取之資訊的保密等級及組織所察覺之風險聘用。

(2) 適用說明： 在篩選欲聘用之人才之前，組織會對應聘人員進行背

景調查，調查時可能涉及對應聘者的資料蒐集。又就業服務法、個資法對雇主招募時蒐集資訊一事有相當規範，公司宜依據法規與就業倫理，考量蒐集與職位相關的資訊。

ISO 29100：2011(CNS29100)

- 5.4 蒐集限制

(1) 標準內容：組織應將個人可是別資訊(personal identifiable information, PII)之蒐集限制於適用之法律及嚴格地為此指定目的所必要之邊界範圍內。組織不宜任意蒐集 PII。蒐集之 PII 數量及形式二者均宜限制於符合由 PII 控制者規定之(合法)目的所必須者。

(2) 適用說明：個資之蒐集，依法有一定之限制。在招募員工的法律關係下，就業服務法特別規定雇主不得要求求職者提供與就業無關之隱私資料。公司於蒐集、詢問求職者任何隱私資料之前，應審慎考慮此蒐集限制，以符合法律規定。

關鍵字	疫苗接種證明、醫療個資、就業服務法、就業隱私規範

類別：資訊保護【案號：S11013】

高中生「學習歷程檔案」因委外廠商失誤而遺失

【焦點話題】

攸關高中生升大學的「學習歷程檔案」，2021 年 9 月 24 日傳出因政府機關委外廠商之硬碟設定失誤而遭還原，造成 81 所學校檔案遺失。主因係政府機關委外廠商使用之學習歷程公版模組，進行資訊向上集中作業，逐步搬移到新機房內的虛擬主機，而該委外廠商於系統搬移到新機房運作十餘天之後，因系統更新而重新開機，發現部分虛擬主機的硬碟設定失誤，造成部分檔案無法連結。

【參考資料來源：聯合新聞網，110/09/26；關鍵評論，110/09/26】

【重點摘要】

1. 本案例除涉及資通系統及資訊委外管理之外，也涉及資通安全防護及控制措施中的保管議題。資訊及資通系統之保管，除應將資訊與系統盤點造冊、分級並持續更新之外，亦應採取適當措施以確保資訊之妥善保存與備份。
2. 組織亦應隨時注意業界對於技術安全措施的實施準則。以備份而言，目前業界實務操作，至少會製作三份備份，並將備份分別存放在兩種不同的儲存媒體，並至少有一份放置於異地保存。在重要資訊毀損滅失的風險實現時，完善的備份機制將可確保營運持續。

【法律觀點】

依據資通安全管理法(下稱資安法)第 10 條，本法納管之公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。資通安全管理法施行細則(下稱資安法施行細則)進一步列出資通安全維護

計畫應包含之內容，包括「核心業務及其重要性」、「資通系統及資訊之盤點，並標示核心資通系統及相關資產」、「資通安全防護及控制措施」、「資通系統或服務委外辦理之管理措施」等事項[1]。

承上資安法第 10 條、資安法施行細則第 6 條等規定所述，資安法所納管之公務機關應訂定並實施資通安全維護計畫，其中應包含「資通系統或服務委外辦理之管理措施」，並依資安法第 9 條之規定，審慎擇選委外之廠商並善盡相關監督義務，相關注意事項可依循資安法施行細則第 4 條規定，如選任及監督受託者時，受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證等，故資安法納管對象應依採購案之性質，適度要求廠商符合 CNS27001(資訊技術-安全技術-資訊安全管理系統-要求事項)、CNS 27018(資訊技術-安全技術-公用雲 PII 處理者保護個人識別資訊(personal identifiable information, PII)之作業規範)或其他資通安全管理措施，此點亦被納入資訊服務採購之資安檢核事項表[2]中。

此外，我國個人資料保護法除規定個資的蒐集、處理、利用之外，亦特別於第 4 條與同法施行細則第 8 條規範委外管理之法律適用與監督機制，主要係為避免資料蒐集機關以委外關係免除責任，故規範若組織委託廠商進行個資的蒐集、處理、利用者，應對受託者實施適當監督，其中還包括組織上與技術上的安全措施，以避免個資遭竄改、毀損、滅失。

【管理 Tips】

學習歷程檔案系統於過去亦曾發生類似事件，當時為公版模組發生問題，造成部分學生無法上傳檔案、甚或上傳後消失，相似事件一再發生之原因究竟為何？結合法律規範與管理來看，政府將標案給廠商後，「是否有適當之監

[1] 資通安全管理法施行細則第 6 條。

[2] 資訊服務採購之資安檢核事項表(網址：https://nicst.ey.gov.tw/Page/7CBD7E79D558D47C/8f9e71e4-e8ba-4ac9-abd5-ef38a9d6d5a2，最後瀏覽日：110 年 11 月 16 日)

督機制」、「監督內容與方式為何」、「行政部門有沒有專業人員具足夠資訊能力監督廠商」等，均為委外監督的範疇。至於防免資料毀損滅失上，則應確認「是否有定期進行模擬與演練」、「若發生資料毀損滅失，後續補救措施為何」等議題。前者包括廠商內部員工是否有進行社交工程演練、發生資料毀損滅失時的通報程序；後者則涉及資料毀損滅失時的應變機制、替代方案與補救計畫。

公司或是組織應依據上述有關委外監督、營運持續、資訊保存與管理建置標準作業流程，在每一次委外管理資通系統與資訊時均詳盡實施檢核。此外，更應隨時注意業界對於技術安全措施的實施準則。以備份而言，目前業界實務操作，至少會製作三份備份，並將備份分別存放在兩種不同的儲存媒體，並至少有一份放置於異地保存。尤其重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。此外，每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接覆寫回原資通系統，最後，備份資料如有機密性考量，宜加密保護之。在重要資訊毀損滅失的風險實現時，完善的備份機制將可確保營運持續。

【相關標準】

ISO 27001：2013(CNS 27001)

- 8.1 運作之規劃及控制

(1) 標準內容：　組織應控制所規劃之變更，並審查非預期變更之後果，必要時採取行動以減輕任何負面效果。組織應確保委外過程經確定並受控制。(摘錄)

(2) 適用說明：　為了維護營運與資訊系統之可用性，組織對於資通系統應有適當的控制，若因人力、資源、專業之限制而須將部分資通系統、營運維護外包，也應確保委外的

過程、監督委外。

ISO 27001：2013(CNS 27001)

- A.12.3.1 資訊備份

(1) 標準內容： 應依議定之備份政策，定期取得資訊、軟體及系統的影像備份副本，並測試之。

(2) 適用說明： 公司應設置備份政策，包括多久備份一次、備份方式為何、備份系統亦應經過測試。

關鍵字	資通安全管理法、個人資料保護法、委外監督、資料備份機制

類別：資訊保護【案號：S11014】

外洩 5.33 億筆個資 Facebook 未通知受害人

【焦點話題】

近日 Facebook 發生高達 5.33 億筆的使用者個人資料外洩事件，其中包含了使用者的生日、住址、姓名與電話號碼[1]等。Facebook 未公開此事，也未通知受影響的用戶，其所持理由有兩項。首先，Facebook 無法透過遭到外洩的資料，精確比對出到底要通知誰或哪個帳號；其次，即便 Facebook 對使用者發出了通知，無論使用者自己或 Facebook 官方，都無法改變數據已經遭到外洩的事實。就使用者角度來看，Facebook 處理個資外流事件的做法，過於消極且意圖冷處理，並不可取。

【參考資料來源：T 客邦，110/04/08；iThome，2021/04/07】

【重點摘要】

1. 依個資法第 12 條及個資法施行細則第 22 條之規定，公務機關或非公務機關當個資遭到竊取、洩漏、竄改或其他侵害時，應以適當方式通知當事人，使其得以知悉個人資料遭違法侵害之情事，其內容應包括個人資料被侵害之事實及已採取之因應措施。
2. 特定非公務機關在資安事件發生時，根據資通安全事件通報及應變辦法第 11 條之規定依中央目的事業主管機關指定之方式及對象，進行資通安全事件之通報。

【法律觀點】

現代人平常上網的時候，常常會需要在網路上留下個人資料，像是加入成為某網站之會員、網購時所填寫之資料或是在社群平台註冊時留下之資料等

[1] 個人資料保護法第 2 條第 1 款：「本法用詞，定義如下：一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」

等。大量個人資料於網路中流動之同時，如何確保資料在網路平台上之安全，此對人們來說一直是個重要議題，故個人資料保護法第 18 條及第 27 條第 1 項之規定，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，而非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

當個人資料被竊取、洩漏、竄改或其他侵害時，應於查明後通知當事人[2]，以使當事人得以知悉個人資料遭違法侵害之情事，以及時採取補救措施或提起救濟。其通知之內容[3]應包含個人資料被侵害之事實及已採取之因應措施，而通知之方式可包含言詞、書面、電話、簡訊、電子郵件、傳真、電子文件，甚至是網際網路或新聞媒體亦可。

另，如民間單位為資安法納管之特定非公務機關發生資安事件時，依資通安全事件通報及應變辦法相關規定，應於知悉資通安全事件 1 小時內，依中央目的事業主管機關指定之方式，進行資通安全事件之通報[4]。而中央目的事業主管機關接獲非公務機關通報或副知，或非因通報或副知而自行知悉個資外洩案件，經確認屬該機關管轄後，應於接獲通報、副知或知悉時起 72 小時內，填列監督通報紀錄表[5]，通報國發會，並得依個資法第 22 條至第 25 條規定，對該非公務機關為適當之監督管理措施[6]。

【管理 Tips】

---

[2] 個人資料保護法第 12 條：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」

[3] 個人資料保護法施行細則第 22 條：「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及
已採取之因應措施。」

[4] 資通安全事件通報及應變辦法第 11 條。

[5] http://www.rootlaw.com.tw/Attach/L-Doc/A040240001016600-1100811-6000-001.pdf

[6] 行政院及所屬各機關落實個人資料保護聯繫作業要點第 6 條。

近年來，關於社交平台個資外洩頻傳[7]，為防止個人資料被竊取、竄改、毀損、滅失或洩漏，組織依規定應制定個資安全措施。其措施，得包括配置管理之人員及相當資源、界定個人資料之範圍、個人資料之風險評估及管理機制、事故之預防、通報及應變機制、個人資料蒐集、處理及利用之內部管理程序、資料安全管理及人員管理、認知宣導及教育訓練、設備安全管理、資料安全稽核機制、使用紀錄、軌跡資料及證據保存、個人資料安全維護之整體持續改善等 11 點事項[8]，並以與所欲達成之個人資料保護目的間，具有適當比例為原則。

另，資通安全管理法第 16 條及第 17 條之規定，關鍵基礎設施提供者及關鍵基礎設施提供者以外之特定非公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，並依規定向中央目的事業主管機關提出資通安全維護計畫實施情形。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 18.1.1 適用之法規及契約的要求事項之識別

  (1) 標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

  (2) 適用說明： 組織應依法判斷是否適用個資法，並識別組織所面臨上的法律風險，同時保護個人可識別資訊安全。

ISO 27001：2013(CNS 27001)

[7] 社群媒體個資外洩連環爆 傳 Clubhouse 130 萬人被看光，(網址：https://udn.com/news/story/7086/5381299 ，最後瀏覽日：110 年 9 月 10 日)

[8] 個人資料保護法施行細則第 12 條。

● A. 18.1.4 個人可識別資訊之隱私及保護

(1) 標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2) 適用說明： 組織如有蒐集、處理或利用個資時，應對個資進行法律面上所要求之事項為法規符合度確認，並依法進行保護，而個資法因所適用之對象不分組織或個人，因此，個人亦應對其所持有個資進行適當保護。

關鍵字	個人資料保護法、個資事件通知、資通安全事件通報及應變辦法、安全維護計畫

類別：資訊保護【案號：S11015】

NCC 抽查台灣 15 款熱銷手機資安！

【焦點話題】

國家通訊傳播委員會(National Communications Commission，下簡稱NCC)公布 109 年智慧型手機內建軟體的資安抽測結果，抽查涵蓋 15 款機型，檢測其內建軟體之資安是否合格。此次抽查係依據 NCC 所公告之「智慧型手機系統內建軟體資通安全檢測技術規範」，目的為確保手機內建軟體與應用程式之安全性。NCC 強調，此次公布通過抽查檢測之各款手機，僅代表其系統操作等內建軟體版本在檢測當下符合測項要求，考量目前資安事件層出不窮及駭客攻擊手法日新月異，因此手機內建軟體如有更新版本，手機製造商應就更新部分重新檢測及驗證，始能維持其通過之資安等級，如事後被發現其系統內建軟體有資安漏洞或風險時，製造商仍應及時修補，並請民眾注意相關修補資訊。

【參考資料來源：twcert/cc，109/6/12】

【重點摘要】

1. 國家通訊傳播委員會訂有「智慧型手機系統內建軟體資通安全檢測技術規範」，將智慧型手機資通安全等級區分為初級、中級及高級，並以此發展智慧型手機系統內建軟體資安(Embedded Software on Smartphone Systems，ESS)認驗證標章。

【法律觀點】

針對手機之資訊安全，國家通訊傳播委員會(National Communications Commission, NCC)於 106 年 3 月 3 日公告智慧型手機系統內建軟體資通安全檢測技術規範(下稱技術規範)，以作為智慧型手機製造商、經銷商、電信業者及資通安全檢測實驗室辦理檢測之依據，而當智慧型手機通過檢

測後，即可取得「智慧型手機系統內建軟體資通安全等級標章」[1]。為因應不同使用者購買智慧型手機之價位考量及資安防護需求，智慧型手機系統內建軟體資安認證，依上述公告之技術規範分為初、中、高三個等級[2]。初級安全等級為智慧型手機基本隱私保護之最低要求，係應提供個人隱私相關之資料安全，包含手機安全性功能和敏感性資料之相關保護，如有蒐集敏感性資料之行為應明確告知使用者。而中級安全等級則應提供完整資料保護機制，所有資料之使用、儲存及傳輸時，皆可被安全保護。高級安全等級則應確保核心底層不被竄改或被不當擷取資訊。

由於該檢測並非基於強制性規定，而是為了提升消費者資安意識，帶動智慧型手機製造商重視手機內建軟體之資通安全而進行[3]，因此並未檢測技術規範之所有項目；惟對業者而言，雖然尚不能因通過該次檢驗即以此宣稱通過技術規範之要求，NCC 仍鼓勵業者透過自主或委託送測等方式，通過相關認驗證而取得認證標章[4]。

【管理 Tips】

為確保系統之安全性，系統於開發、運行等階段即應包含相關安全性之檢測，就資通安全管理法及其子法之相關規範中，有關安全性檢測，於系統運行階段可參照資通安全責任等級分級辦法附表一至附表六，有關技術面

---

[1] 智慧型手機系統內建軟體資安認驗證體系與推動方向二(一):「……106 年 4 月 20 日「智慧型手機系統內建軟體資通安全等級標章」(Embedded SystemSecurity, ESS)認證服務正式啟動。鑑於目前國際標準組織與歐美先進國家提出的行動裝置資安規範多屬指引或風險評估，並未要求經檢測合格始得販售，為避免技術性貿易障礙，現行的智慧型手機資安檢測機制並非強制性，而是由手機製造商自主或委託送測。」(網址：https://nccnews.com.tw/202010/ch1.html ，最後瀏覽日：110 年 7 月 5 日)

[2] 智慧型手機系統內建軟體資通安全檢測技術規範 3。

[3] NCC 公布 109 年手機內建軟體資安抽測結果(網址：https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=46299 ，最後瀏覽日：110 年 10 月 20 日)

[4] 智慧型手機資安認證服務(網址：https://www.ncc.gov.tw/chinese/content.aspx?site_content_sn=5089 ，最後瀏覽日：110 年 10 月 20 日)

辦理事項，可能包含弱點掃描及滲透測試，而於系統開發階段，則可參照同辦法附表十，於系統與服務獲得構面之系統發展生命週期開發階段、測試階段，對於系統安全檢測之內容，依系統等級不同，可能包含源碼掃描(如檢測出 OWASP Top 10、跨站腳本攻擊及資料庫注入，以及緩衝區溢位、程式碼不良寫法、臭蟲等)、滲透測試、弱點掃描(如檢測出 OWASP Top 10、軟體元件版本弱點、通訊協定弱點等)等。

此外，現代科技日新月異，使用智慧型手機幾乎為生活不可或缺之狀態，生活中大小事可能因為求方便，而將重要訊息例如網路銀行或各網站帳號密碼、信用卡資訊等記載於手機，因此，無論智慧型手機的內建軟體或提供使用者自行安裝之軟體皆宜符合一定安全標準，以避免引發資安危機。

是以，NCC 建議民眾應保持良好使用手機習慣，並提供「三不五要」口訣，加強使用者保護個人資料與隱私安全。而所謂「三不」即為：不強行取得根管理者(Root)權限或越獄(JB)、不瀏覽可疑網站、不連接可疑 Wi-Fi 接取點；「五要」則為：要定期更新密碼、要更新軟體程式及備份資料、要關閉未使用的 Wi-Fi/藍牙/NFC 等介面、連接的 Wi-Fi 接取點要開啟加密防護、手機廢置前要刪除機敏資料[5]。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 14.2.1 保全開發政策

(1) 標準內容： 應建立軟體及系統開發之規則，並應用至組織內之開發。

(2) 適用說明： 行動裝置上網佔有率已超越桌上型電腦，智慧型手機

[5] NCC 公布 108 年手機內建軟體資安抽測結果(網址：https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&cate=0&keyword=%e8%b3%87%e5%ae%89&is_history=0&pages=0&sn_f=43108 ，最後瀏覽日：110 年 7 月 5 日)

之相關營收亦年年成長，而製造商因開發智慧型手機必載內建軟體方可驅動，因此無論是出廠內建軟體、銷售商加載軟體或是無圖示軟體，均可依據主管機關所提供之開發 APP 相關資安規範，建立自己的 APP 開發規則，使所開發之 APP 符合法規要求。

ISO 27001：2013(CNS 27001)

- A. 14.2.8 系統安全測試

(1) 標準內容： 於開發中，應實施安全功能性之測試。

(2) 適用說明： 考量新系統或既有系統更新、改版之安全性，組織應對該等系統進行測試及查證，以確保其得如期如質運作。

關鍵字	智慧型手機系統內建軟體資通安全等級標章、智慧型手機系統內建軟體資通安全檢測技術規範

類別：資訊保護【案號：S11016】

美國警局成為受害者 駭客洩漏大量資料

【焦點話題】

華盛頓特區警察局拒絕駭客組織 Babuk 的勒索要求後，該組織在暗網上發布了數千份該警局的敏感文件。美聯社檢視後發現包含數百份警官懲處紀錄及情報報告，諸如：來自聯邦調查局(Federal Bureau of Investigation, FBI)、特勤局及其他機構之資訊。該組織表示希望該警局支付 400 萬美元贖回這些文件，但僅收到 10 萬美元，而該警局尚未說明是否已經付款，在此案中提供協助之 FBI 並不鼓勵付款給駭客組織。

【參考資料來源：Associated Press News，110/05/14】

【重點摘要】

1. 為確保公務機關資料之安全，並配合資安即國安之政策，公務機關就其管理之資料，除妥適進祥相關備份作業等安全控制措施外，並應採取資通安全事件通報及應變辦法所定相關安全演練作業，以防堵、降低風險發生之可能性。

【法律觀點】

為確保單位之資通安全，各組織、單位及一般民眾，就其管理之資料宜養成定期備份之習慣，以降低資安風險發生時之損害，若為公務機關、特定非公務機關[1]等資通安全管理法納管對象，有關資料備份之相關規定可參考資通安全責任等級分級辦法附表十之規定，且其等知悉資通安全事件時，應依資通安全管理法以及資通安全事件通報及應變辦法之相關規定，於知悉資通安全事件後 1 小時內依主管機關或中央目的事業主管機關指定

[1] 資通安全管理法第 3 條第 6 款：「六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。」

之方式，進行資通安全事件之通報[2]，且依事件等級不同，分於 72 小時或 36 小時內完成損害控制或復原作業，並於一個月內送交調查、處理及改善報告[3]。

【管理 TIPS】

以本案所涉及之駭客侵入警局電腦取得內部資料之型態為例，根據行政院資安處報告，110 年 9 月份[4]，政府機關之資安聯防情資共計 49,743 件，而可明確辨識之威脅種類，第 1 名為入侵攻擊類，佔總體 42%，主要係跨目錄存取攻擊及國外 IP 攻擊行為；其次為掃描刺探類，佔總體 27%，主要係外部主機執行掃描探測攻擊；以及政策規則類，佔總體 18%，主要係單一帳號持續登入失敗及排程工作刪除或停用確認。

為防堵公務機關內部資訊外洩之可能，根據資通安全管理法第 10 條及第 16 條第 2 項應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，其計畫內容應符合資通安全維護計畫依資通安全管

[2] 資通安全事件通報及應變辦法第 4 條第 1 項：「公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。」; 第 11 條第 1 項：「特定非公務機關知悉資通安全事件後，應於一小時內 依中央目的事業主管機關指定之方式，進行資通安全事件之通報。」

[3] 資通安全事件通報及應變辦法第 6 條第 1、2 項：「公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。」; 第 13 條第 1、2 項：「特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。」

[4] 資通安全網路月報(網址：https://nicst.ey.gov.tw/Page/8770AD7511CB8DC9/9eb5c27a-f5e8-407e-a9ee-f70049dba9be ，最後瀏覽日：110 年 10 月 25 日)

理法細則第 6 條之規定中 13 項要求[5]。

有關資料備份部分，目前業界實務操作，至少會製作三份備份，並將備份分別存放在兩種不同的儲存媒體，並至少有一份放置於異地保存。尤其重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接覆寫回原資通系統，如有機密性考量，宜加密保護之。

此外，資通安全事件通報及應變辦法中資安演練作業亦為重點之一。演練目的係為檢測機關之資安作業程序是否能因應並且預防資安事件發生，而機關應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關[6]，其演練作業內容得包括社交工程演練、資通安全事件通報及應變演練、網路攻防演練、情境演練及其他必要之演練[7]。

【相關標準】

---

[5] 資通安全法施行細則第 6 條：「本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：一、核心業務及其重要性。二、資通安全政策及目標。三、資通安全推動組織。四、專責人力及經費之配置。五、公務機關資通安全長之配置。六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。七、資通安全風險評估。八、資通安全防護及控制措施。九、資通安全事件通報、應變及演練相關機制。十、資通安全情資之評估及因應機制。十一、資通系統或服務委外辦理之管理措施。十二、公務機關所屬人員辦理業務涉及資通安全 事項之考核機制。十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。 第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關得由其上級或監督機關辦理；特定非公務機關得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辦理，或經中央目的事業主管機關同意，由其所管特定非公務機關辦理。」

[6] 資通安全事件通報及應變辦法第 8 條第 1 項：「總統府與中央一級機關之直屬機關及直轄市、縣市政府，對於其自身、所屬或監督之公務機關、所轄鄉 鎮、市、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉鎮、市、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。」

[7] 資通安全事件通報及應變辦法第 18 條：「公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：一、社交工程演練。二、資通安全事件通報及應變演練。三、網路攻防演練。四、情境演練。五、其他必要之演練。」

ISO 27001：2013(CNS 27001)

- A. 7.2.2 資訊安全認知、教育及訓練

(1) 標準內容： 組織所有員工及相關之約用人員，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2) 適用說明： 組織宜對定期對其員工或相關之約用人員能進行資訊安全教育及訓練。

ISO 27001：2013(CNS 27001)

- A.12.3.1 資訊備份

(3) 標準內容： 應依議定之備份政策，定期取得資訊、軟體及系統的影像備份副本，並測試之。

(4) 適用說明： 公司應設置備份政策，包括多久備份一次、備份方式為何、備份系統亦應經過測試。

ISO 27001：2013(CNS 27001)

- A. 12.6.1 技術脆弱性的管理

(1) 標準內容： 應及時取得關於使用中資訊系統之技術脆弱性的資訊，評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。

(2) 適用說明： 即時於組織中脆弱性做出適當措施，以防範風險產生。

關鍵字	公務機關、駭客、資安事件通報、安全維護計畫、資安演練

類別：資訊保護【案號：S11017】

立委批員警洩漏個資懲戒標準輕 內政部：通盤檢討

【焦點話題】

立委指出警察機關擁有「M-Police 行動警察系統」這個龐大資訊工具，此系統可以連結戶政、役政、交通等人民生活各方面資訊，故對於個人資料之保護十分重要。惟自 2011 年開始，屢有警察未依規定調閱他人資料而有侵害個資之新聞見諸媒體，讓民眾覺得警方對個資的保護很鬆散。警政署雖目前已訂定相關規範，但對於員警侵犯個資之懲戒標準過輕。對此，內政部表示，警察機關的資安因涉及許多民眾個資部分，所以更加重要，不只會檢討懲處辦法，也會一併檢討所有資安管制的要點。

【參考資料來源：中央通訊社，110/03/18】

【重點摘要】

1. 「M-Police 行動警察系統[1]」具備連網功能，能結合後端資料庫提供第一線執勤員警更多資訊。但亦因其功能牽涉到個人資料蒐集、處理及利用，為確保民眾權益並兼顧社會安全，政府應須嚴格把關此系統之安全性。

2. 依照資安維護計畫、資通安全責任等級分級辦法略旨，各機關所涉業務之重要性或機敏性皆有不同，故各機關應先盤點掌握其單位之業務資料，就其資料屬性判定責任等級；例如價值較高之資料，顯具有較高程度之資通安全風險，爰應予以較高程度之資通安全維護責任。

【法律觀點】

[1] 臺中市政府警察局清水分局-常見問答-什麼是 M-Police？警察可利用 M-Police 查詢哪些資料？(網址：https://www.police.taichung.gov.tw/qingshui/home.jsp?id=61&parentpath=0,5&mcustomize=faq_view.jsp&dataserno=201712050094&t=FAQ&mserno=201712050010 ，最後閱讀日期：110 年 9 月 8 日)

公務機關對於個人資料蒐集、處理、利用，應符合個人資料保護法(下簡稱個資法)第 15 條[2]及第 16 條[3]之規定，並且對於保有之個人資料，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。而以本案為例，若員警執行勤務時有使當事人之個資相關權利受到侵害，依據個人資料保護法第 28 條規定，公務機關違反個資法上述公務機關對於個人資料之維護，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，應負損害賠償責任。

此外，在資通安全之維護上，資通安全管理法要求公務機關，依照其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫[4]。因此，為協助公務機關及特定非公務機關有效完成資通安全管理機制，行政院國家資通安全會報提出資通安全維護計畫範本[5]，供各機關進行參考適用，其內容則是依據施行細則第 6 條[6]加以規劃，再針對個別要求予以

---

[2] 個人資料保護法第 15 條：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」

[3] 個人資料保護法第 16 條:「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安全或增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人同意。」

[4] 資通安全管理法第 10 條：「公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」

[5] 資通安全維護計畫範本(網址：https://nicst.ey.gov.tw/File/C30508E3823CE53/6287d1fe-542f-4a48-bbf5-c9f30bf11693?A=C，最後瀏覽日：110 年 9 月 25 日)

[6] 資通安全法施行細則第 6 條：「本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項:一、核心業務及其重要性。二、資通安全政策及目標。三、資通安全推動組織。四、專責人力及經費之配置。五、公務機關資通安全長之配置。六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。七、資通安全風險評估。八、資通安全防護及控制措施。九、資通安全事件通報、應變及演練相關機制。十、資通安全情資之評估及因應機制。十一、資通系統或服務委外辦理之管理措施。十二、公務機關所屬人員辦理業務涉及資通安全 事項之考核機制。十三、資通安全維護計畫

具體化。

另，對於公務機關資通安全業務倘有情節重大之違失，其懲處對象應根據具體事實予以認定。承辦業務人員之長官或督導業務之上級、監督機關人員，公務機關所屬人員資通安全事項獎懲辦法於 110 年 8 月 23 日針對本法第 4 條新增對業務督導不力，致其屬員、所屬或所監督機關之人員違反本條第 1 到 3 款事項，亦應予懲處之對象。

【管理 Tips】

為對公務機關建立良好且有效的管理，其應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，並由公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。據此，行政院國家資通安全會報亦提出「資通安全維護計畫範本」作為參考。

其中，關於資通安全維護計畫必要事項及實施情形之提出，定期辦理資通安全教育訓練[7]。且應於每年特定月份前向上級或監督機關，提出資通安全維護計畫實施情形[8]。為落實安全維護計畫，使公務機關之資通安全管理有效運作，公務機關內之相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄[9]。受稽單位於稽核實施後發現有缺失或待改善

與實施情形之持續精進及績效管理機制。各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。 第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關得由其上級或監督機關辦理；特定非公務機關得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辦理，或經中央目的事業主管機關同意，由其所管特定非公務機關辦理。」

[7] 資通安全維護計畫範本第壹拾參點。

[8] 資通安全維護計畫範本第壹拾陸點。

[9] 資通安全維護計畫範本第壹拾伍點

項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

而就存取控制與加密機制管理而言，分為網路安全控管、資通系統權限管理、特權帳號之存取管理、加密管理等四個方向，並可參考 CNS27001 關於系統與應用系統的存取控制部份予以加強。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 5.1.1 資訊安全政策

(1) 標準內容： 資訊安全政策應由管理階層定義並核准，且對所有員工及相關外部各方公布及傳達。

(2) 適用說明： 就 ISO 27001 之要求，資安政策係由管理階層定義並核准，而就資通安全管理法而言，公務機關之包含有其資安政策之資通安全維護計畫，於資通安全維護計畫範本第壹拾陸點規定「本機關應於〇〇月前向上級或監督機關(中央目的事業主管機關)，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。」，是故對於公務機關之資訊安全政策，不僅止於自律，甚至是由主管機關加以介入，而有更大規範強度。

ISO 27001：2013(CNS 27001)

- A. 7.2.2 資訊安全認知、教育及訓練

(1) 標準內容： 組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並

定期更新。

(2) 適用說明： 警察機關應對人員進行有效之資安及個資教育訓練及宣導，以利人員明確了解工作中應注意之規定，並遵守義務。

ISO 27001：2013(CNS 27001)

- A. 9.4.1 資訊存取限制

(1) 標準內容： 應根據存取控制政策，限制資訊與應用系統功能的存取。

(2) 適用說明： 核對權限細部的存取限制，最小權限原則，如：可讀、可寫、可不可以執行或是可不可以看到。

關鍵字	M-Police 行動警察系統、資通安全法、安全維護計畫、公務機關所屬人員資通安全事項獎懲辦法、資通安全維護計畫範本、存取控制機制

類別：資訊保護【案號：S11018】

五倍券數位綁定相關資安議題

【焦點話題】

政府為因應 COVID-19 疫情帶來的經濟影響，推出振興五倍券方案刺激消費，而為便利多元使用方式，提供以數位綁定之方式，使民眾可利用信用卡等多元支付方式使用。但於民眾數位綁定服務之過程中，卻出現部分系統障礙之情況，包括疑似被冒名綁定、系統流量無法負荷網站當機、綁定郵局 Taiwan Pay 之 OTP 驗證碼可直接透過瀏覽器於網頁中取得等。

【參考資料來源：風傳媒政治新聞，110/9/28】

【重點摘要】

1. 為避免重要系統因開發不當而產生的資安風險，應參考資通系統防護基準執行控制措施，如進行系統之風險分析及評估與回饋、執行「源碼掃描」安全檢測、針對安全需求實作必要控制措施、避免軟體常見漏洞等。
2. 關於本案相關的安全必要控制措施則包括：採用多因子身分驗證機制以強化身分驗證之安全性；增加後端伺服器、增加網路頻寬並整合系統相關資源與檢視使用者習慣；避免於網頁開發者檢查頁面提供任何使用者可以直接修改、攔截或回傳其中關於內容或身分驗證之資訊。

【法律觀點】

五倍券遭到數位冒名綁定，可能與資通系統之身分驗證方式強度有關；而系統因流量大導致無法正常運作，可能受到網站伺服器效能或頻寬不足問題所影響；至於 OTP 驗證碼若可直接從瀏覽器取得，將能避開經由使用者的其他上網裝置進行身份驗證的程序，可能產生被冒用帳號的重大資安風險。而無論上述何種情況，均與資通系統開發過程中，未能妥善針對系統安全需求，包括機密性、可用性與完整性進行確認有關。

根據資通安全責任等級分級辦法第 11 條第 2 項規定要求，各機關自行或委外開發之資通系統應依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，並依附表十所定資通系統防護基準執行控制措施。故無論此次五倍券系統之網站是由政府機關自行建置，或是由其委外開發，均應執行相關資通系統防護基準控制措施。

五倍券系統影響範圍及於全台所有民眾，處理資料量與金額計算均龐大，在資通系統防護需求之分級上，似屬防護需求高等級。關於系統之開發，在防護基準控制措施之相關構面應屬於系統與服務獲得，而就高等級防護需求而言，在系統發展生命週期設計與開發階段，主要相關之措施內容則包括：在設計階段，應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，並將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，例如評估系統能負荷的流量上限並加以調整。而在開發階段，應執行「源碼掃描」安全檢測，設計發生嚴重錯誤時之通知機制，針對安全需求實作必要控制措施，避免軟體常見漏洞，使用者頁面於發生錯誤時僅顯示簡短錯誤訊息及代碼等控制措施。

【管理 Tips】

因五倍券綁定網站此種為特定目的迅速開發出來的系統，基於時程壓力，通常無法兼顧資安或運作有效性。近年資訊業界所提倡的 DevSecOps (開發 development、安全 security、維運 operation)的觀念即值得重視與落實，以兼顧產品開發的敏捷度與安全性。未來在快速開發軟體或服務時，應該要能夠兼顧各個重要的面向，包括流暢度、順暢度以及安全機制[1]。

如前述本案相關的問題包括疑似被冒名綁定、系統流量無法負荷網站當機、綁定郵局 Taiwan Pay 之 OTP 驗證碼可直接透過瀏覽器於網頁中取得等。

[1] TechOrange, 郵局網頁大出包！資安專家：政府、企業要加強 DevSecOps 觀念(網址：https://buzzorange.com/techorange/2021/09/23/stimulus-vouchers-taiwan-pay-threat/，最後瀏覽日：110 年 10 月 8 日)

針對不同問題可採用下列不同之管理措施：

- 冒名綁定：目前針對身分驗證可採用多因子身分驗證機制以強化身分驗證之安全性，除利用輸入手機門號、身分證字號、出生年月日、Email 等基本資料，或利用帳號密碼進行身分驗證外，尚可增加智慧晶片卡、數位憑證、動態密碼(OTP)生物辨識等因子互相搭配。視系統重要性、管理成本與使用者需求來決定搭配之方式[2]。

- 系統流量無法負荷：有效因應系統流量負荷的方式包括增加後端伺服器、增加網路頻寬等傳統方式，但除此之外尚應考量系統效能和前端整合設備的介面、中間負載平衡設備、閘道器設備[3]，更進一步則是掌握網站使用者的習慣對系統可能造成的衝擊[4]、採用內容分發網路(CDN)將資源或應用程式放置在靠近最終使用者的位置[5]。

- OTP 驗證碼可直接透過瀏覽器於網頁中取得：此種可以透過開發者常用的檢查網頁元素功能，係在瀏覽器頁介面中按下 F12，即可檢視網頁的程式碼。但在程式邏輯上，不應於該頁面提供任何使用者可以直接修改、攔截或回傳其中關於內容或身分驗證之資訊。若在 SSDLC 的開發階段與測試階段中，並未透過源碼掃瞄、滲透測試或弱點掃瞄等方式成功發現此一情形，仍應於部署與維運階段隨時進行更新與修補。

【相關標準】

---

[2] 財金資訊第 92 期，以多因子驗證機制強化身分驗證之安全性(網址：https://www.fisc.com.tw/Upload/a19a130b-bb71-43e5-aaec-4c94a3765907/TC/9206.pdf ，最後瀏覽日：110 年 10 月 8 日)

[3] iThome,硬體當機 2 大主因：性能預留不足與備援維護不確實(網址：https://www.ithome.com.tw/news/95494 ，最後瀏覽日：110 年 10 月 12 日)

[4] 數位時代，電商雙 11 大當機，超乎預期的流量不是唯一問題(網址：https://www.bnext.com.tw/article/51258/momo-double-eleven-website-crush ，最後瀏覽日：110 年 10 月 12 日)

[5] aws, 什麼是 DDoS 攻擊？(網址：https://aws.amazon.com/tw/shield/ddos-attack-protection/ ，最後瀏覽日：110 年 10 月 12 日)

ISO 27001：2013(CNS 27001)

- A. 9.2.4 使用者之秘密鑑別資訊的管理

(1) 標準內容： 應以正式之管理過程控制秘密鑑別資訊的配置。

(2) 適用說明： 除採用一般基本資料作為系統綁定之鑑別資訊外，如能進一步搭配其他多因素驗證機制，則更可確保相關身分之安全性。

ISO 27001：2013(CNS 27001)

- A. 9.4.5 對程式源碼之存取控制

(1) 標準內容： 宜限制對程式源碼之存取。

(2) 適用說明： 嚴格控制程式源碼及相關項目，預防引進未授權的功能性及避免非意圖的變更，如本案中不應將 OTP 驗證碼之顯示保存於實際瀏覽器檢查網頁元素之頁面。

ISO 27001：2013(CNS 27001)

- A. 12.1.3 容量管理

(1) 標準內容： 各項資源之使用宜受監視及調適，並對未來容量要求預作規劃，以確保所要求之系統效能。

(2) 適用說明： 由於五倍券系統屬於全體國民均得使用之系統，且可預見在短期內會有龐大的流量，因此更應對其容量作出準確預估，並避免對其服務產生威脅之潛在瓶頸，規劃適切作為。

關鍵字	五倍券、系統開發、源碼檢測、滲透測試、OTP、

	DevSecOps

類別：資訊保護【案號：S11019】

GCP 服務完成金融雲端委外獨立第三方單位查核

【焦點話題】

近年來金融業之雲端服務有委外辦理之需求，而 Google 雲端 GCP(Google Cloud Platform, GCP)為金融業者選擇委外之對象之一，其表示已透過獨立第三方稽核單位，於 110 年初，依據金管會法規，即金融機構作業委託他人處理內部作業制度及程序辦法，完成虛擬稽核(Virtual Auditing，或稱遠端查核)。這是三大公有雲業者中，第一家揭露自家服務應金融機構用戶上雲需求，已接受獨立第三方查核的業者。

除了金管會透過相關法規開放並管理金融機構雲端委外，身為醫療院所監管單位的衛福部也準備開放電子病歷上雲。是時衛福部資訊處處長龐一鳴與常務次長石崇良也分別提出：目前正研擬放寬電子病歷上雲端，並賦予相關法源依據，從資安、委外到平臺建置等都能有所依循[1]，後續可觀察其與金融行業對於雲端委外查核的標準異同。

【參考資料來源：iThome，110/8/31】

【重點摘要】

1. 關於雲端委外服務的資安查核要求，目前在金融業已有金融機構作業委託他人處理內部作業制度及程序辦法作為強制規範，課以金融機構有委外查核監督之義務，同時也是賦與其對於委外業者查核之權利。而其他領域業者在未有其中央目的事業主管機關特別針對雲端委外稽核之規定前，如屬適用資通安全管理法之業者，亦應依據資通安全管理法第 9 條與資通安全管理法施行細則第 4 條之相關規定，對受託者

[1] 中時新聞網，電子病歷上雲端 衛福部擬開放第三方代管。(網址：https://www.chinatimes.com/realtimenews/20210925003165-260405?chdtv ，最後瀏覽日：110 年 10 月 18 日)；iThome，電子病歷上雲草案 2 大重點首度公開(網址：https://www.ithome.com.tw/news/147698，最後瀏覽日：110 年 11 月 12 日)

加以監督。

2. 管理雲端委外查核時，在程序面應注意透過契約對查核要求與相關事項加以約定，並注意執行時受查核廠商之配合情況。而在內容方面可參考目前與雲端相關之標準，確保查核之有效性。

【法律觀點】

金融機構作業委託他人處理內部作業制度及程序辦法已於 108 年 9 月修正通過，在第 19-1 條與 19-2 條納入雲端委外的相關管理規則。由於將作業委外雲端業者，實為本身作業之延伸，因此為確保金融機構健全經營，委外作業仍應受相當監督，關於雲端委外的查核，在該辦法第 19-1 條第 3 款與第 4 款分別規定，金融機構應確保其對於雲端服務業者有實地查核權力，且得委託具資訊專業之獨立第三人來查核雲端服務業者[2]。另為確保委託第三人查核之品質，並對第三人查核範圍及第三人適格性等有所要求。

除金融業可透過前述規定取得對雲端服務業者進行外部查核之權力外，關於其他運用雲端服務之產業，如符合資通安全管理法之適用範圍，亦可根據資通安全管理法施行細則第 4 條第 1 項第 9 款之規定，以稽核或其他方式確認受託業務之執行情形[3]。

【管理 Tips】

金融業基於數位轉型之需求，在考量營運成本與新興業務開發時程的前提下，採用雲端服務，便成為提升企業效率之首選。無論是基礎設施即服務

[2] 金融機構作業委託他人處理內部作業制度及程序辦法第 19-1 條第 3 款：「金融機構應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行受託作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。」; 第 4 款:「金融機構得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核，並應符合下列規定：(一)確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節。(二)應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。(三)應針對金融機構所委託作業範圍進行查核並出具報告。」

[3] 資通安全管理法施行細則第 4 條第 1 項第 9 款：「委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。」

(Infrastructure as a Services, IaaS)、資訊平台即服務(Platform as a Services, PaaS)或軟體即服務(Software as a Services, SaaS)，金融機構均可依照其需求選擇，但也均面臨資料須提供外部公司，脫離企業自己掌握的風險。

為落實風險管理，對於雲端委外服務之查核，管理方式可從以下兩方面為之：

- 查核程序面：由於業務委外單位要對於雲端服務業者進行實地查核，或委託第三方獨立驗證機構進行查核時，均涉及到對雲端服務業者的系統或營業的外力干涉。為避免雲端服務業者拒絕接受查核，或是查核過程當中發生爭議，最好能於委外契約內就議定委外機關具有稽核委外廠商之權利，或者退而求其次，也能要求由委外廠商提供由第三方獨立評估者所提出的查核報告作為一種監督方式[4]。如行政院公共工程委員會所提供的資訊服務採購契約範本(110 年 4 月 9 日修正版)[5]，其中第 9 條第 10 項即賦予機關得檢查與稽核廠商之權利[6]，另外第 16 條第 17 項第 1 款除要求廠商應遵守資安相關法令與標準外，亦說明機關保有查核權利[7]。

[4] 政府資訊作業委外資安參考指引 v6.1，p36(網址：https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh ，最後瀏覽日：110 年 11 月 12 日)

[5] https://www.pcc.gov.tw/cp.aspx?n=99E24DAAC84279E4 (最後瀏覽日：110 年 11 月 12 日)

[6] 資訊服務採購契約範本第 9 條第 10 項：「1.機關得定期或不定期派員檢查或稽核廠商提供之服務是否符合本契約之規定，廠商應以合作之態度在合理時間內提供機關相關書面資料，或協助約談相關當事人。上述提供機關相關書面資料，以法令規定或契約約定者為限，其檢查或稽核得以不預告之方式進行之，廠商不得拒絕。2.機關得委由專業之第三人稽核廠商提供之服務，費用由機關負擔。3.廠商作業經機關檢查或稽核結果不符合本契約規定者，需於接獲機關通知期限內改善。」

[7] 資訊服務採購契約範本第 16 條第 17 項第 1 款：「廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。此外機關保有依機關與廠商同意之適當方式對廠商及其分包廠商以派員稽核、委由資通安全管理法主管機關籌組專案團隊稽核或其他適當方式執行相關稽核或查核的權利，稽核結果不符合本契約約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲機關通知後應於期限內完成改善，未依限完成者，依第 14 條第 1 款約定核計逾期違約金。」

- 查核內容面：
  - 在查核內容應著重的項目，可參考我國與國際資通安全標準如 CNS 19086-1、雲端安全聯盟(CSA)雲端控制矩陣(Cloud Control Matrix, CCM)、ISO 27000 系列，以及美國 NIST SP800-144 等建議控制措施，選擇必要項目作為查核重點[8]。
  - 針對不同雲端服務模式(IaaS, PaaS, SaaS)在安全需求管理方面，亦區分可用性管理、存取控制、弱點管理、變更管理、設定管理、意外應變、監測系統使用與存取、資料安全、電子蒐證、實體環境等項目訂定相關管理要求[9]。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 15.1.2 於供應者協議中闡明安全性

(1) 標準內容： 應與每個可能存取、處理、儲存或傳達資訊，或提供 IT 基礎建設組件資訊之供應者，建立及議定所有相關資訊安全要求事項。

(2) 適用說明： 應於與雲端服務業者之契約內或是採購相關服務的 RFP 內，約定委外機關保有稽核雲端服務業者之權利，以檢視服務過程中的安全性。

ISO 27001：2013(CNS 27001)

- A. 15.2.1 供應者服務之監視及審查

(1) 標準內容： 組織宜定期監視、審查及稽核供應者服務交付。

[8] 政府資訊作業委外資安參考指引 v6.1，p46。

[9] 同前註，附件 5。

(2) 適用說明： 為確保雲端服務的安全性並符合法規要求，應定期進行查核，且應注意雲端服務業者於查核過程中所指派之相關負責人員，能取得充分技術技能與資源，方得有效協助查核進行。而查核所發現之應改善事項亦應落實追蹤矯正。

關鍵字	雲端服務、委外查核、獨立第三人、政府資訊作業委外資安參考指引、資訊服務採購契約範本

類別：資訊保護【案號：S11020】

愛心協會大規模捐款個資外洩，關鍵在於資訊服務廠商

【焦點話題】

自 2021 年 7 月底，警方接獲大量民眾通報，多個捐款協會遭到冒名，且捐款人的姓名、電話、捐款金額等個人資料均遭詐騙組織掌握，已用於取信被害人。警方調查後發現，這些慈善愛心協會均委託同一資訊系統商，即提供非營利組織捐款系統的 A 公司。A 公司在該年 8 月向其客戶(即愛心協會)通知捐款系統遭駭客攻擊，並提到已封鎖可疑 IP 位址，限制具風險性的功能、建置即時監控系統以偵測網路異常、強化用戶帳號登入安全。

【參考資料來源：iThome，110/08/25】

【重點摘要】

1. 個資委外管理是我國業界常見情形，也是個人資料保護法(下稱個資法)的一個規範重點，本文說明委外管理的法律規範，委託機關應對受託者進行適當監督，且受託者對於受委託之個資管理，若有違法之情形，委託機關亦應負擔法律責任，而無法以個資已經委外、未經手個資等理由卸責。

2. 本文另涉及資安事件通報與應變機制之建置，針對本案，分為委託機關(愛心機構)與受託者(A 公司)兩塊給予不同的管理建議。愛心機構應對 A 公司實施適當監督，可行之監督手段舉例如下：於合約中訂定相關個資委外管理條款。至於 A 公司，首先應識別法規，確認自己作為個資委外處理廠商之角色，並規劃個資管理的責任，以及事件回應之程序。以從資安事件學習，降低未來事件發生之可能性與衝擊。

【法律觀點】

個資法第 4 條[1]與個資法施行細則第 8 條[2]針對個人資料之委外訂有規範，除前者規定受委託蒐集、處理、利用個人資料的機關，於個資法的範疇內，視同委託機關之外，後者更規定委託機關應對受託者為適當監督，且針對應監督事項，列有六項，包括預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間等。此外，該法施行細則第 8 條也規範了委託機關應定期確認受託者執行個資蒐集、處理、利用之情形，並記錄結果，至於受託者則應依據委託機關的指示執行任務，若認為委託機關的指示違法，應立即通知委託機關。

以本案的事實而言，愛心協會即為委託機關、A 公司為受託者，依據個資法第 4 條規定，A 公司因管理之漏洞或威脅而導致個資外洩，此外洩責任視同愛心協會的責任，亦即愛心協會無法以其未經手個資、或該個資已委外管理而卸責。至於 A 公司亦負有依法管理個資，以及事件發生時應通報愛心協會的義務。

此外，資通安全管理法(下稱資安法)對於資安相關事務之委託也有明文規定。對於資通系統之建置、維運或資通服務之委外，資安法第 9 條[3]規定公務機關或特定非公務機關應考量受託者之專業能力與經驗、委外項目之

---

[1] 個人資料保護法第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

[2] 個人資料保護法施行細則第 8 條：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。　前項監督至少應包含下列事項:一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。　第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。　受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。」

[3] 資通安全法第 9 條:「公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。」

性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。而行政院國家資通安全會報技術服務中心亦提供資訊作業委外資安參考指引[4]，其中提供資訊委外關係下的資安管理要求、資訊委外類型與相關注意事項，包括委外計畫作業階段應注意資通安全責任等級分級，履約管理階段應對廠商或稽核人員實施控管，驗收階段應回收或請委外廠商銷毀屬於委託機構的資訊資產等項目，有利於實務上資訊委外之執行。本案的愛心協會與 A 公司雖非資安法之適用對象，但是資安法之相關規範仍值各界參考。

本案另涉及事件通報，根據個資法施行細則第 12 條第 2 項第 4 款，事件之預防、通報及應變機制屬於個資法上適當安全維護措施之一環。於 110 年 8 月，行政院為防止非公務機關個人資料檔案外洩，加強所屬中央目的事業主管機關對非公務機關個人資料保護之監管，發布行政院及所屬各機關落實個人資料保護聯繫作業要點，該要點針對個資外洩之監督通報有所規範:非公務機關個資外洩時，依安全維護辦法應通報之對象、時點、應通報事項、後續行政檢查等事項，應納入中央目的事業主管機關所訂之安全維護辦法中[5]。

【管理 Tips】

針對本案，個資委外的管理應分為委託機關(愛心機構)與受託者(A 公司)兩塊給予不同的管理建議。愛心機構既然將捐款人資料委託 A 公司管理，則應實施適當監督，可行之方式包括：於合約中訂定相關個資委外管理條款，確認個資委託的範圍、類別、期間、受託者應提供的適當安全維護措施，以及受託者應定期接受委託機關的稽核，確認其個資管理的落實情形。

至於 A 公司，首先應識別法規，確認自己作為個資委外處理廠商之角色，並規劃個資管理的責任，以及事件回應之程序。除應依法蒐集、處理、利用

[4] 行政院國家資通安全會報技術服務中心，109 年政府資訊作業委外資安參考指引(網址：https://www.nccst.nat.gov.tw/CommonSpecification?lang=zh 最後瀏覽日：110 年 11 月 16 日)

[5] 行政院及所屬各機關落實個人資料保護聯繫作業要點第四點參照。

個資之外，尚應落實資安管理的程序，於事件發生時通報眾家愛心機構(委託機關)，另應對內部與外部人員傳達資安事件之存在與其他細節，存錄所有與資安事件相關的回應，分析、識別事件來源，從資安事件學習，以降低未來事件發生之可能性與衝擊。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.16.1.1 責任與程序

(1) 標準內容： 應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。

(2) 適用說明： 對於資訊安全事件之管理，應確認相關責任與程序。以 A 公司的角色為例，其作為受委託蒐集、處理、利用個人資料之機關，例首先應識別法規、合約，確認其處理個人資料時的角色與責任，並進一步規劃事件回應之程序。

ISO 27001：2013(CNS 27001)

- A.16.1.5 對資訊安全事故之回應

(1) 標準內容： 應依文件化程序，回應資訊安全事故。

(2) 適用說明： 發生資安事件之後，A 公司應盡速蒐集證據、實施資安鑑識分析，並依法規、合約等進行提報。此外，應對內部與外部人員傳達資安事件之存在與其他細節，且所有與資安事件相關的回應、資料均應錄存，以供日後分析、識別事件來源。

ISO 27001：2013(CNS 27001)

● A. 18.1.4 個人可識別資訊之隱私及保護

(1) 標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2) 適用說明： 愛心機構應識別個資法對於委外管理的規定，並對 A 公司施行適當的監督機制，蓋對於眾多個資遭外洩的捐款人而言，愛心機構是蒐集其資料之非公務機關，因此事件發生之後，愛心機構也是主要承擔個資外洩責任的主體。若愛心機構未對 A 公司進行適當監督，則有違法之風險。

關鍵字	委外監督、事故通報、資安管理

類別：資訊保護【案號：S11021】

聚焦資安專業人才培訓：美國的共同責任 vs.台灣的公私協力

【焦點話題】

美國總統拜登日前邀集大型科技、金融和能源企業，在白宮舉行國家網路安全高峰會；拜登表示，資安是美國目前面臨的重大挑戰，網路安全是政府和產業共同的責任，尤其那些經營重要基礎設施的公司；俄羅斯駭客入侵聯邦機構及今年勒索軟體攻擊迫使美東輸油管線關閉，讓網路安全議題成美國國安首要事項。他敦促企業強化網路安全；數家重要企業均承諾，將投資數百億美元提升資安。

【參考資料來源：聯合新聞網，110/08/27】

【重點摘要】

1. 美國政府主張網路安全是政府和產業的共同責任，也要求許多大型公司投入資源強化網路安全、培訓資通安全人才。相較於此，我國則是採取公私協力的立場，從資通安全管理法(下稱資安法)的規範架構上來看，是以政府作為推動資通安全人才培育之主體，且即使於人才培育上有公私協力的想法，也是採取由政府構築資安發展環境、進行關鍵基礎設施之防護，將資安防護能量擴及至民間單位。而和民間單位之間的合作，也主要是由政府提供情資分享平台或是辦理攻防演練，相較於美國直接將企業做為資安人才培育的責任主體，有所差異。

【法律觀點】

美國於 2019 年 5 月發布的第 13870 號總統令(Executive Order)，說明美國的資安人力政策規劃，於聯邦層級，針對國土安全局與其他機關的資安人員應具備最低資安技能，其最低標準為 2017 年提出之國家網路安全教育倡議(National Initiative for Cybersecurity Education, NICE)和網路安全人力框架(National Initiative For Cybersecurity Education

Cybersecurity Workforce Framework, NICE Framework，以下稱 NICE 框架)。

至於國家層級的資安人力提升則由公部門應鼓勵地方、學術界、非營利與私部門實體於合法之情況下，自願於教育、訓練和人力發展中納入 NICE 框架[6]。

除以上政策的確立之外，實務層面上，2021 年 8 月 25 日美國總統拜登於資安高峰會上強調美國網路安全人才欠缺，與民間企業商討如何協同合作降低美國資安威脅、共同擔負資安人才培訓的責任[7]，企業也對此要求做出相應承諾。

相對於美國將資安人才培育視作政府與產業的共同責任，我國法律與實務發展框下則有不同概念。我國資安法第 4 條第 1 項[8]規定，為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動資通安全專業人才之培育。可知於我國的法律規範架構下，政府是推動資通安全人才培育的主體。

實務上，為資安基礎教育，強化資安人才培育，教育部推動「資訊安全人才培育計畫」[9]。此外，對於民間專業人才培育上，根據國家資通安全發展方案，政府部門各權責機關推動相關計畫、挹注資源、構築資安人才培育環境，強調資安人才之培育可供產業所用。在公私協同治理方面，我國以資通安全法之落實確認資安治理的發展環境，以關鍵基礎設施的資安作為

---

[6] America's Cybersecurity Workforce(網址：https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce ，最後瀏覽日：110 年 11 月 16 日)

[7] 行政院國家資通安全會報技術服務中心，資安新聞。(網址：https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=16607，最後瀏覽日：110 年 11 月 16 日)

[8] 資通安全管理法第 4 條第 1 項：「為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項:一、資通安全專業人才之培育。」

[9] 教育部資訊安全人才培育計畫。(網址：https://isip.moe.edu.tw/wordpress/?page_id=50 ，最後瀏覽日：110 年 10 月 28 日)

重點防護對象，深化公部門與民間單位之間的情資分享與應變演練。從以上發展可知，我國在資安政策之推動與人才培育上，公部門仍係以國家整體資安環境之建構、關鍵基礎設施之防護作為重點，和民間單位之間的合作，也主要是由政府提供情資分享平台或是辦理攻防演練，相較於美國直接將企業做為資安人才培育的責任主體，有所差異。

【管理 Tips】

為維護資訊安全，企業需對組織內部進行管理與風險控制，為達成此目標，應掌握資訊安全人人有責的原則，凡企業內的員工、組織編制外的相關承包者，都應接受與其工作職能相關之資安政策與管理程序的認知教育與相關訓練，且應定期更新、做成紀錄。

【相關標準】

ISO 27001：2013(CNS 27001)

- A.7.2.2　資訊安全認知、教育及訓練

(1) 標準內容：　組織所有員工及相關之承包者，均應接受與其工作職能相關的組織政策及程序之適切認知、教育及訓練，並定期更新。

(2) 適用說明：　對於企業端而言，資訊安全管理標準中並不會賦予企業培訓資安人才的責任。但是回歸到資訊安全人人有責的原則，企業內的員工、組織編制外的相關承包者，都應接受與其工作職能相關之資安政策與管理程序的認知教育與相關訓練，且應定期更新、做成紀錄。

關鍵字	資通安全管理法、認知教育、人才培育

類別：資訊保護【案號：S11022】

金融機構之資通安全長設置義務

【焦點話題】

金融監督管理委員會(下稱金管會)近來推動「金融資安行動方案」，要求銀行、保險、證券期貨等符合條件的金融機構要在六個月內完成指派「副總經理以上或職責相當之人」兼任資訊安全長 CISO(Chief Information Security Officer)。為持續強化金融業資安，金管會於民國 110 年 5 月底分別公布「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「保險業內部控制及稽核制度實施辦法」與「證券暨期貨市場各服務事業建立內部控制制度處理準則」草案，明定符合條件的業者須設副總以上層級資安長。

【參考資料來源：聯合新聞網，中央社，110/05/27】

【重點摘要】

1. 資通安全管理法(下稱資安法)第 11 條規定，「公務機關」應設置資通安全長；資通安全長由機關首長指派副首長或適當人員兼任。資通安全長之責任包括推動及監督機關內資通安全相關事務。至於特定非公務機關，雖於資安法本文中，並未明定其等應指定資安長或資通安全管理代表，惟於該法第 16 條、17 條亦授權中央目的事業主管機關得就其所管特定非公務機關擬訂相關資安遵行事項，報請主管機關核定後實施，有關資安長或資通安全管理代表之設置亦可能為遵行事項之一。

2. 依金管會公布之「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「保險業內部控制及稽核制度實施辦法」及「證券暨期貨市場各服務事業建立內部控制制度處理準則」，要求金融機構須指派資安長，以有效推動資安維護事項、控管資安風險。

【法律觀點】

依資安法第 11 條規定，公務機關應設置資通安全長；資通安全長由機關首長指派副首長或適當人員兼任。資通安全長之責任包括推動及監督機關內資通安全相關事務。至於特定非公務機關，目前資安法本文中，並未明定特定非公務機關應指定資安長或資通安全管理代表。

而中央目的事業主管機關得否要求特定非公務機關指定一定層級之人員擔任資安長或資通安全管理代表？依據資安法第 16 條第 6 項、第 17 條第 4 項之規定：「…資通安全維護必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬定，請主管機關核定」，故各中央目的事業主管機關基於資安防護整體考量，得要求其所管特定非公務機關指定適當層級之人員擔任資安長或資通安全管理代表，相關規定並得訂定於相關管理辦法中。

以本案為例，金融業者根據「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「保險業內部控制及稽核制度實施辦法」與「證券暨期貨市場各服務事業建立內部控制制度處理準則」等已於本年 9 月陸續修正通過之規定，進行資安長之設置。銀行業應指派副總經理以上或職責相當之人兼任資安長[10]，並給予業者 6 個月調整緩衝期[11]。保險業前一年度經會計師查核簽證資產總額達新台幣 1 兆元以上者，應指派副總經理以上或職責相當之人兼任資安長[12]，待修正條文生效，符合適用條件的業者須在 6 個月內調整。至於證券暨期貨業亦相同，各服務事業符合一定條件者，應指派

[10] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條：「銀行業應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。但主管機關對信用合作社及票券金融公司另有規定者，依其規定。」

[11] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 46 條：「銀行業不符第三十八條之一第一項前段有關兼任之規定者，應自……本辦法修正發布之日起六個月內，調整至符合規定。」

[12] 保險業內部控制及稽核制度實施辦法第 6-1 條第 2 項：「保險業前一年度經會計師查核簽證之資產總額達新臺幣一兆元以上者，應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務，且應設置具職權行使獨立性之資訊安全專責單位，並指派協理以上或職責相當之人擔任資訊安全專責單位主管。」

副總經理以上或職責相當之人兼任資安長[13]，也給予業者 6 個月調整期。

由上開辦法可知，雖資安法並未明定特定非公務機關應指定資安長，但高度監理的中央目的事業主管機關，例如金管會，對其所主管的事業單位，包括銀行業、保險業、證券暨期貨業者，於符合一定條件下，應依上開各別辦法設置資安長，確保資通安全事項可以有效推動。

【管理 Tips】

資安法下所規定之資安長設置義務，主要的規範對象為公務機關，至於特定非公務機關，雖資安法並未明定特定非公務機關應指定資安長，惟，特定非公務機關若可指定資安長或資通安全管理代表，將能確保更有效推動資通安全維護事項。

除法規上對於資安專責化的發展之外，一般企業對於資安管理的落實，也可見於企業組織人力之配置。進行資安管理時，在資安政策確立之後，為建立管理框架，組織內應確認資訊安全之角色及責任，將資安責任做出確切定義與配置，且對資安責任配置相應的人力資源進行風險監督與控管。雖管理制度下為保留組織人力配置之彈性，並未明確要求專責人員或是資安長的配置，但是在資安大幅影響企業安全的現代社會，資安專責的觀念逐步發展，舉凡建置資安設備與維護系統、修補程式更新、限制應用程式之使用、帳號密碼與存取權限管理、資安教育訓練、資訊設備或產品之採購，都會需要資安風險控管，故業界設置專責資安主管或成立專責資安部門的情況日益增加，成為強化資安管理的一環。

【相關標準】

ISO 27001：2013(CNS 27001)

[13] 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 36-2 條第 1 項：「各服務事業符合一定條件者，應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務；其一定條件，由主管機關定之。」

- A.6.1.1 資訊安全之角色及責任

(1) 標準內容： 應定義及配置所有資訊安全責任。

(2) 適用說明： 管理上，組織應配置資訊安全責任，且被賦予資安責任者，雖可將安全任務委派他人，但是仍由其負責。以本案而言，銀行、保險、證券期貨等符合條件的金融機構依法應設置資安長，於企業決策中主掌資訊安全之風險管理。

ISO 27001：2013(CNS 27001)

- A. 18.1.1 適用之法規及契約的要求事項之識別

(1) 標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2) 適用說明： 除資通安全法、個人資料保護法等對於資訊與資料之法律之外，組織應識別其產業所特別適用之法律，例如金管會推動之「金融資安行動方案」，以及銀行、保險與證期局分別公布的「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「保險業內部控制及稽核制度實施辦法」與「證券暨期貨市場各服務事業建立內部控制制度處理準則」草案，其中明定符合條件的業者須設副總以上層級資安長。都是應予識別的法律要求事項。

關鍵字	資安長、資安管理代表、資通安全管理法

貳、資訊公開(Disclosure)

類別：資訊公開【案號：D11023】

立院三讀 不當勞動行為裁決書原則應予公開

【焦點話題】

立法院會三讀通過修正勞資爭議處理法部分條文。為使裁決委員會運作更具效率及專業，三讀通過條文增訂設置 1 至 3 位常務裁決委員，且明定裁決委員會應秉持公正立場，獨立行使職權。由於目前不當勞動行為裁決決定書公開與否，取決於申請裁決人是否同意公開，三讀通過條文也增訂，勞動部應將公開裁決決定書定期出版、登載於網站或以其他適當方式公開；裁決書含有政府資訊公開法應限制公開或不提供事項，應僅公開其他部分。三讀通過條文明定，公開的裁決決定書內容，得不含自然人名字、身分證統一編號及其他足以識別的個人資料，但應公開自然人姓氏及能夠區辨人別之代稱。

【參考資料來源：中央通訊社，110/4/13】

【重點摘要】

1. 裁決決定書亦屬政府資訊公開法(下稱政資法)所稱之政府資訊，故依政資法之規定，以主動公開為原則。
2. 政資法第 7 條、第 18 條等規定，對於政府資訊公開，採取原則主動公開，例外明示限制範圍[1]。

[1] 法務部 108 年 1 月 22 日法律字第 10803500640 號函釋。

【法律觀點】

依政資法第 7 條[2]規定，政府資訊除有同法第 18 條限制公開或不予提供之事由[3]外，均屬政府應主動公開之資訊[4]。而政資法第 18 條對於資訊公開範圍限制，則以列舉限制範圍之方式，因資訊公開與限制公開之範圍互為消長，如不公開之範圍過於擴大，勢將失去立法之意義；惟公開之範圍亦不宜影響國家整體利益、公務之執行及個人之隱私等[5]。故勞資爭議處理法增訂第 47-1 條，因現行中央主管機關就不當勞動行為而做出之裁決決定書屬政資法第 3 條所稱之政府

---

[2] 政府資訊公開法第 7 條：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：一、條約、對外關係文書、法律、緊急命令、中央法規標準法所定之命令、法規命令及地方自治法規。二、政府機關為協助下級機關或屬官統一解釋法令、認定事實、及行使裁量權，而訂頒之解釋性規定及裁量基準。三、政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號。四、行政指導有關文書。五、施政計畫、業務統計及研究報告。六、預算及決算書。七、請願之處理結果及訴願之決定。八、書面之公共工程及採購契約。九、支付或接受之補助。十、合議制機關之會議紀錄。前項第五款所稱研究報告，指由政府機關編列預算委託專家、學者進行之報告或派赴國外從事考察、進修、研究或實習人員所提出之報告。第一項第十款所稱合議制機關之會議紀錄，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單。」

[3] 政府資訊公開法第 18 條：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之:一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。二、公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。四、政府機關為實施監督、管理、檢(調)查、取締等業務，而取得或製作監督、管理、檢(調)查、取締對象之相關資料，其公開或提供將對實施目的造成困難或妨害者。五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資料，其公開或提供將影響其公正效率之執行者。六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。八、為保存文化資產必須特別管理，而公開或提供有滅失或減損其價值之虞者。九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。政府資訊含有前項各款限制公開或不予提供之事項者，應僅就其他部分公開或提供之。」

[4] 法務部 98 年 8 月 26 日法律字第 0980024475 號函釋。

[5] 政府資訊公開法第 18 條 94 年立法理由一：「資訊公開與限制公開之範圍互為消長，如不公開之範圍過於擴大，勢將失去本法制定之意義；惟公開之範圍亦不宜影響國家整體利益、公務之執行及個人之隱私等，爰於本條第一項列舉政府資訊限制公開或提供之範圍，以資明確。」

資訊[6]，故依政資法之規定，以主動公開為原則，然而當事人自然人名字、身分證統一編號及其他足以識別的個人資料，根據個人資料保護法屬個人資料，依照政資法第 18 條規定應限制公開，僅就其他部分公開之。

【管理 TIPS】

由於大眾日益重視及關注裁決案件，但裁決案件數量卻與日俱增，新修法之 1 到 3 名「常務裁決委員」，以專職設置，專以處理相關裁決並保障勞工組織或參與工會活動之團結權、簽訂團協之團體協商權，以達到勞資爭議處理法之立法目的[7]。

政府資訊對外公開是必要的，但在公開資料時仍應採取妥適之管制，而非任意性全面公開，亦應衡酌其公開之目的及手段。應避免侵害個人隱私，對公開範圍加以限制，應僅得公開必要資料且降低涉及會影響結果之資訊，以期達到資訊保護與公開之平衡。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 8.1.1 資產清冊

(1) 標準內容： 應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。

(2) 適用說明： 組織為釐清其持有之資產，以及對於該等資產進行妥適之分類、分級等管理措施，對於其所持有之資產應予以分類並製表列冊，以供需要時得以快速檢驗。本案政府機關對於其所管之資訊，平時即應妥適進行盤點並列冊管考，並

[6] 政府資訊公開法第 3 條：「本法所稱政府資訊，指政府機關於職權範圍內作成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。」

[7] 勞資爭議處理法第 1 條：「為處理勞資爭議，保障勞工權益，穩定勞動關係，特制定本法。」

對其中屬限制公開或不予提供者，加註說明。

ISO 27001：2013(CNS 27001)

- A. 18.1.4 個人可識別資訊之隱私及保護

(1) 標準內容： 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。

(2) 適用說明： 機關所製出符合政資法之文書時，應對個資進行法律面上所要求之事項為法規符合度確認，並依法進行其保護，以確保個人可識別資訊之隱私及保護並符合資訊公開之意義。

關鍵字	勞資爭議處理法、政府資訊公開法

類別：資訊公開【案號：D11024】

落實公民參與 全台 22 地方議會均已公開議事資訊

【焦點話題】

目前全國 22 個地方議會均已依規定主動揭露議事日程、會議紀錄、議事錄及會議影音檔等議事資訊，並全程直播大會，強化地方層級的公民參與及公眾監督。內政部指出，「地方立法機關組織準則」第 25 條規定，地方議會除秘密會議外，應在會議前將議事日程公開於網站；除考察或現勘的議程外，大會應透過網路或電視全程直播;大會及委員會應全程錄影,並應於會議後一定期限內將會議紀錄、議事錄與影音檔公開於網站。內政部表示，地方議會議事透明化的推動，議會除了要以現有預算及人力辦理資訊揭露工作外，也必須建立起公開透明的議事觀念。

【參考資料來源：聯合新聞網，110/04/18】

【重點摘要】

1. 依地方立法機關組織準則第 25 條第 2 項之規定[1]，應公開地方立法機關大會會議應開放民眾旁聽。但會議主席或議員、代表三人以上提議或依地方制度法第 49 條列席人員[2]之請求，經會議通過時，得舉行秘密會議。
2. 保障人民知的權利，公開地方議會的運作與議員職權的行使接受大眾的檢驗，落實議事公開，強化政府透明度。

---

[1] 地方立法機關組織準則第 25 條第 1 項：「前項公開舉行之會議，依下列規定辦理:一、大會會議應開放旁聽。二、會議議事日程，應於會議前公開於網站。三、會議應製作會議紀錄，除考察及現勘外，並應製作議事錄，且分別於會議後一個月內及六個月內，公開於網站至少五年。四、直轄市議會、縣(市)議會，除考察及現勘外，大會會議實況應透過網路或電視全程直播；大會及委員會會議應全程錄影，於會議後十五日內將影音檔公開於網站至少五年。五、鄉(鎮、市)民代表會、山地原住民區民代表會，除考察及現勘外，大會及小組會議應全程錄音，於會議後十日內將錄音檔公開於網站至少五年。」

[2] 地方制度法第 49 條：「直轄市議會、縣(市)議會、鄉(鎮、市)民代表會大會開會時，對特定事項有明瞭必要者，得邀請前條第一項各該首長或單位主管列席說明。直轄市議會、縣(市)議會委員會或鄉(鎮、市)民代表會小組開會時，對特定事項有明瞭必要者，得邀請各該直轄市長、縣(市)長、鄉(鎮、市)長以外之有關業務機關首長或單位主管列席說明。」

【法律觀點】

按政府資訊公開法(下稱政資法)之制定，係為建立政府資訊公開制度，便利人民共享及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與[3]。其政資法第 6 條之規定[4]，舉凡與人民權益攸關之施政、措施及其他有關之政府資訊，因對人民之影響至深且鉅，以主動公開為原則。但政府機關於職權範圍內作成或取得之資訊，如符合第 18 條[5]第 1 項所定政府資訊公開例外限制之事項者，自應限制公開或拒絕提供。惟因情事變更，已無繼續限制或拒絕之必要者，為貫徹政府資訊公開原則，自當允許並受理申請提供，以滿足人民知的權利。

地方立法機關組織準則第 25 條之規定，明定地方立法機關大會會議應開放民眾旁聽，透過議事資訊公開，民眾可以瞭解議會開會狀況、議案審議情形以及選區議員的問政內容與表現，讓地方議會的運作與議員職權的行使接受大眾的檢驗，落實地方民意代表向選民負責的精神，對於地方民主的深化具有正面意義。

---

[3] 政府資訊公開法第 1 條。

[4] 政府資訊公開法第 6 條：「與人民權益攸關之施政、措施及其他有關之政府資訊，以主動公開為原則，並應適時為之。」

[5] 政府資訊公開法第 18 條：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之:一、經依法核定為國家機密或其他法律、法規命令規定應秘密事項或限制、禁止公開者。二、公開或提供有礙犯罪之偵查、追訴、執行或足以妨害刑事被告受公正之裁判或有危害他人生命、身體、自由、財產者。三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。四、政府機關為實施監督、管理、檢(調)查、取締等業務，而取得或製作監督、管理、檢(調)查、取締對象之相關資料，其公開或提供將對實施目的造成困難或妨害者。五、有關專門知識、技能或資格所為之考試、檢定或鑑定等有關資料，其公開或提供將影響其公正效率之執行者。六、公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。八、為保存文化資產必須特別管理，而公開或提供有滅失或減損其價值之虞者。九、公營事業機構經營之有關資料，其公開或提供將妨害其經營上之正當利益者。但對公益有必要者，得公開或提供之。　政府資訊含有前項各款限制公開或不予提供之事項者，應僅就其他部分公開或提供之。」

根據政資法第 2 條規定[6]，明定此法與其他法律之適用關係，將政資法定位為普通法，其他法律對於政府資訊之公開另有規定者，自應優先適用。故此條但書，若會議主席或議員、代表三人以上提議或依地方制度法第 49 條列席人員之請求，經會議通過時，得舉行秘密會議。

【管理 TIPS】

政府資訊公開之目的，在於增進一般民眾對公共事務之瞭解、信賴及監督，故機關應確實知悉政府資訊公開法所規範之政府資訊，基於民主政治原理，立法機關應踐行議事公開制度，以落實民主權與人民知的權利。而議事公開制度之內容亦為各國民主化之重要指標，落實議事公開，強化政府透明度。本於「資訊共享」及「施政公開」之理念，根據政資法第 7 條政府機關藉由依法應公開之事項[7]，以便利人民公平利用政府依職權所作成或取得之資訊，除增進一般民眾對公共事務之瞭解、信賴及監督外，更能促進民主之參與。

當政府資訊公開於網路或是在資通系統上傳輸時，對於政府資訊屬於應主動公開或應人民申請而公開之資訊，以及政府資訊屬於應限制公開或不予提供之資訊，政府機關應盤點其所持有之政府資訊，加以列冊管考，而在列管後，對應不同資訊之重要性及應祕密性，其管理面亦可為相關思考。諸如：涉及應祕密事項之資通系統，就資料傳輸面而言，資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更，且加密金鑰或憑證應設定更換週期，以維持資料之機密性[8]。就儲存之安全性而言，則對具保護需求之機密資訊應加密儲存

---

[6] 政府資訊公開法第 2 條：「政府資訊之公開，依本法之規定。但其他法律另有規定者，依其規定。」

[7] 政府資訊公開法第 7 條第 1 項：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：一、條約、對外關係文書、法律、緊急命令、中央法規標準法所定之命令、法規命令及地方自治法規。二、政府機關為協助下級機關或屬官統一解釋法令、認定事實、及行使裁量權，而訂頒之解釋性規定及裁量基準。三、政府機關之組織、職掌、地址、電話、傳真、網址及電子郵件信箱帳號。四、行政指導有關文書。五、施政計畫、業務統計及研究報告。六、預算及決算書。七、請願之處理結果及訴願之決定。八、書面之公共工程及採購契約。九、支付或接受之補助。十、合議制機關之會議紀錄。」

[8] 資通安全責任等級分級辦法附表 10 資通系統防護基準，構面系統與通訊保護措施內容傳輸之機密性與完整性。

[9]，以降低機密資訊遭未經授權存取之風險。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 8.1.1 資產清冊

(1) 標準內容： 應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。

(2) 適用說明： 組織建立資產清冊之目的在確保採行有效之資產保護，而政府資訊本身即屬於須保護之重要資產，且透過資產清冊之建立，並對屬於有無限制公開或不予提供之情形及理由加以註記，可降低第一線人員於處理資訊公開時之困擾。

ISO 27001：2013(CNS 27001)

- A. 18.1.1 適用之法規及契約的要求事項之識別

(1) 標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2) 適用說明： 組織在業務開發時應瞭解並依循其應適用之法令，以避免觸法。以本案例而言，政府機關在資訊公開前，必須瞭解所掌握的資訊為何，是否得以公開，以避免在無法源依據下公開不得公開之政府資訊。

關鍵字	政府資訊公開法、議事公開、地方立法機關組織準則

[9] 資通安全責任等級分級辦法附表 10 資通系統防護基準，構面系統與通訊保護措施內容資料儲存之安全。

參、資訊監察(Monitors)

類別：資訊監察【案號：M11025】

簡訊實聯制使用爭議 前法官：應立法明定

【焦點話題】

前台中地院法官指出在審核刑事警局搜索票聲請書時，發現警方以簡訊實聯制鎖定嫌犯行蹤；就算該簡訊是經由法官核發調取票或是依通訊監察所得的資訊，都違反發送簡訊者原本信任指揮中心所說的「限於疫調使用」的承諾，警方以簡訊內容來鎖定嫌犯行蹤，恐怕也是不當行為。刑事局當時回應，辦案調取的電信通訊資料，都是根據通訊保障及監察法向法院聲請核發得來，警方並未向衛福部調取得任何資料，作為犯罪偵查使用；警方依法得來的資料，本來就會包含手機簡訊資料，當然也就包括簡訊實聯制，這種矛盾並非警方製造，警方只是執行單位。中央流行疫情指揮中心指出，不會同意任何機關將簡訊實聯制進行疫調外的使用，已請警政署通令，未來偵辦時若調用的簡訊中有出現實聯制內容，主動排除不使用，避免外界不必要的誤解。

【參考資料來源：聯合新聞網，110/09/20】

【重點摘要】

1、簡訊實聯制之資料搜集目的雖僅在於防疫之用，不得做目的外利用；惟電信業者基於通訊保障及監察法之義務相關規定，實聯制的簡訊內容仍可能屬提供檢調機關調查之資料範圍。

2、行政機關於委託電信業者建置簡訊實聯制之資料庫，蒐集使用者資料時，應注意其對於委外之監督義務，例如受委託業者是否有採取適當之安全維護措施(如使用紀錄、軌跡資料及證據保存之措施)。

【法律觀點】

「通訊監察」是國家針對個人的通訊行為及內容所做的監控。而通訊保障及監察法(下稱通保法)係為保障人民秘密通訊自由及隱私權不受非法侵害，並確保國家安全，維護社會秩序所制定，規範國家對人民進行通訊監察的要件與限制。

依通保法之規定，如具有足夠的事實認定犯罪嫌疑人涉犯特定重罪，且有相當理由可信其通訊內容與案件相關，並難以由其他方式進行調查時，得聲請核發通訊監察書進行監察。此時電信事業有協助執行通訊監察之義務[1]，該義務包含電信事業應使其通訊系統之軟硬體設備具有配合執行通訊監察時所需之功能，並協助執法機關執行通訊監察[2]。因此就通保法為犯罪偵防之目的所設計的制度，在符合法律要件並由法院核發通訊監察書之前提下，其調閱的資料範圍即可能就會包含到由電信業者所蒐集的簡訊實聯制內容。

「簡訊實聯制」係重要科技防疫措施，其所蒐集之個人足跡資訊，目的僅供指揮中心疫調使用，不得做目的外利用[3]，此制度係根據傳染病防治法第 37 條第 1 項第 6 款[4]，衛生福利部公告「嚴重特殊傳染性肺炎(COVID-19)第三級疫情警戒標準及防疫措施裁罰規定[5]」，規定外出時應全程佩戴口罩，並配合實聯制；行政院為遏止疫情擴散，並減少實聯制紙本填寫之接觸，推出「簡訊實聯制」供民眾及商家使用，使民眾可透過簡易的簡訊傳送，即可完成資訊之登錄。

---

[1] 通訊保障及監察法第 14 條：「通訊監察之執行機關及處所，得依聲請機關之聲請定之。法官依職權核發通訊監察書時，由核發人指定之；依第七條規定核發時，亦同。 電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。 前項因協助執行通訊監察所生之必要費用，於執行後，得請求執行機關支付；其項目及費額由交通部會商有關機關訂定公告之。電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限， 並不得逾越期待可能性。 前項協助建置通訊監察系統所生之必要費用，由建置機關負擔。另因協助維持通訊監察功能正常作業所生之必要費用，由交通部會商有關機關訂定公告之。」

[2] 通訊保障及監察法第 5 條：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。」

[3] 「COVID-19(武漢肺炎)」防疫新生活運動:實聯制措施指引(網址：https://www.cdc.gov.tw/File/Get/t-_Xs5DDee2qzBFC1fRXJA ，最後瀏覽日：110 年 11 月 25 日)

[4] 傳染病防治法第 37 條第 1 項:「地方主管機關於傳染病發生或有發生之虞時，應視實際需要，會同有關機關(構)，採行下列措施：一、管制上課、集會、宴會或其他團體活動。二、管制特定場所之出入及容納人數。三、管制特定區域之交通。四、撤離特定場所或區域之人員。五、限制或禁止傳染病或疑似傳染病病人搭乘大眾運輸工具或出入特定場所。六、其他經各級政府機關公告之防疫措施。」

[5] 嚴重特殊傳染性肺炎(COVID-19)第三級疫情警戒標準及防疫措施裁罰規定(網址：https://www.cdc.gov.tw/File/Get/OQgL0X5SE3TyxgLzy79-oA，最後瀏覽日：110 年 11 月 15 日)

與此同時，檢調機關若為進行犯罪偵防而向電信業者調取用戶資料時，依前述規定，由於簡訊實聯制亦屬通聯紀錄的一部分，相關資料即可能被涵蓋於受通訊監察之範圍中；惟就簡訊資料之蒐集與使用之本身，亦有論者指出仍應完善其法律依據[6]，以使相關行政作為確實於法有據，並最大程度地給予人民基本權利的保障。

【管理 TIPS】

簡訊實聯制係為維持國內疫情之穩定控制，使民眾生活及產業經濟能於具備一定安全條件下，逐步恢復正常運作。然而針對簡訊實聯制蒐集之資料，應做適當管理。簡訊實聯制中「免個資」實際上為「免留個資給店家」，民眾發送的簡訊會越過店家，直接交由電信業者留存 28 天，期間指揮中心可向業者調閱資料用於疫調所需，但這也代表個人的電話號碼以及所到場所代碼依然會交到電信業者的資料庫進行保管。

而「個人資料」的定義包含「聯絡方式」、「其他得以直接或間接方式識別該個人之資料」[10]，前者可對應簡訊實聯制中提供的電話號碼；而場所代碼則能夠用以拼湊出個人的足跡，屬於與其他資料串接後可能識別個人之資料，因此簡訊實聯制所傳送的資訊亦應受個資法的保障；準此，政府應根據個資法第 4 條[7]及其細則第 8 條[8]委外規定，對受委託之電信業者為適當之監督，例如受委託業者

---

[6] 李榮耕(110)，〈【李榮耕觀點】警察，我在這裡—簡訊實聯制的法律依據何在？〉(網址：https://www.lepenseur.com.tw/article/744，最後瀏覽日：110 年 12 月 7 日)

[10] 個人資料保護法第 2 條。

[7] 個人資料保護法第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」

[8] 個人資料保護法施行細則第 8 條：「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。　前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。　第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。　受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委

是否有採取適當之安全維護措施(如使用紀錄、軌跡資料及證據保存之措施)。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 18.1.1 適用之法規及契約的要求事項之識別

(1) 標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2) 適用說明： 執法機關與電信業者均應瞭解所涉法律及應用範圍，以進行相關業務之執行，避免觸法。本案中電信業者對於通訊監察有配合義務，執法機關與電信業者均應瞭解所涉法律及應用範圍，對於建置通訊設備之必要性及流程操作應予以瞭解，俾符合依法行政原則。

ISO 27001：2013(CNS 27001)

- A. 15.2.1 供應者服務之監視及審查

(3) 標準內容： 組織宜定期監視、審查及稽核供應者服務交付。

(4) 適用說明： 為確保受託之電信業者妥適進行相關業務，應定期進行查核，且應注意包含民眾個人資料之管理。而查核所發現之應改善事項亦應落實追蹤矯正。

關鍵字	簡訊實聯制、通訊保障及監察法、通訊監察、電信業者、委外

託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。」

類別：資訊監察【案號：M11026】

智慧型兒童手錶之後門資安漏洞

【焦點話題】

一家於北歐地區之資安公司發現一智慧型兒童手錶，具有後門(backdoors)程式，該手錶之製造商及代銷商，可透過該程式遠端啟動監控模式，於使用者無法察覺之情況下，啟動相機拍照並回傳至其雲端以及進行其他諸如查詢目前位置等監控。研究人員透過逆向工程研究該手錶之程式碼，發現並且成功地測試傳送一個加密過的簡訊給該手錶，就可以無聲無息地觸發上述偷拍。除了偷拍功能之外，研究人員在程式碼中還發現該手錶之「聯絡人」App 為遠方攻擊者提供了 WIRETAP_INCOMING 跟 WIRETAP_BY_CALL_BACK 這兩個服務，猜測應該就是「竊聽來電」跟「視需要竊聽」。

【參考資料來源：科學月刊，109/11/15】

【重點摘要】

1. 業者若於隨身穿戴裝置植入後門程式，竊取使用者個資，將涉及刑法、個人資料保護法，以及通訊保障及監察法等法規之相關規範。
2. 使用者在選購資通設備時，應優先選擇注重資安之廠商；若為組織或企業進行採購者，應確認並管控資安風險，以避免公務及機敏資料遭不當竊取。

【法律觀點】

隨著資通訊產品的技術發展，加上與網路相互搭配所形成的各類應用，物聯網及各式隨身穿戴裝置為人們的生活帶來了相當大的便利。惟隨著人們對資通訊產品的依賴程度上升，若遭設置後門程式，將造成相當大的資安危害。

以本案例情形而言，即是具連網功能的隨身穿戴裝置遭開發業者於裝置內設置後門程式，使業者得以隨意蒐集使用者的各類資料，例如使用者週遭的環境照片、地理位置資訊，甚至使用者的通聯對話內容等；由於隱私權是受憲法保障

的基本權利[1]，業者對使用者採取這些行為，將可能涉及刑法、個人資料保護法(下稱個資法)，以及通訊保障及監察法(下稱通保法)的問題。

此類行為在刑法上會涉及 315 條以下[2]的妨害秘密相關罪責，自不待言，於此不再贅述。另值得注意的是，業者由隨身穿戴裝置所蒐集到的使用者資料係個資法所保護之範圍，依個資法第 8 條[3]與第 19 條[4]，業者應於蒐集個人資料前，明確告知當事人相關事項並取得完整的同意；惟就案例內容而言，業者的資料蒐集可能未充分讓消費者知情，且並未取得同意(例如消費者雖知道該裝置有照相功能，但不知道照片會被回傳到業者所控制的雲端空間)，將有違反個資法的疑慮。

此外，於本案中業者甚至可能竊聽使用者的通話內容，因此有適用通保法的討論空間。依照通保法之定義，利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信即屬於通訊的一種[5]，在使用者對

---

[1] 參照大法官釋字第 585 號理由書：「 其中隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活秘密空間免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障(本院釋字第五 0 九號、第五三五號解釋參照)。」

[2] 中華民國刑法第 315 條：「無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或九千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。」第 315-1 條：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[3] 個人資料保護法第 8 條：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。(第一項) 有下列情形之一者，得免為前項之告知：一、依法律規定得免告知。二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。三、告知將妨害公務機關執行法定職務。四、告知將妨害公共利益。五、當事人明知應告知之內容。六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。(第二項)」

[4] 個人資料保護法第 19 條第一項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」

[5] 通訊保障及監察法第 3 條。

於其通訊內容有隱私或秘密之合理期待時，屬於通保法所要保障之通訊。

通保法除規範國家為犯罪偵查而訂有進行通訊監察所需具備之要件與程序外，依實務見解[6]，在私人之間違法監察他人通訊的情形亦有相關刑責的適用。不可不慎。

【管理 TIPS】

隨著生活模式不斷改變，「穿戴式裝置」的定義已擴大到包括我們與之互動的所有可攜式裝置。現今穿戴式因可獲取許多個人資訊，例如：獲取與管控關於健康、位置及工作任務的資訊。

一般消費者在選擇資通訊產品時，通常沒有能力直接檢驗產品的資訊安全性，因此需要在選購之時挑選商譽、技術較值信賴的品牌，注意其產品內的使用者授權條款範圍是否合理、售後服務(如軟體漏洞修補、更新)是否確實等。

若是組織或企業的角色，則應於購入資通設備前，詳細檢視相關報告及技術文件，確認潛在之資安風險。如發現該設備有諸如使組織機密洩漏或遭竄改之可能時，基於風險控制之考量，應該執行風險規避，不予採購；但如已購入或該設備為組織運作所必須者，則應採取相對應之控管機制或其他補償性措施，以降低風險或風險轉嫁。例如行政院即曾發函予各機關[7]，禁止於公務環境使用中國大陸廠牌之資通設備，以避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩，造成國家資通安全危害風險。

【相關標準】

ISO27001:2013(CNS27001)

---

[6] 最高法院 101 年度台上字第 3416 號刑事判決要旨：「通訊保障及監察法第二十四條第一項規定：「違法監察他人通訊者，處五年以下有期徒刑」，其犯罪行為主體並未規定限於公務員；參酌同條第二項所規範之對象，為執行或協助執行通訊監察之公務員或從業人員，第三項則為前二項營利犯罪之行為人，足見其第一項之處罰對象應係針對一般人民；況若認同條第一項之犯罪主體亦以公務員為限，則與同條第二項所規定之犯罪主體雷同，其第一項規定豈非成為具文；又同法第三十條復規定同法第二十四條第一項之罪，須告訴乃論，苟同法第二十四條第一項之犯罪主體限於公務員，則公務員違法監察他人通訊，不僅侵犯被害人之隱私權，更違背公務員之忠實義務，有辱官箴，實不宜規定為告訴乃論之罪，足見同法第二十四條第一項之罪所規範之行為人，應為一般人民。」

[7] 行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函。

- A.13.1.2 網路服務之安全

(1) 標準內容： 應識別所有網路服務之安全機制、服務等級及管理要求事項，並應被納入網路服務協議中，不論此等服務係由內部或委外提供。

(2) 適用說明： 組織應確保無論是內部或外部服務，其所使用之網路已具備相關安全機制，以進行網路服務之管理與安全維護，當設備需要透過網際網路進行資料傳輸時，因此應具備相當之通訊安全措施，避免第三方透過弱點入侵導致相關損害。

ISO27001:2013(CNS27001)

- A.18.1.1 適用之法規及契約的要求事項之識別

(1) 標準內容： 對每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織為符合此等要求之作法。

(2) 適用說明： 組織在業務開發時應瞭解並依循其應適用之法令，以避免觸法。以本案例而言，當組織在開發兒童智慧手錶時，並未清楚認知到其所應適用之法律，導致當政府機關下達禁止兒童使用智慧手錶要求時，組織將蒙受損失。

關鍵字	通訊保障及監察法、設備資訊安全

肆、資訊應用(Application)

類別：資訊應用【案號：A 11027】

歐盟執委會提出人工智慧法令，制定一致性規則草案

【焦點話題】

2021 年 4 月 21 日歐盟執委會提出人工智慧(Artificial Intelligence,下簡稱 AI)法令制定一致性規則(下稱本規則)草案，而後續歐洲議會將針對該提案其進行討論。此份首度針對人工智慧的架構性法案，將伴隨歐盟會員國的協調計畫，加強整個歐盟的人工智慧應用、投資及創新，同時保障人民、企業安全及基本權利。而如歐洲議會與成員國在後續之立法程序中，經審議後採納執委會此次關於 AI 的提案，該通過之法規將直接適用於整個歐盟。與此同時，執委會將繼續與成員國合作實施相關協調計畫中宣布的行動。

【參考資料來源：European Commission Press release，110/4/21】

【重點摘要】

1. 本法對於 AI 系統在歐盟內的市場進入、納入服務應用與各種使用，提供一致性的規則，並可進行市場的監督與管理。
2. 根據風險高低作為管制標準，依據風險高低將相關 AI 系統或應用分為：(1)無法接受的風險，應禁止使用；(2)高風險，應嚴格管理；(3)其他低風險，僅須負擔基本的透明度義務。

【法律觀點】

法規中依照風險高低的程度，將使用 AI 所具有的風險區分為三種，由高至低分別為：無法接受的風險(unacceptable risk)、高風險(high risk)，以及低風險或最小風險(low or minimal risk)。

一、無法接受的風險係來自於對人類的安全、生活及各種權利純粹帶來威脅的 AI 系統，這類系統應被禁止使用。即下列四種情況[1]：

[1] Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial

(1)該系統設置的影響人類意識的技術，使其將傷害自身或他人(例如使用語音助理的玩具，會勸誘幼童進行危險行為)；(2)利用特定族群的弱點，如年齡、身體或精神障礙等，影響其行動並造成其身體或心理上的傷害；(3)可提供政府進行「社會評分」的 AI 系統，進一步利用該系統進行分類與不合理的差別待遇；(4)除為了鎖定特定犯罪或避免恐怖攻擊等特定情況外，在公共場合使用即時遠端生物辨識系統。

二、當 AI 技術運用於下列領域時，將被認為屬於高風險[2]，並會有相關的限制或要求：

(一) 涉及的領域包括(1)使用生物辨識或分類系統；(2)關鍵基礎設施，如交通建設，可能對民眾的生命健康產生風險；(3)教育或職業訓練，可能決定某人接受教育與專業課程的機會，如大考評分；(4)就業與員工管理，如求職程序中使用履歷分類軟體；(5)必要的公私領域服務，如透過信用評分拒絕民眾貸款；(6)法律執行，可能干涉民眾基本權，如評估證據的可信度；(7)移民、庇護及邊境管制，如檢核旅行文件的真實性；(8)司法或民主程序，如適用法律於個案事實的行為等。

(二) 在開發運用於高風險領域的 AI 系統時，如運用資料進行 AI 之訓練、驗證或測試時，該資料集應滿足下列要求[3]：

(1)應採取適當的資料治理與管理措施；(2)與 AI 系統所欲運用的人群間具備關聯性、代表性，且無錯誤且完整；(3)配合其使用目的，參考特定區域、行為或功能相關的特徵或元素；(4)避免 AI 系統產生偏見而進行監測或校正而有必要時，得使用相關個人資料，但應採取當前最新的技術保護相關個資隱私。

三、而上述以外的其他 AI 服務例如聊天機器人，或支援 AI 的電視遊戲，屬於低風險 AI，草案中對於此類型的 AI 服務提供者，鼓勵其制訂其自身的行為守則

Intelligence Act) and Amending Certain Union Legislative Acts, Art.5.

[2] Id., Art.6 & Annex III.

[3] Id., Art.10

(Code of conduct)，以自願之方式落實本草案中相關義務要求[4]。

而若違反前述法規中要求之義務時，最高可處以 3,000 萬歐元或全球年營收的6%的金額做為罰鍰，並應視何者金額較高而定[5]。

值得注意的是，本規則如同歐盟一般資料保護規則(GDPR)，亦具備域外效力，即便 AI 系統服務提供者位於歐盟境外，只要其所提供的 AI 系統服務或應用該系統之產出在歐盟境內，依然屬於本規則適用範圍內[6]。因此我國廠商如有提供類似服務者，應密切注意相關的法規發展情形與衍生的法遵議題，於開發 AI 系統或提供服務前，確認是否符合相關法規之要求。

【管理 Tips】

為確保資通系統之安全性，宜就相關系統進行相關盤點、風險評估，為分級管理，較高風險之系統宜有較高強度之管理義務，參考本規則第二章節之相關內容，高風險的 AI 系統於進入市場運用前，另應負擔下列相關管理義務，如：

- 在開發與應用 AI 的生命週期內進行充分的風險管理程序[7]。
- 撰擬 AI 系統的技術文件證明其符合法規要求並可供主管機關評估其合規性[8]。
- AI 系統應具備留存行為軌跡紀錄(Logs)的功能，以確保運作結果可受監控與追蹤[9]。
- 提供使用者清楚且充分的資訊，包括服務提供者的資料、系統的目的、安全保護的等級、可能會發生誤用等相關風險等情形[10]。

---

[4] Id., Art.69.
[5] Id., Art.71.
[6] Id., Art.2.
[7] Id., Art.9.
[8] Id., Art.11.
[9] Id., Art.12.
[10] Id., Art.13.

- 妥適的人為監督程序以降低風險[11]。
- 保持充分水準的穩定性、安全性與準確性[12]。

【相關標準】

ISO27001：2013(CNS27001)

- A. 6.1.2 資訊安全風險評鑑與 A.6.1.3 資訊安全風險處理

(1)標準內容： 組織應定義及應用資訊安全風險評鑑過程(下略)；組織應定義並應用資訊安全風險處理過程(下略)。

(2)適用說明： 根據規則第 9 條要求，應用高風險 AI 系統時，應建立風險管理系統，該管理系統應能持續處理 AI 系統全生命週期之風險。

關鍵字	人工智慧、AI、風險、生物辨識、社會評分

[11] Id., Art.14.

[12] Id., Art.15.

類別：資訊應用【案號：A11028】

衛福部官方「台灣社交距離」App 登場！

【焦點話題】

降低人群互動及暴露風險的官方 App「台灣社交距離 App」係由衛生福利部疾病管制署與台灣人工智慧實驗室共同研發。這款 App 主要透過蘋果及 Google 合作研發之新冠肺炎病毒追蹤技術來打造，除了強調隱私，也改運用藍牙技術而非電信追蹤來記錄用戶彼此間距離遠近。用途上，App 也能在出現確診者時發出廣播，到其他有安裝此 App 之手機上，提醒用戶是否有接觸風險，作為之後旅遊、通勤、購物的決策參考，並強調去中心化，只會將資料儲存在用戶自己的手機端，不會上傳至雲端中心。

【參考資料來源：自由時報，110/04/19】

【重點摘要】

1. 台灣社交距離 App 主要透過藍牙近距離傳輸特性，並採去中心化架構，以降低資訊外洩之風險。但亦因其功能牽涉個人資料之蒐集、處理及利用，為確保民眾權益並兼顧與社會安全，政府亦須嚴格把關防疫 App 之安全性。
2. 目前我國於疫情警戒期間之相關資料蒐集係依嚴重特殊傳染性肺炎防治及紓困振興特別條例第 7 條作為法規依據，惟該特別條例於法界亦有不同意見，實際上個別作為仍應檢視是否有其他法源依據，以避免嗣後爭議。

【法律觀點】

嚴重特殊傳染性肺炎(COVID-19)疫情在世界各國持續緊張，我國在防疫上以加強民眾隔離、檢疫以及建置多項智慧防疫系統[1]等多項措施，使國內疫情暫時趨緩。然而智慧防疫系統，例如台灣社交距離App對於是否有個資相關疑慮，仍

[1] 衛生福利部-建立健康安全防護網，持續優化科技智慧防疫 (網址：https://www.mohw.gov.tw/cp-4631-54201-1.html，最後瀏覽日：110 年 7 月 7 日)

有待討論。

台灣社交距離App為利用藍牙訊號強度，偵測使用者間接觸的距離與時間。依照個人資料保護法(下稱個資法)第2條規定，姓名、聯絡方式及社會活動等得以識別特定個人之資料時，均屬個人資料。在蒐集個資時，即須符合個資法第15、16條針對蒐集、處理及利用之相關規定，此外蒐集民眾個人資料時，應明確告知當事人包含蒐集機關、目的、個人資料項目、利用期間、利用對象及方式、當事人依個資法可請求的權益及不同意提供時的影響等事項[2]。

中央流行疫情指揮中心說明，台灣社交距離App無須註冊及登錄資料，不會擷取使用者資訊，也無個人資料上傳，且相關接觸資料僅儲存於個人手持裝置端，用戶可隨時刪除App，具備嚴密維護隱私機制[3]。

針對資料蒐集部分，中央流行疫情指揮中心即以嚴重特殊傳染性肺炎防治及紓困振興特別條例第7條規定[4]，作為其法源依據。另外，針對防疫期間違反隔離、檢疫可能者或染疫者，中央流行疫情指揮中心指揮官得公布其個資或實施其他必要措施，同時亦要求於疫情結束後，應回歸個人資料保護相關法規處理，而當疫情結束後，則應屬於特定目的消失，應主動或依當事人之請求，刪除、停止處理或利用該個人資料[5]。目前中央流行疫情指揮中心針對資料蒐集，

---

[2] 個人資料保護法第 8 條：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得 行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。 有下列情形之一者，得免為前項之告知：一、依法律規定得免告知。二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。三、告知將妨害公務機關執行法定職務。四、告知將妨害公共利益。五、當事人明知應告知之內容。六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。」

[3] 衛生福利部-「台灣社交距離 App」常見問答集 Q2 (網址：https://www.cdc.gov.tw/File/Get/nw1Kx64XF3Yn4WeZzHrvxg，最後瀏覽日：110 年 7 月 8 日)

[4] 本處係以嚴重特殊傳染性肺炎防治及紓困振興特別條例第 7 條作為法規依據，惟該特別條例於法界亦有不同意見，緊急命令可解旅遊禁令法源爭議 學者：內容 仍須符合明確及必要，(網址：https://www.rti.org.tw/news/view/id/2055833，最後瀏覽日：110 年 7 月 9 日)，其爭議所在主要係特別條例第 7 條屬概括性條文，實際上個別作為仍應檢視是否有其他法源依據，以避免嗣後爭議。

[5] 個人資料保護法第 11 條第 3 項：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」

公布「『COVID-19(武漢肺炎)』因應指引：實聯制措施指引」，要求各機關對於蒐集之個人資料僅可保存28日[6]。

【管理 Tips】

我國社交距離 App 係透過藍牙傳輸，週期性地廣播隨機 HashID[7]，附近如有安裝該社交距離 App 的裝置，偵測超過一定時間，隨即記錄對方的 HashID，與停留的時間及距離，並儲存於設備中，若有使用者確診之情形，即可透過手機掌握所記錄之其他 HashID 及其停留的時間與距離，更甚者，亦可提醒與該人接近的其他使用者，建議其自行隔離並進行檢驗。

因 HashID 會隨機產生且定期更換，故很難透過 ID 所傳達的資訊連結回特定使用者，且也不容易追蹤特定使用者的行蹤，再加上隨機 HashID 能透露的資訊亦相當有限。此外，App 軟體中只會儲存自己廣播過的隨機 ID，以及收到別人的隨機 HashID，並不儲存其他資料。若需要準確提升事後回溯比對的效果，要有以下前提：1. App 的使用者須正確安裝啟用，並確實將藍牙訊號打開；2. 正確啟用的人數需達一定規模；3. 盡量減少環境障礙物；4. 避免群聚。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 13.2.1 資訊傳送政策及程序

(1)標準內容： 應備妥正式之傳送政策、程序及控制措施，以保護經由使用所有型式通訊設施之資訊傳送。

(2)適用說明： 社交距離 App 須開啟藍牙功能並 24 小時不間斷紀錄相關資訊，因此透過自願性及去中心化等方式，用以維

[6] 「COVID-19(武漢肺炎)」防疫新生活運動：實聯制措施指引五：「各機關對於蒐集之個人資料僅可保存 28 日，屆期即應主動將個人資料予以刪除或銷毀，並應留存執行刪除或銷毀之項目及日期等軌跡紀錄。」

[7] HashID 是指將 ID 透過雜湊演算法，將資料打亂混合，重新建立一個雜湊值所得出的 ID，而透過雜湊演算法所得出的雜湊值可用於唯一地識別機密資訊，且具有不可逆的性質，故具有保護資料的效果。

護資訊傳送的安全性，並定期更新裝置、確保系統為最優化狀態，以降低資訊傳送之風險。

ISO 27001：2013(CNS 27001)

- A. 12.5.1 運作中軟體之控制

(1)標準內容： 應實作各項程序，以控制對運作中系統之軟體安裝。

(2)適用說明： 個人於使用 App 時，應注意使用官方應用程式商店所發布具有一定安全性之 App，且當軟體修補程式能協助移除或減少資訊安全弱點時，亦應安裝之。

關鍵字	個人資料保護法、嚴重特殊傳染性肺炎防治及紓困振興特別條例、HashID

類別：資訊應用【案號：A11029】

微軟啟用「無密碼登入」新趨勢

【焦點話題】

近年資料外洩與網路釣魚事件頻傳，根據微軟 Microsoft Defender Antivirus 遙測數據指出，平均每秒有 579 起密碼攻擊事件正在發生，可見傳統密碼成為駭客攻擊的首要目標之一。為加強保護企業及使用者的機密資訊，微軟推動多因素驗證(Multi-Factor Authentication, MFA)已行之有年。自 2018 年起，微軟帳戶、Edge 瀏覽器及 Windows 10 皆已陸續支援使用者可透過 Windows Hello 與 FIDO2 安全性金鑰登入。另於 2021 年 9 月正式宣布全球企業使用者可以完全捨棄傳統密碼，採用無密碼(Passwordless)登入，幫助使用者省去設定、更改密碼的繁雜程序，並避免可能發生的密碼問題，加速邁向無密碼時代。

【參考資料來源：ETtoday 新聞網，110/09/19; 微軟新聞中心，110/09/17】

【重點摘要】

1. 我國資通安全管理法(下稱資安法)對於防護需求等級為普級或中級之資通系統，要求須具備唯一識別及鑑別機關使用者之功能，且禁止使用共用帳號；對於高級之資通系統，則除前述要求外，另須對帳號之網路或本機存取採取多重認證技術。

2. 目前資安業界致力於發展新的登入方式，以克服舊有密碼機制所存在的問題。例如新的網路識別標準 FIDO(Fast Identity Online)採用公開金鑰基礎架構，伺服器端不再保存帳號密碼，逐漸成為企業兼顧安全與使用者便利性的選擇之一。

【法律觀點】

為使資通系統具備基本之安全防護能力，系統登錄帳號之安全十分重要，相關防護措施諸如在資安法對於各機關的資通安全要求之中，於資通安全責任等級分級

辦法附表十的識別與鑑別構面中，列有「內部使用者之識別與鑑別」之控制措施：對於防護基準為普級或中級之資通系統，要求須具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，且禁止使用共用帳號；對於高級之資通系統，則除前述要求外，另外須對帳號之網路或本機存取採取多重認證技術。

然而上述密碼(通行碼)之設置要求，其強度依密碼的複雜度而改變，在為了追求安全性的前提下使用高複雜度的密碼，在使用上將較不便利，因此現今業界已在研擬是否有更佳的替代作法。案例當中所提及之無密碼登入即是替代方案的概念，例如採行多重因素驗證取代傳統密碼登入機制；以此類作法不僅可達到兼顧安全性與便利性的使用需求，而若以我國資安法規定來看，亦能符合對於重要程度高的資通系統防護要求，顯示此類無密碼登入機制在資安防護上具有相當的效益，值得組織或企業加以參考。

【管理 Tips】

現代人與資訊、資通系統密不可分，每個網路平台都要求設置帳號密碼，這也是基本的資安防護措施。然而隨著數位服務逐漸增加，使用者必須設定、管理多組帳號密碼，耗時費力之餘，更可能增加資安風險。微軟根據使用者統計，指出傳統密碼的四大問題，包括:「設定及管理密碼程序繁雜」[1]、「密碼難以保存」[2]、「使用者習慣反而增加密碼攻擊威脅」[3]、「密碼本身存在的資安風險」[4]。

---

[1] 根據微軟的統計，近年來密碼的設定要求日益複雜，時常必須包含符號、數字、區分大小寫，必須定期更新又不允許使用舊密碼。43%的受訪者每月都會遇到密碼問題，更有 30%因此停止使用帳戶或服務，而非進行密碼重置，顯示出創建足夠安全又能記住的密碼是一項挑戰。

[2] 微軟的統計指出，27%的受訪者僅依靠記憶來儲存密碼，更有 28%會將所有密碼寫下，以紙本記錄的方式保存不僅容易遺失，更增加資訊外洩的風險。

[3] 微軟的統計指出，使用者為了能記住密碼，經常使用與自身相關的現成字詞，根據近期微軟調查，30%的受訪者表示使用與寵物、家人相關的密碼，其他常見的包含姓氏、生日等個人資訊，更有 10%的受訪者坦承所有帳號都使用同一組密碼。此外，更有 40%表示設定密碼時皆有公式，例如本年秋季使用 Fall2021，隨著冬天、春天來臨便改為 Winter2021、Spring2022。這些設定習慣皆讓駭客可在快速瀏覽使用者的社群媒體後，更輕鬆快速地破解密碼。

[4] 微軟指出，一旦帳號密碼外洩，便經常被發布在暗網上以攻擊用途出售。駭客可利用諸多工具與技術，透過「密碼噴灑」(password spraying) 的方式亂槍打鳥嘗試侵入帳戶，也能以網路釣魚手法讓使用者在假冒網站

過去習慣的密碼登入方式，由於是以使用者為核心，因此多圍繞著使用者的習慣進行管理；然而這樣容易衍生出許多問題與風險，包括密碼難以記憶，寫下來又容易遺失、密碼外洩之後帳戶遭受攻擊等。為解決這些問題，網路身分驗證的不斷發展演進，例如簡訊動態密碼[5]、兩步驟驗證[6]等，都已日漸普及，現階段資安業界致力於發展新的登入方式，以克服舊有密碼機制所存在的問題。

例如，網路識別標準 FIDO(Fast Identity Online)以便於使用(ease of use)、隱私安全(privacy and security)以及標準化(standardization)為原則，其特徵在於透過公開金鑰加密(Public Key Cryptography)的架構，使「伺服器端將不再保管祕密」。從驗證架構上來看，傳統密碼的驗證架構中，個人裝置與伺服器都會記錄帳號與密碼以進行驗證；而 FIDO 則是採用公開金鑰基礎架構，FIDO 認證伺服器端(FIDO Authentication Server)只保存相對應的公鑰，而私鑰只保存在裝置端。使用者在登入時只需於其裝置上用私鑰解鎖進行登入，而不需將帳號密碼傳送至雲端服務的伺服器上管理。

類似 FIDO 以搭配多重因素驗證、實體安全金鑰以及生物辨識登入等方式來保護帳號的作法正持續發展中，值得企業或組織予以關注，並思考以之協助升級組織內部系統登入機制的可行性，以此提升組織的資安防護。

【相關標準】

ISO 27001：2013(CNS 27001)

- A. 9.4.2 保全登入程序

(1)標準內容： 當存取控制政策要求時，應以保全登入程序，控制對系統

中輸入帳號密碼。前述攻擊手法並不高深複雜，數十年來駭客持續使用卻仍然有效，原因是密碼依然由「人」所設置。

[5] 例如消費者每次於網路交易，或是使用金融服務進行非約定帳號轉帳時，系統自動發送一組簡訊「動態密碼」至消費者手機，必須輸入該動態密碼後進行身分驗證，以完成交易。

[6] 兩步驟驗證通常是配合手機簡訊或應用程式使用，用戶在帳戶裡設定好兩階段驗證，往後在登入帳戶時，會有一組驗證碼透過簡訊或是藉由 App 產生，用戶需要輸入這組驗證碼登入帳號。

及應用之存取。

(2)適用說明： 組織應建置存取控制政策與相關措施，並透過適當的保全登入程序，管理與控制內部與外部人士對資訊系統之存取與應用。例如對於重要系統之登入進行限制，避免系統及應用遭到未經授權之存取。

ISO 27001：2013(CNS 27001)

- A. 9.4.3 通行碼管理系統

(1)標準內容： 通行碼管理系統應為互動式，並應確保嚴謹通行碼。

(2)適用說明： 關於資訊存取控制，使用者對於個人通行碼應盡保護及保密責任，且使用者初次登入電腦系統後應立即更改預設之通行碼。例如通行碼之長度應大於 8 碼、強度上應包含英文大小寫、數字與特殊符號、3 個月更換一次等等，均為通行碼管理政策的實踐。惟本案例中指出傳統密碼不僅不便利，且增加資安風險，故無密碼登入已成為身分驗證的新趨勢。

關鍵字	網路識別標準 FIDO、資通安全管理法、通行碼

類別：資訊應用【案號：A11030】

歐盟對抗假消息之實務準則與指引

【焦點話題】

為了維護民主的穩定與社會公民的信任，並能兼顧保障言論自由，面對日益氾濫的假消息帶來的衝擊，歐盟理事會於 2018 年 6 月 28 日通過了假消息實務準則(Code of Practice on Disinformation，下稱本準則)，以建立管制假消息的有效機制，作為歐盟民主行動計畫一部分。包括 Facebook, Google, Twitter, Mozilla, Microsoft 及,TikTok 等數位巨頭均陸續加入簽署本準則，承諾落實本準則所要求對於假消息的共同管理措施[1]，而其亦作為對抗關於 COVID-19 疫情期間的假消息問題的方式之一[2]。但準則實施三年多來，亦發現有諸如在不同平台或會員國適用上的不一致或不完全、對於準則承諾上的落差、缺乏適當的監控機制、缺乏平台承諾配合提供相關資料以供研究等問題，因此於 2021 年 5 月歐盟執委會又公布了對於準則的強化指引，對上述問題做出改善建議，並預計讓參與簽署的企業與機構依據指引將準則做出進一步的補充修正，在此同時並陸續邀請更多的企業與機構加入簽署[3]。

【參考資料來源：European Commission Press release，110/10/1】

【重點摘要】

1. 歐盟推動假消息實務準則與指引，從審查廣告投放、管制政治廣告或特定議題的廣告、誠信服務、賦予消費者權力、賦予研究團體權力等五大面向，要求簽署之平台業者依照相關原則自主落實相關要求，並同步結合社群與相關

[1] Roadmaps to implement the Code of Practice on disinformation(網址：https://digital-strategy.ec.europa.eu/en/news/roadmaps-implement-code-practice-disinformation，最後瀏覽日：110 年 10 月 22 日)

[2] First baseline reports – Fighting COVID-19 disinformation Monitoring Programme(網址：https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme，最後瀏覽日：110 年 10 月 22 日)

[3] Code of Practice on disinformation: Commission welcomes new prospective signatories and calls for strong and timely revision(網址：https://ec.europa.eu/commission/presscorner/detail/en/IP_21_4945，最後瀏覽日：110 年 10 月 22 日)

利害團體，共同防制假消息。

2. 包括 Facebook, Google, Twitter, Mozilla 等簽署者均依照上述五大方向訂定相關政策並採取行動，從系統流程、技術工具、資源支持等方面貫徹準則所要求之內容。

【法律觀點】

目前我國對於散布假消息之行為，雖已有包括刑法[4]、社會秩序維護法[5]、農產品市場交易法[6]、災害防救法[7]、傳染病防治法[8]等規定對於散布假消息之處罰或禁止規定，但普遍來說並沒有對於假消息之事前預防、事中更正、事後復原之整體性規定[9]。況且假消息的種類眾多，未必均能適用相關處罰規定。考量假消息對於公共利益、社會安全與言論自由的影響，歐盟此次的準則與指引即採取政府機關、企業平台與公共團體協力合作之方式來管理假消息，並開放由參與者自行簽署承諾準則中所規定之事項，而非上命下從式的強制規定。

準則與指引之重要管制措施略有：

- 審查廣告投放[10]

  準則：透過限制廣告投放之位置，並與查核組織合作或利用查核工具，降低

[4] 刑法第 253 條第 3 項：「意圖影響第一項物品之交易價格，而散布不實資訊者，處二年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

[5] 社會秩序維護法第 63 條第 1 項第 5 款：「有左列各款行為之一者，處三日以下拘留或新臺幣三萬元以下罰鍰：...五、散佈謠言，足以影響公共之安寧者。」

[6] 農產品市場交易法第 6 條第 2 項：「任何人不得故意散播影響農產品交易價格之謠言或不實訊息。」

[7] 災害防救法第 41 條第 3 項：「散播有關災害之謠言或不實訊息，足生損害於公眾或他人者，處三年以下有期徒刑、拘役或新臺幣一百萬元以下罰金。」

[8] 傳染病防治法第 63 條：「散播有關傳染病流行疫情之謠言或不實訊息，足生損害於公眾或他人者，科新臺幣三百萬元以下罰金。」

[9] 傳染病防治法第 9 條：「利用傳播媒體發表傳染病流行疫情或中央流行疫情指揮中心成立期間防治措施之相關訊息，有錯誤、不實，致嚴重影響整體防疫利益或有影響之虞，經主管機關通知其更正者，應立即更正。」可算是事中更正類型之法令。

[10] Code of Practice on Disinformation, Point 1; Guidance on Strengthening the Code of Practice on Disinformation, Point 4.

錯誤廣告對投放者帶來利益的可能性。

指引：透過措施過濾重複提供假消息的業者。

- 管制政治廣告或特定議題的廣告[11]

  準則：確保廣告透明度，關於政治贊助或是特定議題立場的廣告，應揭露其贊助情形，並讓網路使用者易於識別。

  指引：提供更有效率的標籤讓使用者能區分此類廣告，甚至在經過免費轉載或透過社交平台分享後仍能辨認出該內容曾被贊助，並加強對精準投放與 API 的管理。

- 誠信服務[12]

  準則：管理假帳號或自動機器人產生的訊息，避免使用者混淆。

  指引：透過政策與措施因應駭客入侵洩漏、收購帳號、創建虛偽群組、深度偽造(deep fake)等持續演進的行為操縱技術。

- 賦予消費者權力[13]

  準則：投資、發展相關科技，協助使用者能優先檢索到真實或權威的資訊，並與各利益方合作，以加強批判性思維與數位媒體閱讀能力。

  指引：具推薦功能的系統應具備可排除錯誤訊息的措施，設計可標籤錯誤訊息的系統以提供識別，並提供使用者標註假消息的功能。

- 賦予研究團體權力[14]

  準則：在保護隱私的前提下，不禁止或阻止研究單位對平台上的廣告、訊息

[11] Code of Practice on Disinformation, Point 2-4; Guidance on Strengthening the Code of Practice on Disinformation, Point 5.

[12] Code of Practice on Disinformation, Point 5-6; Guidance on Strengthening the Code of Practice on Disinformation, Point 6.

[13] Code of Practice on Disinformation, Point 7-11; Guidance on Strengthening the Code of Practice on Disinformation, Point 7.

[14] Code of Practice on Disinformation, Point 12-15; Guidance on Strengthening the Code of Practice on Disinformation, Point 8.

或資料集進行研究。

指引：建立即時可取得平台資料的架構，並兼顧相關權利(如隱私權)的保護。全面提升與事實查核者的合作，減少不同會員國於此方面的落差。

【管理 Tips】

另外準則附件也提供了關於上述五大管制面向的最佳實務做法[15]：

- 廣告政策：可透過尋找假消息可獲得利益的方法並防止惡質活動者因此獲利，如臉書的假新聞政策規定會移除違規帳號或相關內容以影響該行為人的經濟誘因。
- 政治廣告政策：增加政治廣告的透明度並使消費者了解其為何會看相關廣告，如 Google 的廣告政策讓消費者可自行決定其所能見到的廣告。
- 誠信服務政策：限制不實用戶濫用平台，如 Twitter 的冒名政策規定如帳號以混淆或欺騙方式假冒他人，該帳號將被永久禁用。
- 賦權與消費者的政策：提供使用者資訊、工具與支援讓消費者使用網路服務時獲得更多權力，如 Facebook 提供工具使消費者可以通報假新聞。
- 賦權與研究團體的政策：鼓勵團體研究平台上的假消息與政治廣告，如 Mozilla 提出的資訊與信任倡議(Mozilla Information Trust Initiative, MITI)，致力於開發產品、研究及相關社群以對抗資訊污染與假消息。

【相關標準】

ISO27001：2013(CNS27001)

- A. 18.1.1 適用之法規及契約的要求事項之識別

(1) 標準內容： 對於每個資訊系統及組織，應明確識別、文件化及保持更新所有相關法律、法令、法規及契約要求事項，以及組織

[15] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54455(最後瀏覽日：110 年 10 月 25 日)

為符合此等要求之作法。

(2) 適用說明： 平台對於其所同意簽署之準則，應就其同意之部分，努力推動對於假消息之防制。

關鍵字	假消息、精準行銷、廣告審查、資訊透明、誠信服務

伍、自我評量

是非題

1. (X) 公務機關應每兩年向上級或監督機關提出資通安全維護計畫實施情形。**【資訊保護 S11001】**

   解析：根據資通安全管理法第 12 條規定：「公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。」公務機關應每年提出資通安全維護計畫實施情形給上級或監督機關，故答案為錯誤。

2. (X) 我國公務機關因應資安事件時，應於知悉後二小時內通報主管機關。**【資訊保護 S11002】**

   解析：依據資通安全事件通報及應變辦法第 4 條第 1 項規定：「公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。」故應在知悉後一小時內通報，答案為錯誤。

3. (O) 依照我國個人資料保護法所定告知之方式，不限以書面方式告知當事人。**【資訊保護 S11003】**

   解析：依照個人資料保護法施行細則第 16 條規定：「依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。」故本題答案為正確。

4. (O) 不動產經紀業應區分直接蒐集與間接蒐集個資的情形，並分別訂定告知方式、內容及注意事項，並要求所屬人員確實辦理。**【資訊保護 S11004】**

   解析：根據不動產經紀業個人資料檔案安全維護管理辦法第 10 條規定：「經紀業於蒐集個人資料時應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。」故答案為正確。

5. (O) 資通安全指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。**【資訊保護 S11005】**

   解析：依據資通安全管理法第 3 條第三款定義：「三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。」故答案為正確。

6. (O) 如我國公務員因職務或業務知悉或持有我國國防以外應秘密之文書、圖畫、消息或

物品且進而洩漏或交付，將構成刑法公務員洩漏國防以外秘密罪。**【資訊保護 S11006】**

解析：根據刑法第 132 條規定:「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。因過失犯前項之罪者，處一年以下有期徒刑、拘役或九千元以下罰金。」故答案為正確。

7. (O) 公務機關使用資通訊產品時，宜審慎評估產品之來源。**【資訊保護 S11007】**

解析：為避免公務及機敏資料遭不當竊取，導致機關機敏資訊外洩或造成國家資通安全危害風險，公務機關之資通設備及服務，宜採用受信任之供應商或非敵意勢力所控制者，並避免採購具資安風險之產品。故答案為正確。

8. (X) 金融資安行動方案提出金融改革與便民服務為主軸之四大精進方向。**【資訊保護 S11008】**

解析：依照金管會推動「金融資安行動方案」，金融資安行動方案係提出強化資安監理、深化資安治理、精實金融韌性及發揮資安聯防等四大策勵方向，據此提列 36 項執行措施，並以此方向修訂資安自律規範，使金融機構有所遵循，故答案為錯誤。

9. (O) 非一般涉及該類資訊之人所知之方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊為營業秘密之範疇。**【資訊保護 S11009】**

解析：依照營業秘密法第 2 條規定：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」故答案為正確。

10. (O) 各機關應依照分級辦法所分類的資通安全等級 A 級至 E 級的公務與非公務機關，在管理面、技術面、認知與訓練面，應當依照該辦法附表一至附表八規定之事項辦理。**【資訊保護 S11010】**

解析：依照資通安全責任等級分級辦法第 11 條規定：「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。」而附表一至附表八中，資通安全等級 A 級到 C 級分公務機關及特定非公務機關，各有不同應辦事項，則等級 D 級與 E 級為各機關適用之應辦事項，故答案為正確。

11. (X) 特定非公務機關於知悉資通安全事件時，應向上級機關通報。**【資訊保護 S11011】**

解析：依據資通安全管理法第 18 條第 2 項規定：「特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。」且依同條第 3 項特定非公務機關應向中央目的事

業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。所以特定非公務機關通報對象應為中央目的事業主管機關，故答案為錯誤。

12. (X) 雇主在招募或僱用員工時，得因為求人員對於公司或業主向心力，可視情況所需，留置其國民身分證、工作憑證或其他證明文件，或要求提供非屬就業所需隱私資料。**【資訊保護 S11012】**

解析：依據就業服務法第 5 條第 2 項第二款規定：「雇主招募或僱用員工，不得有下列情事：二、違反求職人或員工之意思，留置其國民身分證、工作憑證或其他證明文件，或要求提供非屬就業所需之隱私資料。」故答案為錯誤。

13. (O) 公務機關應考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。**【資訊保護 S11013】**

解析：根據資通安全管理法第 10 條規定：「公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。」故答案為正確。

14. (X) 公務機關或非公務機關當個資遭到竊取、洩漏、竄改或其他侵害時，應確認情事後，依事件損害程度大小決定是否通知當事人，程度準則由機關明定之。**【資訊保護 S11014】**

解析：根據個人資料保護法第 12 條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」無論事件損害程度大小，都應以適當方式通知當事人。本法施行細則第 22 條則明定通知方式使當事人可得知悉之方式為之，故答案為錯誤。

15. (O) 智慧型手機系統內建軟體資通安全檢測技術規範將智慧型手機資通安全等級區分為初級、中級及高級。**【資訊保護 S11015】**

解析：為配合不同安全需求，NCC 訂定之智慧型手機系統內建軟體資通安全檢測技術規範中，將智慧型手機資通安全等級區分為初級、中級及高級，並對各安全等級有不同適用要求及說明。故答案為正確。

16. (O) 公務機關或特定非公務機關遇到資安事件時，依資通安全管理法及相關規定，且依資通安全事件之嚴重性，並於知悉後，於 1 小時內依主管機關或中央目的事業主管機關指定之方式，進行資通安全事件之通報。**【資訊保護 S11016】**

解析：依資通安全事件通報及應變辦法第 4 條第 1 項規定：「公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。」；同辦法

第 11 條第 1 項規定：「特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。」

17. (O)　針對業務督導不力，致其屬員、所屬或所監督機關之人員違反公務機關所屬人員資通安全事項獎懲辦法第 4 條第 1 到 3 款事項，亦應予懲處之對象。**【資訊保護 S11017】**

解析：根據公務機關所屬人員資通安全事項獎懲辦法第 4 條第 4 款規定：「一、未依本法、本法授權訂定之法規或機關內部規範辦理下列事項，情節重大：(一)資通安全情資分享作業。(二)訂定、修正及實施資通安全維護計畫。(三)提出資通安全維護計畫實施情形。(四)辦理資通安全維護計畫實施情形之稽核。(五)配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。(六)訂定資通安全事件通報及應變機制。(七)資通安全事件之通報或應變作業。(八)提出資通安全事件調查、處理及改善報告。二、辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。三、其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。四、對業務督導不力，致其屬員、所屬或所監督機關之人員有前三款情形之一。」故答案為正確。

18. (O)　各機關自行或委外開發之資通系統應依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，並依附表十所定資通系統防護基準執行控制措施。**【資訊保護 S11018】**

解析：依照資通安全責任等級分級辦法第 11 條第 2 項規定：「各機關自行或委外開發之資通系統應依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，並依附表十所定資通系統防護基準執行控制措施.....」故答案為正確。

19. (X)　依據金融機構作業委託他人處理內部作業制度及程序辦法，金融機構就委外業務並無監督之義務。**【資訊保護 S11019】**

解析：依照金融機構作業委託他人處理內部作業制度及程序辦法作為第 6 條第 1 項第 2 款規定：「第四條第二項第一款規定之專責單位應執行之事項如下：二、就委外事項涉及客戶權益保障、風險管理及內部控制作業之監督，並定期評估檢討將結果呈報董(理)事會或外國銀行在台分行之總行授權人員，若有重大異常或缺失亦應儘速通報主管機關及中央銀行。」明訂金融機構對於委外作業應負監督之責，故答案為錯誤。

20. (O)　主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。**【資訊保護 S11020】**

解析：依據資通安全法第 6 條第 1 項規定：「主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。」且於本條第 2 項針對關鍵基礎設施提供者內部資料秘密予以保護，故答案為正確。

21. (O)　鑒於資通安全之提升須以全民重視為前提，並須佐以先進之資通安全技術、軟硬體、專業人才等資源，政府應與民間共同提升全民資通安全意識，推動資通安全產業，以利先進資通安全技術、軟硬體、專業人才等之發展。**【資訊保護 S11021】**

解析：根據資通安全管理法第 4 條規定：「為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：一、資通安全專業人才之培育。二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。三、資通安全產業之發展。四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。　前項相關事項之推動，由主管機關以國家資通安全發展方案定之。」，故答案為正確。

22. (X)　公務機關應設置資通安全長，並且機關首長指派具有資安背景之適當人員專任，負責推動及監督機關內資通安全相關事務。**【資訊保護 S11022】**

解析：根據資通安全管理法第 11 條規定：「公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。」為確保有效推動資通安全維護事項，公務機關應置資通安全長，由其成立相關推動組織及督導推動相關工作。考量資通安全長如由副首長擔任，更能提升資通安全於機關中之重要性，並非由人員專任之，故答案為錯誤。

23. (X)　依勞資爭議處理法相關規定，由裁決委員做成之裁決決定書，因涉及當事人個資，故雖屬政府資訊公開法所稱之政府資訊，但以不公開為原則。**【資訊公開 D11023】**

解析：裁決決定書屬政府資訊公開法(下稱政資法)所稱之政府資訊，依政資法之規定，以主動公開為原則。然而當事人自然人名字、身分證統一編號及其他足以識別的個人資料，根據個人資料保護法屬個人資料，依照政資法第 18 條規定應限制公開，僅就其他部分公開之，故答案為錯誤。

24. (O)　地方議會開會時，應依地方立法機關組織準則之規定開放旁聽。**【資訊公開 D11024】**

解析：根據地方立法機關組織準則第 25 條第 2 項第一款規定：「前項公開舉行之會議，依下列規定辦理：一、大會會議應開放旁聽。」故答案為正確。

25. (O)　最輕本刑為三年以上有期徒刑之罪，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。**【資訊監察 M11025】**

解析：根據依照通訊保障及監察法第 5 條第 1 項規定：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全、經濟秩序或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。

一、最輕本刑為三年以上有期徒刑之罪。……」故答案為正確。

26. (O)　利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信即屬於通訊保障及監察法所稱之通訊。**【資訊監察 M11026】**

解析：根據依照通訊保障及監察法第 3 條規定：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。 前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」故答案為正確。

27. (O)　依據人工智慧法律調和規則草案之內容，AI 系統服務提供者位於歐盟境外，只要其所提供的 AI 系統服務或應用該系統之產出在歐盟境內，依然屬於本規則適用範圍內。**【資訊應用 A11027】**

解析：根據人工智慧法律調和規則草案 Article 2，本條例適用於：(a)在歐盟內投放市場或投入使用人工智慧系統之提供商，無論這些提供商是在歐盟內還是在第三國建立；(b)位於歐盟內的人工慧系統之用戶 ; (c)位於第三國的人工智慧系統之提供者與用戶，其中該系統產生的輸出用於聯盟……」故答案為正確。

28. (O)　根據我國個人資料保護法規定，可因執行職務或業務所必須或經當事人書面同意後，雖蒐集之特定目的消失或是期限屆滿，仍可不用刪除當事人之資料。**【資訊應用 A11028】**

解析：根據個人資料保護法第 11 條第 3 項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」故答案為正確。

29. (O)　政府組態基準(Government Configuration Baseline，簡稱 GCB)目的在於規範資通訊設備的一致性安全設定，以降低成為駭客入侵管道而引發資安事件之風險。**【資訊應用 A11029】**

解析：根據行政院國家資通安全會報技術服務中心所公告之 GCB，針對作業系統、瀏覽器、網通設備、應用程式提供說明文件，並說明此基準目的為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)。故答案為正確。

30. (X)　關於歐盟之假消息實務準則(Code of Practice on Disinformation)係採取政府機關、企業平台與公共團體協力合作之方式來管理假消息，並開放由參與者自行簽署承諾準則中所規定之事項，並且為上命下從式的強制規定。**【資訊應用 A11030】**

解析：歐盟之假消息實務準則及後續對於準則的強化指引係即採取政府機關、企業平台與公共團體協力合作之方式來管理假消息，並開放由參與者自行簽署承諾準則中所規定之事項，而非上命下從式的強制規定。故答案為錯誤。

選擇題

1. (1) 請問下列何者不屬於公務機關就資通安全事件之應變訂定作業規範內容?(1)應變小組之私下討論記錄(2)事件發生前之演練作業。(3)事件發生後之復原、鑑識、調查及改善機制。(4)應變小組之組織。**【資訊保護 S11001】**

   解析：根據資通安全事件通報及應變辦法第 10 條規定：「公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：一、應變小組之組織。二、事件發生前之演練作業。三、事件發生時之損害控制機制。四、事件發生後之復原、鑑識、調查及改善機制。五、事件相關紀錄之保全。六、其他資通安全事件應變相關事項。」應變小組之私下討論記錄並非法律規範內包含之內容，故選項(1)為錯誤。

2. (4) 根據我國資通安全管理法第 14 條規定，當公務機關面對資安事件時，下列敘述何者錯誤? (1)公務機關因應資通安全事件，應訂定通報及應變機制。(2)公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告。(3)應變機制之必要事項由主管機關定之。(4)公務機關知悉資通安全事件僅需內部呈核。**【資訊保護 S11002】**

   解析：依據資通安全管理法第 14 條規定：「公務機關為因應資通安全事件，應訂定通報及應變機制。公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。」公務機關知悉資通安全事件應向上級或監督機關及主管機關進行通報，故選項(1)(2)(3)為正確，選項(4)為錯誤。

3. (3) 依照我國個人資料保護法應告知之事項，下列何者不在法定應告知的事項內? (1)個人資料利用之期間、地區、對象及方式。(2)蒐集之目的。(3)蒐集機關的負責人姓名。(4)當事人依第三條規定得行使之權利及方式。**【資訊保護 S11003】**

   解析：依照個資法第 8 條第 1 項規定：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」故選項(1)(2)(4)為正確，選項(3)為錯誤。

4. (4) 非公務機關對個人資料之利用，下列何者錯誤?(1)非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。(2)當事人表示拒絕接受行銷時，應

即停止利用其個人資料行銷。(3)經當事人同意後可進行個人資料之特定目的外利用。(4)蒐集或處理者知悉禁止對該資料之處理或利用時，應等待當事人之請求，刪除、停止處理或利用該個人資料，不得自行處理該個人資料。**【資訊保護 S11004】**

解析：根據個人資料保護法第 19 條第 2 項規定：「蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。」蒐集或處理者知悉或經當事人通知時，應主動刪除、停止處理或利用該個人資料，故選項(4)為錯誤。

5. (3) 依照資通安全管理法第 3 條規定，下列對資通安全事件之敘述何者正確?(1)指系統經授權之登入。(2)包含一台文書處理電腦偶然當機但不會影響該機關系統運作之事件。(3)是否為資通安全事件應考量對系統之影響以及對機關資通安全政策之威脅。(4)指資料未經加密儲存。**【資訊保護 S11005】**

解析：根據資通安全管理法第 3 條第 4 款規定：「資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅」，故選項(3)為正確。

6. (3) 請問下列何者行為未涉及犯罪?(1)傳送不明連結之簡訊後入侵他人手機致使其個資外洩。(2)藉由隨機寄送含病毒電子郵件入侵他人電腦並竄改其檔案。(3)開啟 Wifi 供人使用。(4)入侵校園考試系統取得學生成績資料。**【資訊保護 S11006】**

解析：依照刑法第 359 條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。」選項(1)、(2)、(4)均係違反刑法第 359 條之行為，故選項(3)為正確答案。

7. (3) 政府機關採購資通安全產品宜考量之內容，下列何者錯誤?(1)資通安全產品是否有共同供應契約可供訂購。(2)評估供應商之可靠性。(3)宜採購大陸廠牌之產品。(4)政府採購法相關規定。**【資訊保護 S11007】**

解析：考量資安即國安之政策方向，政府之資通設備及服務，若由不受信任之供應商或敵意勢力所控制，該供應商或外國勢力很可能藉以破壞我國網路安全、竊取資訊、進行間諜活動、網路攻擊破壞關鍵基礎設施等，故不宜採購大陸廠牌之產品。選項(3)為錯誤。

8. (3) 請問關於個人資料保護法下列何者內容為非?(1)非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(2)中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。(3)非公務機關之個人資料檔案安全維護計畫及處理方法之標準等相關事項之辦

法，由各機關依其機關特性定之。(4)前項所稱之適當之安全措施應依個人資料保護法施行細則第 12 條第二項內容訂之。**【資訊保護 S11008】**

解析：依照個人資料保護法第 27 條規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。　中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」；個人資料保護法施行細則第 12 條第一項：「本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，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。」非公務機關之個人資料檔案安全維護計畫及處理方法之標準等相關事項之辦法，應由中央目的事業主管機關定之，故選項(3)為錯誤。

9. (4)　請問下列何種情形下違反營業秘密法之規定?(1)以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。(2)知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。(3)持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。(4)以上皆是。**【資訊保護 S11009】**

解析：依照營業秘密法第 13-1 條第 1 項規定：「資意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣一百萬元以上一千萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。二、知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。三、持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。四、明知他人知悉或持有之營業秘密有前三款所定情形，而取得、使用或洩漏者。」選項(1)(2)(3)為正確，故選擇選項(4)。

10. (3)　下列敘述何者錯誤?(1)依美國州資安長協會之建議，採購應從最初階段便納入資安評估。(2)進行資安評估時，宜由各利害關係人組成共同團隊為之，以利降低資安風險。(3)進行資安評估時，宜由各利害關係人組成共同團隊為之，以利降低採購成本。(4)美國總統拜登已簽署關於供應鏈資安之行政命令，以確保美國之供應鏈不受干擾，我國亦宜強化供應鏈資安。**【資訊保護 S11010】**

解析：有關宜由相關利害關係人進行資安評估，主要係為確保各層面之風險均受到考量，而非以降低採購成本為出發點。故選項(3)為錯誤。

11. (1) 特定非公務機關發生資通安全事件時之通報，下列敘述何者錯誤? (1)特定非公務機關知悉資通安全事件後，應於二小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。(2)前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。(3) 特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。(4) 特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。**【資訊保護 S11011】**

解析：依據資通安全事件通報及應變辦法第 11 條規定：「特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。 特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。 特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。」特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報，故選項(2)(3)(4)為正確，選項(1)為錯誤。

12. (4) 欲判斷疫苗接種證明是否屬於醫療個資的認定上，應確認下列何者?(1)是否由醫師或醫事人員進行。(2)目的是否為治療、矯正、預防人體疾病、傷害、殘缺。(3)是否有進行「診察及治療」; 或基於以上之診察結果，所為處方、用藥、施術或處置。(4)以上皆是。**【資訊保護 S11012】**

解析：根據個人資料保護法行細則第 4 條第 2 項規定：「本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。」故選項(4)為正確。

13. (3) 請問下列何者不屬於委外辦理資通系統之建置、維運或資通服務之提供，選任及監督受託者時應注意事項?(1)受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。(2)受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。(3) 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應於知悉後 24 小時內通知委託機關及採行之補救措施。(4) 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。**【資訊保護 S11013】**

解析：根據資通安全管理法施行細則第 4 條第 1 項規定：「各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供(以下簡稱受託業務)，選任及監督受託者時，

應注意下列事項：一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。.....六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。.....」受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應採立即通報作業，故選項(3)為錯誤。

14. (4) 依資通安全管理法及其子法之規定，下列就特定非公務機關辦理資通安全事件之通報及應變，何者錯誤?(1)應通報之對象為其中央目的事業主管機關。(2)應通報之時限為知悉事件後之 1 小時內。(3)通報之方式由其中央目的事業主管機關指定。(4)以上皆錯誤。**【資訊保護 S11014】**

解析：根據資通安全事件通報及應變辦法第 11 條規定：「特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。」故選項(4)為錯誤。

15. (1) NCC 為求民眾保持良好使用手機習慣，提供「三不五要」口訣，請問下列何者為「三不五要」?(1)密碼等想到再更新即可。(2) 不瀏覽可疑網站。(3) 手機廢置前要刪除機敏資料。(4) 不瀏覽可疑網站。**【資訊保護 S11015】**

解析：國家通訊傳播委員提倡「三不五要」之使用口訣，加強使用者保護個人資料與隱私安全，而「三不」即為：不強行取得根管理者(root)權限或越獄(JB)、不瀏覽可疑網站、不連接可疑 Wi-Fi 接取點；「五要」則為：要定期更新密碼、要更新軟體程式及備份資料、要關閉未使用的 Wi-Fi/藍牙/NFC 等介面、連接的 Wi-Fi 接取點要開啟加密防護、手機廢置前要刪除機敏資料。故選項(1)為錯誤。

16. (3) 依據資通安全事件通報及應變辦法中資通安全演練作業，下列何者不是作業項目?(1)社交工程演練。(2)資通安全事件通報及應變演練。(3)資料審查。(4)網路攻防演練。**【資訊保護 S11016】**

解析：根據資通安全事件通報及應變辦法第 18 條規定：「公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：一、社交工程演練。二、資通安全事件通報及應變演練。三、網路攻防演練。四、情境演練。五、其他必要之演練。」故選項(3)為錯誤。

17. (4) 資通安全法下之資通安全維護計畫，不包括下列何種事項?(1)核心業務及其重要性。(2)資通安全政策及目標。(3)資通安全推動組織。(4)公務機關資通安全長得依機關情況設

置，不為強制性。**【資訊保護 S11017】**

解析：根據資通安全法施行細則第 6 條規定：「本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：一、核心業務及其重要性。二、資通安全政策及目標。三、資通安全推動組織。四、專責人力及經費之配置。五、公務機關資通安全長之配置。.....」。公務機關資通安全長為應設置之職位故選項(4)為錯誤。

18. (2) 請問根據資通安全責任等級分級辦法，下列何者錯誤?(1)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。(2)行政院直屬機關應每年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。(3)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。(4) 主管機關應每兩年核定自身資通安全責任等級。**【資訊保護 S11018】**

解析：根據資通安全責任等級分級辦法第 3 條第 2 項規定：「行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。」故選項(2)為錯誤。

19. (4) 參照政府資訊作業委外資安參考指引中，下列何者不屬於委外廠商內部控制評估事項? (1)研擬契約時應決定政府機關是否有稽核委外廠商內部控制之權利。(2)或由委外廠商或第三方獨立評估者提出委外廠商內部控制評估報告。(3)擁有眾多客戶之委外廠商通常會事先準備好第三方獨立評估報告，提供客戶以確認其內部控制措施無誤。(4) 以上皆是。**【資訊保護 S11019】**

解析：依照政府資訊作業委外資安參考指引中 2.6.2.19 實施委外廠商內部控制評估之內容，於研擬契約時應決定政府機關是否有稽核委外廠商內部控制之權利，或是由委外廠商或第三方獨立評估者提出委外廠商內部控制評估報告，這些都應事先訂定於契約內。一般而言，擁有眾多客戶之委外廠商通常會事先準備好第三方獨立評估報告，提供客戶以確認其內部控制措施無誤。故選項(1)(2)(3)為正確，故選擇選項(4)。

20. (3) 個人資料保護法第 4 條與個人資料保護法施行細則第 8 條針對個人資料之委外訂有規範，下列敘述何者錯誤? (1)受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。(2)委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。(3)受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應先行採取補救措施，待事件後通知委託機關。(4)委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。**【資訊保護 S11020】**

解析：依據個人資料保護法施行細則第 8 條第 2 項第 4 款規定：「前項監督至少應包含下列事項：四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。」受託者應在違反個人資料保護法、其他個人資料保護法律或其法規命令時，應主動項委託機關通報，而非事後告知，故選項 (3)為錯誤。

21. (4) 政府為與民間共同提升全民資通安全意識，行政院國家資通安全會報組織編列中，設有認知教育及人才培育組，由教育部主辦。請問下列有關於教育部資訊安全人才培育計畫之策略與目標，何者錯誤?(1)跨域教學以培育跨資安人才。(2)國際合作與交流以培養學生國際化視野及培育國際化資安人才。(3)實務實戰以培訓國際資安競賽選手及資安攻防人才。(4)以上皆錯誤。**【資訊保護 S11021】**

解析：根據教育部資訊安全人才培育計畫，為因應國家發展之資安人力需求，教育部推動「資訊安全人才培育計畫」，本計畫主要的推動策略與目標為：1.跨域教學以培育跨資安人才、2.實務實戰以培訓國際資安競賽選手及資安攻防人才、3.產學鏈結以培育產業所需人才、4.資安扎根以發掘具資安潛力學子、5.國際合作與交流以培養學生國際化視野及培育國際化資安人才。故選項(1)(2)(3)為正確，故選擇選項(4)。

22. (2) 請問下列資通安全長或資通安全管理代表之派任何者錯誤?(1)公務機關應設置資通安全長。(2)特定非公務機關與公務機關一樣，應設置資通安全長或是資通安全管理代表。(3)銀行業應指派副總經理以上或職責相當之人兼任資訊安全長。(4)公務機關之資通安全長，由機關首長指派副首長或適當人員兼任。**【資訊保護 S11022】**

解析：根據資通安全管理法第 11 條規定：「公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。」以及金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條：「銀行業應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。但主管機關對信用合作社及票券金融公司另有規定者，依其規定。」對於特定非公務機關是否為指定一定層級之人員擔任資安長或資通安全管理代表除其他法律規定外，並無強制設置，故選項(2)為錯誤。

23. (1) 根據勞資爭議處理法第 47-1 條及政府資訊公開法第 18 條，對於不當勞動行為所製出之裁決決定書，下列敘述何者錯誤?(1)裁決決定書中公開之事項，為求資料完整性及資訊公開為原則，應將當事人之資料詳列於裁決決定書中。(2)中央主管機關應以定期出版、登載於網站或其他適當方式公開裁決決定書。(3)處理或儲存機關公務資訊時，應主管機關

同意。(4)個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者原則上限制公開或不予提供。**【資訊公開 D11023】**

解析：根據勞資爭議處理法第 47-1 條第 2 項規定：「前項公開，得不含自然人之名字、身分證統一編號及其他足資識別該個人之資料。但應公開自然人之姓氏及足以區辨人別之代稱。」以及政府資訊公開法第 18 條第 1 項第 7 款：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：七、個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害該個人、法人或團體之權利、競爭地位或其他正當利益者。但對公益有必要或為保護人民生命、身體、健康有必要或經當事人同意者，不在此限。」為保障個人資料，應限制公開，就公開自然人之姓氏及足以區辨人別之代稱。故選項(1)為錯誤。

24. (3)　與人民權益攸關之施政、措施及其他有關之政府資訊，以主動公開為原則，並應適時為之，請問下列何者非政府資訊公開法第 7 條所述之應主動公開事項?(1)條約、對外關係文書、法律、緊急命令、中央法規標準法所定之命令、法規命令及地方自治法規。(2)施政計畫、業務統計及研究報告。(3)政府機關作成意思決定前，內部單位之擬稿或其他準備作業。(4)請願之處理結果及訴願之決定。**【資訊公開 D11024】**

解析：依照政府資訊公開法第 18 條第 1 項第 3 款規定：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。」政府機關之內部意見或與其他機關間之意見交換等政府資訊，如予公開或提供，因有礙該機關最後決定之作成且易滋困擾，例如對有不同意見之人加以攻訐，自應限制公開或不予提供，惟對公益有必要者，自不在限制範圍之列，故選項(3)為錯誤。

25. (2)　請問下列何者非我國通訊保障及監察法所保障之通訊?(1)簡訊內容。(2)臉書公開貼文。(3)言論及談話。(4)郵件及書信。**【資訊監察 M11025】**

解析：依照通訊保障及監察法第 3 條規定：「本法所稱通訊如下：一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。二、郵件及書信。三、言論及談話。 前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」故選項(2)為錯誤。

26. (3)　個人隱私近年來普遍受國人重視，如欲以高科技電子產品紀錄他人隱私活動、言談或身體隱私部位等，請問下列何者行為恐有違法之虞?(1)甲邀請乙擔任網拍模特兒並支付薪水。(2)丙攝影紀錄家族聚會時光。(3)丁因懷疑女友出軌，擅自於女友家角落裝設微型錄影機，紀錄女友在家的活動情形。(4)戊參加偶像戶外簽唱會並錄影。**【資訊監察 M11026】**

解析：依照刑法第 315-1 條規定：「有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」是以，僅有選項(3)為私人隱私活動且未經允許，故有違法之虞。

27. (4) 面對人類的安全、生活及各種權利純粹帶來威脅的 AI 系統，下列何種形況應被禁止使用?(1)該系統設置的影響人類意識的技術，使其將傷害自身或他人。(2)利用特定族群的弱點，如年齡、身體或精神障礙等，影響其行動並造成其身體或心理上的傷害。(3)可提供政府進行「社會評分」的 AI 系統，進一步利用該系統進行分類與不合理的差別待遇。(4)以上皆是。**【資訊應用 A11027】**

解析：根據人工智慧法律調和規則草案 Article 5 規定禁止人工智慧行為，選項(1)(2)(3)皆為草案禁止事項，另還有除為了鎖定特定犯罪或避免恐怖攻擊等特定情況外，在公共場合使用即時遠端生物辨識系統。故選擇選項(4)。

28. (2) 請問下列何者不屬於我國個人資料保護法所稱之個人資料?(1)姓名。(2)某公司之名稱。(3)財務情況。(4)病歷。**【資訊應用 A11028】**

解析：依照個人資料保護法第 2 條規定：「本法用詞，定義如下：一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。……」，選項(2)為法人之資料而非自然人之資料，故為錯誤。

29. (3) 根據通行碼應符合政府組態基準規範及資通安全責任等級分級辦法之政策，下列何者非設置通行碼時之基準?(1)通行碼長度 8 碼以上。(2)使用者通行碼最短需使用 1 天，最長使用期限為 90 天，且通行碼需保留三次歷史紀錄不得相同。(3)使用者每 60 天應更換通行碼。(4)通行碼複雜度應包含英文大小寫、特殊符號或數字三種以上。**【資訊應用 A11029】**

解析：根據通行碼應符合政府組態基準規範及資通安全責任等級分級辦法之政策，使用者應於每 90 天更換通行碼，以防風險。故選項(3)為錯誤。

30. (4) 關於歐盟假消息實務準則(Code of Practice on Disinformation)之附件，對於審查廣告投放、管制政治廣告或特定議題的廣告、誠信服務、賦予消費者權力、賦予研究團體權力等五大管制面向，提供了的最佳實務做法，請問下列何者為非?(1)可透過尋找假消息可獲得利益的方法並防止惡質活動者因此獲利。(2)增加政治廣告的透明度並使消費者了解其為何會看相關廣告。(3)提供使用者資訊、工具與支援讓消費者使用網路服務時獲得更

多權力。(4)以上皆是。**【資訊應用 A11030】**

解析：依據歐盟此準則之附件，廣告政策：可透過尋找假消息可獲得利益的方法並防止惡質活動者因此獲利；政治廣告政策：增加政治廣告的透明度並使消費者了解其為何會看相關廣告；誠信服務政策：限制不實用戶濫用；賦權與消費者的政策：提供使用者資訊、工具與支援讓消費者使用網路服務時獲得更多權力；賦權與研究團體的政策：鼓勵團體研究平台上的假消息與政治廣告。故選擇選項(4)。