LINE來LINE去，LINE出問題

鍵盤007

失控的手機

LINE來 LINE去， LINE出問題

／鍵盤 007

根據 iThome 於 107 年 3 月間的報導，LINE 用戶已突破 1,900 萬，每天使用 LINE 進行語音通話人數也突破 700 萬，毫無懸念地，LINE 已成為臺灣最主要的社群通訊軟體。舉凡學生喜歡用 LINE 溝通，老師用 LINE 教學分享、指導課業，公務機關亦起而效尤，隨手建立公務群組，藉此橫向連繫、有效溝通。但是每天使用的你，知道它也存在一些「黑歷史」嗎？每天 LINE 來 LINE 去到底會不會出事？其他通訊軟體像是 WhatsApp、Instagram 會不會比較安全？這些疑問從來就沒有消停過！

LINE 近期議題

東森新聞於 2018 年 11 月 29 日報導「手誤傳錯群組，潘姓員警被依過失洩密罪送辦，檢方給予緩起訴處分」，內容陳述 2017 年間偵辦擄人勒贖案的潘姓員警，原本要傳「偵辦進度報告」給負責調閱監視器的同事，卻誤傳到反年金改革的群組「台灣憤怒鳥」，該案檢方於 2018 年給予緩起訴處分，需繳交公庫 3 萬元。

LINE 最常遇到的態樣，當屬詐騙集團竊取個資及財務等問題。趨勢科技所屬「資安趨勢部落格」曾指出詐騙集團善於偽造「瘋傳 7-11 限時發送 100 元禮券」、「FamilyMart 送全家千元禮券」等等詐騙帳號，吸引民眾加入好友或點選釣魚網站連結。據趨勢科技防詐達人調查，臺灣前 15 大 LINE@ 詐騙帳號受害品牌店家，以臭跩貓詐騙貼圖排名第一，共有將近 150 組詐騙 Line@ 帳號；而被發現的詐騙帳號中，1/2 為假貼圖，1/4 則透過假冒如星巴克、王品、中油、全聯、7-11、全家等店家假優惠名義引誘消費者上鉤。

其他通訊軟體，像是 WhatsApp、Instagram 等亦存在類似資安風險，例如 iThome 亦指出 WhatsApp 於 2018 年 10 月才修復一項漏洞，該漏洞允許使用者於視訊通話時，讓駭客有機會操控手機程式。

此外 LINE 也成為假訊息散布平台，長輩、朋友間都用 LINE 轉傳不實消息，例如「菌類不能和茄子一起吃」、「柿子加優

詐騙集團以偽造各種免費貼圖、優惠和抽獎，吸引消費者加入好友或點選釣魚網站，導致民眾財物損失或個資外洩。（圖片來源：截自民視新聞，https://youtu.be/vvNP8WPxlIY；LINE@ 生活圈，http://at-blog.line.me/tw/archives/75713444.html）

酪乳會中毒」等，另 107 年 9 合 1 大選之前，LINE 更成為攻擊各候選人的大平台，常有人轉傳「韓國瑜造勢現場發走路工 1,500 元」、「陳其邁辯論會帶耳機」等攻訐候選人不實訊息。

LINE 潛藏風險

總結上述各項議題，我們得知 LINE 本身存在許多資安風險，可約略將之分為「操作風險」及「軟體風險」，分述如下：

一、操作風險

1. 如前述案例所載，使用者於公務上可能同時與多群組人員聯繫，稍有不慎，易誤傳公務相關文件予不相干第三人，即使 LINE 具備「訊息回收」功能，也難得知第三人是否已知悉內容。

2. 許多人使用 LINE 未了解軟體具備之功能，像是 LINE 聊天室的「相簿」、「儲存至 Keep」功能等，可將檔案上傳雲端，若不善用而隨意儲存在手機目錄、相簿內，一旦手機誤植木馬軟體等，手上資料恐遭外洩。

3. LINE若設定不當，允許陌生人加為好友，讓有心人士有可趁之機，偽冒熟識、家人，誘騙點選連結進行 APT（Advanced Persistent Threat）攻擊或交付資料等，均可能引發資安風險。

4. 公務機關人員為求跨部會聯繫提升效率，往往建立許多群組，群組成員間彼此也未必熟識；又尚未在 LINE 群組裡指定管理者時，任何成員均可邀請他人進入該族群內；倘若誤加入非此公務相關人員，將滋生公務資料外洩疑慮。

二、軟體風險

1. LINE 可隨意轉貼及點選任何網址，若是該網址潛藏惡意代碼，手機極可能被植入惡意程式，導致機敏資訊遭竊。

2. LINE 建置雲端資料庫能儲存用戶或群組對話內容及檔案，但若 LINE 公司遭駭客入侵，即可能洩漏用戶或群組之檔案及對話內容，即使循司法調查管道，亦因 LINE 屬國外公司而增加偵辦難度；此外，使用者在通訊過程中亦存在遭 LINE 公司側錄對話內容之風險，故以國安角度考量，確實不宜在機敏公務上使用。

風險防制

一、安裝訊息加解密軟體

若 LINE 群組人員欲傳送公務資料，請務必安裝第三方加解密軟體，例如資通電腦與國家中山科學研究院研發之「ME 通訊

ME 通訊軟體介紹。（圖片來源：截自資通電腦網站，https://www.ares.com.tw/products/ncsist/?_ga=2.250067718.1418945601.1549964666-605880405.1549964666#ineme）

軟體」，透過該軟體對訊息、檔案加密後，再以 LINE 傳送，避免訊息誤傳或訊息遭他人擷取之資安疑慮。

二、「LINE」群組中建立管理人員

透過設定群組管理人，可統籌管理群組成員，必要時可將不適合人員踢出群組，以確保該群組談話內容不外流。

三、持續更新 LINE 版本

LINE 近年持續進行「資安漏洞回報獎金計畫」，用於挖掘軟體漏洞等各項缺失，並於後續版本中修補漏洞，故當 LINE 跳出新版本（電腦版）要求更新時，務必持續更新，避免遺留漏洞給駭客趁機攻擊。

四、安裝防毒軟體

由於 LINE 可傳送各項超連結網址、檔案、圖片等，甚至許多使用者亦安裝 LINE 電腦板，往往給駭客可趁之機，誘騙使用者下載檔案、開啟連結，最終再植入木馬程式。因此若加裝防毒軟體，就可讓防毒軟體進行初步篩選，降低中毒機會。

五、不隨便加好友、加官方帳號

不隨意加陌生人為好友，可點選 LINE「設定」中的「好友」設定，關閉「自動加入好友」、「允許被加入好友」功能，即可避免被色情業者、陌生人士誘騙。另網路上常常充斥各種假官方帳號，建議可利用「趨勢防詐達人」、「刑事局 165 APP」，先查證該帳號是否為「官方正版」後再加入。

LINE「好友」設定。

刑事局 165 反詐騙 APP 和趨勢防詐騙達人。（圖片來源：Google Play，https://play.google.com/store/apps/details?id=tw.gov.cib.app.fraud165&hl=zh_TW；趨勢科技防詐騙達人網站，https://www.getdr.com/）

假訊息防制

雖然坊間已有不少假訊息查證平台，像是 LINE 帳號「真的假的」、網站「MyGoPen」等，但迄今最方便、最受歡迎的查證管道，當屬「美玉姨」LINE 聊天機器人。使用者僅需將「美玉姨」加入聊天群組，即可以提問方式丟出訊息，讓「美玉姨」直接查證該訊息是否真實；惟「美玉姨」系採擷取使用者訊息並傳送至資料庫查詢運作方式，公務群組若加入「美玉姨」恐有資料外洩之虞。

LINE「美玉姨」及謠言查證結果。

結論

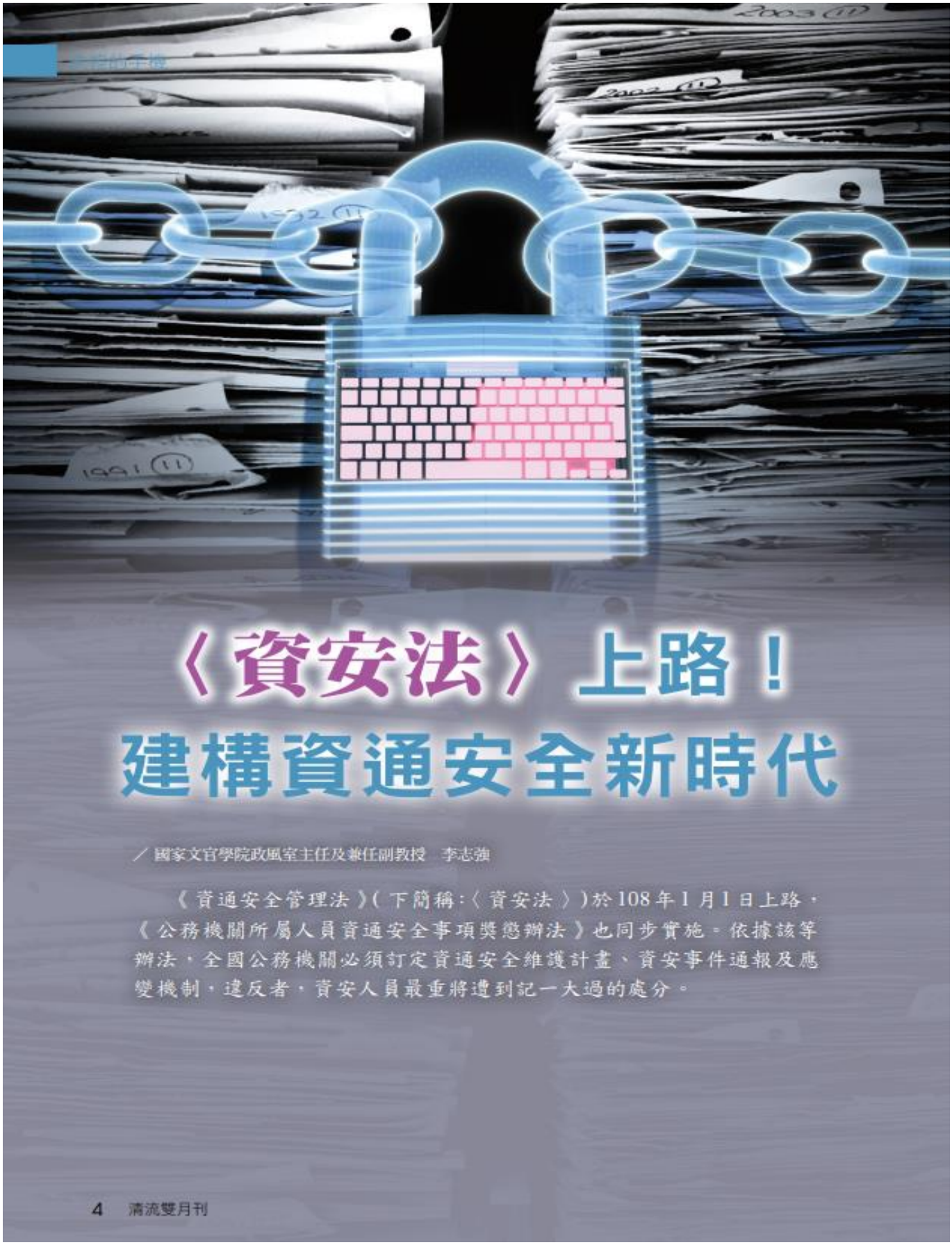
LINE 在臺灣儼然成為生活不可或缺的一部分，公務機關也常藉此開設公務群組，期以「行動辦公室」增進行政效率，然而在享受便利的同時，我們也要明白使用 LINE 所必須承擔的資安風險，盡可能不要在 LINE 上處理公務，倘仍須處理公務，務必考量 LINE 使用上的安全性。您可透過安裝加解密軟體、調整 LINE 操作等預防方式，在最低的風險下，方能享受 LINE 帶給我們的便利。

公務機關透過 LINE 增進行政效率的同時，務必考量 LINE 的安全性。圖為臺北市政府針對 LINE 之使用，所訂定的參考指引。（圖片來源：臺北市政府資訊局，https://doit.gov.taipei/News_Content.aspx?n=6CB3401DAD37F659&s=3284900CC421A8E1）

本文摘自清流雙月刊中華民國108年3月 號P10-P14

〈資安法〉上路！建構資通安全新時代

國家文官學院政風室主任及兼任副教授　李志強



〈資安法〉上路！
建構資通安全新時代

／國家文官學院政風室主任及兼任副教授　李志強

《資通安全管理法》（下簡稱：〈資安法〉）於108年1月1日上路，《公務機關所屬人員資通安全事項獎懲辦法》也同步實施。依據該等辦法，全國公務機關必須訂定資通安全維護計畫、資安事件通報及應變機制，違反者，資安人員最重將遭到記一大過的處分。

前言

當大家透過手機或電腦享受網路便利的同時，駭客也無時無刻伺機入侵，輕者個人資料外洩，重者公司商業機密遭竊，甚至有政府機關因而停擺，可見資訊安全已是刻不容緩之議題。

由於缺乏一套以風險管理為基礎，規範整體資通安全的專法，行政院參酌先進國家立法原則，並考量我國社經環境與法規制度，研訂〈資安法〉草案，於 107 年 6 月 6 日總統華總一義字第 10700060021 號令制定公布，行政院另於同年 11 月 21 日訂定發布《資通安全管理法施行細則》、《資通安全責任等級分級辦法》、《資通安全事件通報及應變辦法》、《特定非公務機關資通安全維護計畫實施情形稽核辦法》、《資通安全情資分享辦法》及《公務機關所屬人員資通安全事項獎懲辦法》等 6 種配套規定，且已自 108 年 1 月 1 日施行。

有鑑於各界面對上路不久的資安新法，一時恐難探究竟，故本文歸納分析之，期能提供各界參考遵行。

資通安全管理法架構

（108 年 1 月 1 日施行）

〈資安法〉相關重點

一、立法目的

為因應網際網路及其他資通科技快速發展與普及，〈資安法〉的立意即是加速建構完善的國家資通安全環境，以保障國家安全，維護社會公共利益，並建立以風險管理為核心的機制，要求規範對象於發生資安事件時，能立即通報並應處。另一目的則盼此帶動我國資安科技研發、資安服務、資安教育等產業發展。在此說明，法條中所稱「資通安全」，係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。而所謂「資通安全事件」，則指系統、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。

二、規範對象

〈資安法〉規範對象分為兩大類，其一是公務機關，係指依法行使公權力之中央、地方機關（構）或公法人，但不包括軍事機關及情報機關；另一對象則是特定非公務機關，此限於關鍵基礎設施提供者、公營事業及政府捐助之財團法人，並不及於一般民眾。前述所稱關鍵基礎設施，指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大

資安法規範對象包含公務機關與特定非公務機關，後者包含關鍵設施提供者、公營事業及政府捐助之財團法人，不及於一般民眾。（圖片來源：行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1280）

影響之虞者，例如電力、交通、金融、醫療、水資源、通訊傳播、緊急救援等系統或網路。

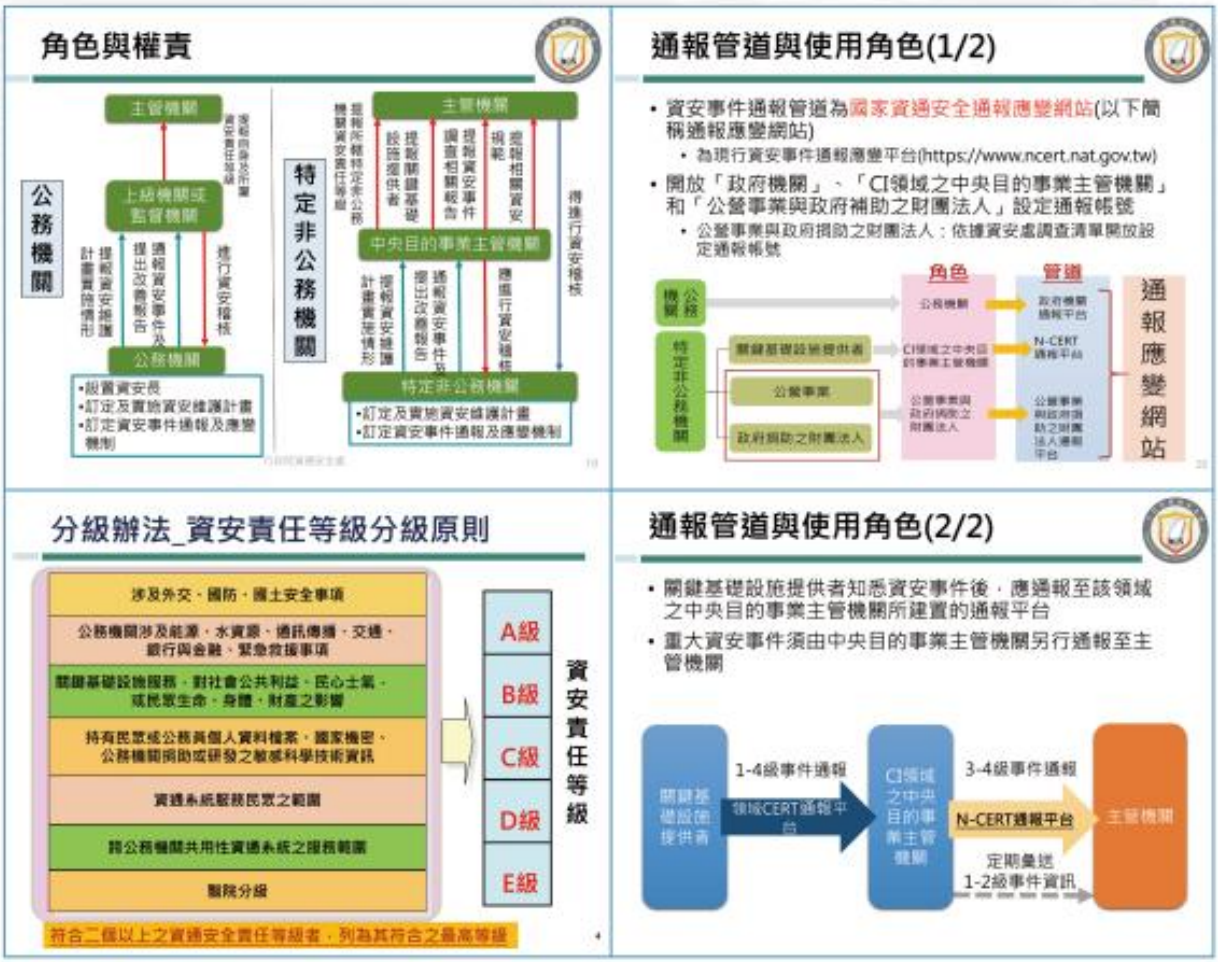
提醒注意者，依據〈資安法〉第 9 條規定，公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

三、應行義務

〈資安法〉乃就公務機關、特定非公務機關兩種規範對象分別訂定其相關義務。在公務機關資通安全管理部分，於本法第 10 至 15 條設有明文，重點有公務機關應符合其所屬資通安全責任等級之要求，並考量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，而《資通安全管理法施行細則》第 6 條則明確列舉資通安全維護計畫應包括之 13 點必要事項；由機關首長指派副首長或適當人員兼任資通安全長，負責推動及監督機關內資通安全相關事務設置；每年向上級或監督機關提出資通安全維護計畫實施情形；稽核其所屬或監督機關之資通安全維護計畫實施情形，受稽機關有缺失或待改善者，應將改善報告送交稽核機關及上級或監督機關，有關改善報告之內容，在《資通安全管理法施行細則》第 3 條明列 4 項必要事項；為因應資通安全事件，應訂定通報及應變機制，當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，另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；所屬人員對於機關之資通安全維護績效優良者，應予獎勵。

另在特定非公務機關資通安全管理部分，於本法第 16 至 18 條予以規範，重點首先是中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知；關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫，並向中央目的事業主管機關提出資



資安法分別就公務機關與特定非公務機關明文規定相關義務，並將資通安全責任等級劃分為 5 級，依據不同等級規範應辦事項。（圖片來源：行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1280）

通安全維護計畫實施情形，有缺失或待改善者亦應提出改善報告，而中央目的事業主管機關應辦理稽核；關鍵基礎設施提供者以外之特定非公務機關，比照前述規範訂定、修正及實施資通安全維護計畫，中央目的事業主管機關得要求其提出資通安全維護計畫實施情形，並得辦理稽核；特定非公務機關為因應資通安全事件，應訂定通報及應變機制，於知悉資通安全事件時，應向中央目的事業主管機關通報，並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。

此外，依據《資通安全責任等級分級辦法》，公務機關及特定非公務機關之資通安全責任等級，係根據業務所涉機敏程度及有無涉及關鍵基礎設施為判斷標準，並將資通安全責任等級由高至低，分為A、B、C、D、E等5級，且就不同等級在管理面、技術面、認知與訓練等面向，分別規範其應辦事項。

四、相關罰則

〈資安法〉第19條規定，公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。

第20條明文，特定非公務機關若未依本法訂定、修正或實施資通安全維護計畫；違反資通安全維護計畫法定必要事項；未向中央目的事業主管機關提出資通安全維護計畫之實施情形；未訂定資通安全事件之通報及應變機制，或違反法定必要事項；未向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告；違反有關通報內容之規定，有上述情形之一者，由中央目的事業主管機關令限期改正，屆期未改正者，按次處新臺幣（下同）10萬元以上100萬元以下罰鍰。

另為強化通報機制，第21條明定，特定非公務機關未通報資通安全事件，由中央目的事業主管機關處30萬元以上500萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

結語

由上可知，不論是公務機關或者特定非公務機關，均須界定資通安全責任等級及訂定資通安全維護計畫，方能依法推動資通管理，現雖定有相關法令可供遵循，然而法條內容錯綜複雜，若未瞭解法規、審慎訂定並落實執行，恐失立法美意。申言之，各機關首要之務即是釐清資通安全責任等級及核心業務，因兩者均攸關資通系統之後續安全管理，可說牽一髮而動全身。透過本文，希望協助公務機關及社會大眾認識這套資安專法，並共同為建構完善的國家資通安全環境攜手努力，以避免自身及國家權益遭駭。

本文摘自清流雙月刊中華民國108年3月 號P4-P9