教育部國教署｜115年度

校園資通安全專責人員知能研習

亞洲大學　陳偉嵩

研習導覽

從觀念到制度建立校園韌性

本次內容聚焦三條主線：資通安全基本概念及法規、個人資料保護，以及資訊安全管理系統 ISMS。

大綱

01

基本觀念

威脅趨勢、CIA 目標、風險管理與 NIST 框架。

02

相關法規

資通安全管理法、個資法及相關子法修正重點。

03

ISMS 建置

ISO 27001、PDCA、文件制度與建置流程。

第一章

資通安全基本觀念

先理解風險，才能選擇適切的防護

核心目標

資訊安全的核心要素：CIA 與法遵

C

機密性

確保只有授權人員才能存取資訊。

I

完整性

確保資訊不被未授權篡改或破壞。

A

可用性

確保授權使用者需要時能及時存取。

L

法律合規性

符合法律法規、標準與合約的各項安全要求。

防護技術

用技術守住 CIA

機密性保護

資料加解密、存取控制

完整性保護

雜湊函數、數位簽章

可用性保護

備份與備援、負載平衡

把資產、威脅與控制連起來

資產

需要保護的資料、系統與服務。

風險

威脅利用弱點造成影響的可能性。

控制

依風險高低採取適當控管措施。

NIST

網路安全框架的目的

降低營運關鍵基礎設施組織的網路安全風險，並以共同語言協助評估與改善。

NIST 框架核心

五大功能，形成完整循環

01

辨識 Identify

資產管理、企業環境、治理、風險評估、供應鏈風險管理。

02

保護 Protect

身分驗證、資料安全、訓練、流程、維護與防護技術。

03

偵測 Detect

異常與事件、持續安全監控、偵測流程。

04

回應 Respond

回應規劃、溝通、分析、減緩、改善與事件調查。

05

復原 Recover

復原規劃、改善建議與內外部溝通協調。

第二章

資通安全相關法規

權責清楚，管理才有一致的尺度

法規地圖

校園資安的制度基礎

資通安全管理法及八大子法

明定機關權責、監督、稽核、人力與產品管理。

個人資料保護法

規範個資蒐集、處理、利用與安全維護

其他法律

國家機密保護法、智慧財產相關法律

修法重點 01

明確機關權責及規管範圍

主管機關修正為數位發展部；配合財團法人法，修正特定非機關定義，並納管受政府控制且具資通安全重要性的事業。

規管範圍

特定財團法人如何認定?

政府捐助

財團法人法定義之政府捐助財團法人，捐助比例 50% 以上。

例：財團法人大學入學考試中心基金會(大考中心)、財團法人資訊工業策進會（資策會）

民間捐助

民間捐助財團法人，並由主管機關指定。

例：財團法人台灣網路資訊中心（TWNIC）、大型醫療財團法人

增納受政府控制的組織

新增納管銓敘部依公務人員退休資遣撫卹法公告之事業、團體或機構；如屬地方政府控制者，應經地方主管機關同意後核定。

銓敘部原則上按季公告受政府控制之事業、機構或團體清單。

修法重點 02

明訂委外事項完善監督機制

協力義務入法

政府機關應配合推動國家資通安全措施，決議事項由相關部門執行。

權限得以委託

整體防護、演練、稽核與國際合作等事務，得委託公務機關、法人或團體。

跨機關協調，提升法律位階

特定非公務機關業務涉及數個中央目的事業主管機關時，主管機關得協調指定單獨或共同辦理應辦事項。

修法重點 03

強化資安人力與查核

調度支援

重大事件時得調度各級機關資安人員支援，並視為在職訓練。

職能訓練

推動資安專職人員持續培訓，提升實務能力。

適任性查核

任用考試錄取人員及現職專職人員，得進行適任性查核。

適任性查核的實務效果

1

提出查核

主管機關或用人機關提出。

2

調查辦理

函請法務部調查局辦理。

3

結果認定

拒絕或未通過者不得辦理特定業務。

4

保障機密

避免接觸國家及國防秘密的風險。

特定非公務機關的責任

設置資安長

比照公務機關，設置資安長及資安專職人員。

獎勵績效

資通安全維護績效優良者，應予獎勵。

重大違規懲處

未依規定辦理且情節重大者，依機關規定懲處。

修法重點 04

擴大稽核範圍調整分層監督

針對無上級機關的公務機關，強化外部稽核機制，建立中央與地方的分層監督及事件通報應處架構。

稽核體系：中央與地方分層

數發部得稽核

中央府會五院；地方直轄市政府、縣（市）政府及議會。

地方政府應稽核

直轄市山地原住民區，以及鄉（鎮、市）公所與民代表會。

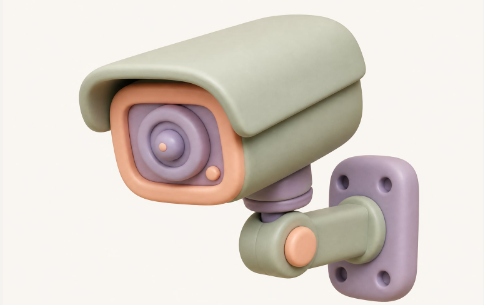
管理目標

實施情形審查、事件通報與應處。

修法重點 05

強化危害國家資安產品管理

原行政規則提升至法律位階。原則上不得下載、安裝或使用；若因業務需求且無替代方案，須敘明理由，經機關資安長及上級資安長逐級核可，函報數位發展部核定。



專案使用的三項管控

01

限定區域

指定特定區域及特定人員使用。

02

理由消失即停用

使用理由消失，應立即停止。

03

隔離使用

以不含個資及資料的單機，斷網或使用獨立網路。

04

列冊管理

專案購置後持續管理。

限制範圍：哪些組織納入？

公務機關

中央及地方機關（構）、公立學校、行政法人。

特定非公務機關

公營事業、關鍵基礎設施提供者、政府捐助財團法人。

受政府控制

受政府控制之事業法人或團體。

危害國家資安資通訊產品使用原則

Ø<ßÛþ

公務機關

原則上不得下載、安裝或使用危害國家資安產品；公務人員獲配的公務設備亦同。

特定非公務機關

維護資安必要時，中央目的事業主管機關得限制或禁止。因業務需求且無替代方案者，須經資安長核可並函報核定；管控措施由中央目的事業主管機關報主管機關備查。

法律適用架構

行政程序法於調查之適用要領

公務機關於進行行政調查時，應回歸《行政程序法》之規範核心

01

職權調查原則

依職權調查證據，不受當事人主張之拘束，全面釐清有利及不利事項。

02

證據保全蒐集

透過文書閱覽、聽取陳述及鑑定勘驗，確保證據取得之合法性與關聯性。

03

正當法律程序

落實告知義務與陳述意見機會，確保當事人於調查中之防禦權利。

04

事實認定處分

依據調查結果與心證，作成具備理由說明之行政決定或後續處置。

事件調查 • INCIDENT INVESTIGATION

特定非公務機關安全事件調查流程

01

調查機關

中央目的事業主管機關

02

調查時機

限於「重大」資安事件發生

03

受調查者

特定非公務機關(當事人)
受託之資訊廠商(關係人)

04

調查程序

通知到場陳述意見
通知提出獨立第三方機構出具之鑑識或調查報告
前往應受調查者之處所實施必要之檢查

政府資安實務做法

公務機關做法與執行框架

依據《資通安全管理法》，公務機關須建構「管理、技術、通報」三大維度的防護體系，以確保國家機敏資訊與關鍵系統之運作安全。

01

資安維護計畫落實

依機關責任分級(A-E級)訂定維護計畫，包含資產盤點、風險評估及管理流程。

02

技術防護與檢測機制

執行資安防護基準要求，落實弱點掃描、滲透測試及每年度對外資安稽核。

03

應變通報與職能培育

建立24小時通報處理機制，並確保人員每年完成法定資安職能教育時數。

實務執行指南

特定非公務機關之落實要點

維護計畫訂定

依據資安法規範，訂定並實施資通安全維護計畫，涵蓋資產盤點與風險評估。

事件通報應變

建立資安事件通報機制，於時限內完成通報，並執行損害控制與復原作業。

實施情形申報

每年向中央目的事業主管機關申報維護計畫實施情形，並配合外部稽核作業。

納管範圍與義務

特定非公務機關的法規配套與說明

特定非公務機關包含關鍵基礎設施提供者、公營事業及政府捐助之財團法人。依資安法規定，應訂定、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申報辦理情形，確保整體防護體系之完整性。

子法草案修正

特定非公務機關管理規範與責任

稽核機制強化

明確規範特定非公務機關資通安全維護計畫實施情形之稽核頻率與改善報告提報流程。

委外安全查核

受託辦理業務之廠商及人員，應納入妨害電腦使用罪章之適任性查核，降低供應鏈風險。

通報程序精進

修正資安事件通報與應變程序，確保關鍵基礎設施提供者在事故發生時能迅速應對。

第三章

個人資料保護

保護人格權，也促進合理利用

立法歷程與目的

歷程

99/5/26 公布

101/10/1 施行

104/12/30、112/05/31 修正

目的

規範個人資料蒐集、處理及利用，避免人格權受侵害，並促進合理利用。

什麼是個人資料?

屬性資料

姓名、生日、身分證字號等。

行為資料

健康檢查、犯罪前科等。

可識別資料

其他可直接或間接識別個人的資料。

個資處理的基本要求

- 當事人的個人資料自主權利，不得預先拋棄。
- 應基於特定目的蒐集、處理或利用。
- 明確告知蒐集目的、資料類別、使用範圍與來源。
- 保持資料正確；蒐集目的消失後，負刪除義務。

特種個人資料

類別 01

病歷

個人過去與現在的醫療診斷與診療過程資料。

類別 02

醫療

醫師對於病患進行診斷、處置或給藥之紀錄。

類別 03

基因

包含 DNA 片段等具有遺傳特性之生物特徵資訊。

類別 04

性生活

涉及個人性傾向、性行為或性取向之私密資料。

類別 05

健康檢查

包含理學檢查與各項生理數據之體格檢查報告。

類別 06

犯罪前科

由司法機關判定之刑事案件有罪紀錄及執行情形。

校園情境中的特種個資

除法律規定外，不得蒐集、處理或利用

> 學生健康檢查依《學校衛生法》第 8 條辦理
> 教職員工須提供警察刑事紀錄證明，涉及短期補習班不適任人員認定通報資訊的蒐集與查詢。

違反規範的法律風險

- 販售個資給不法集團：可能違反個資法第 19 條；意圖營利者依第 41 條可處 5 年以下有期徒

- 惡意程式攻擊公務機關：可能觸犯刑法妨害電腦使用罪，可處 3 年以下有期徒刑。
- 涉盜賣個資並收受賄賂：可能觸犯貪污罪，可處 5 年以上有期徒刑，得併科 3,000 萬元以下罰金。

個資法修法：裁罰與監督更明確

修法焦點	修法後方向
主管機關	由個人資料保護委員會整合目前分散權責。
裁罰	可直接處 2 萬至 200 萬元；情節重大可提高至 15 萬至 1,500 萬元。

個人資料安全維護措施

管理基礎

配置人員與資源、界定資料範圍、風險評估與管理。

日常控制

內部程序、人員管理、教育訓練、設備安全管理。

持續改善

稽核、軌跡保存、事故預防通報應變與持續改善。

教育部行政檢查

以年度計畫提升管理能力

各目的事業主管機關應每年擬定行政檢查計畫，落實非公務機關個資處理監管；私立專科以上學校及私立學術研究機構，依辦法建立安全維護計畫。

第四章

資訊安全管理系統 ISMS

把要求變成可執行、可稽核、可改善的制度

STANDARD UPDATE

ISO 27001:2022 版本重點

控制措施精簡與整合

附錄 A 控制措施從舊版的 114 項精簡為 93 項，並重新劃分為組織、人員、實體與技術四大領域。

新增 11 項安全控制

因應現代資安需求，新增威脅情資、雲端服務安全、資安監控與資料遮蔽等關鍵控制項。

導入「屬性」標籤管理

新增屬性 (Attributes) 概念，讓企業能依照控制類型、資安特性或營運功能進行彈性篩選與管理。

MANAGEMENT SYSTEM CYCLE

PDCA 管理循環機制

P：規劃 (Plan)

建立資安目標與流程，識別風險並擬定對應的控制措施與處理計畫。

D：實作 (Do)

落實管理制度，執行資安防護措施、人員教育訓練與日常維運作業。

C：檢查 (Check)

監控並衡量績效，透過內部稽核與管理審查，評估制度是否有效達成目標。

A：改善 (Act)

針對稽核發現的缺失執行矯正措施，並持續優化流程以提升整體資安水準。

ISMS 四階文件定義

一階：手冊

二階：程序

三階：標準

四階：紀錄

研習總結

從今天開始
讓資安成為日常

理解 CIA，遵循法規，落實 ISMS，持續改善校園防護。

謝謝聆聽