

教育部 115 年教育體系資安專業課程

校園資安與個資防護暨教育機構資訊作業委外安全(通識)

壹、課程介紹

面對各種可能的駭客攻擊，教育機構除了應積極提升校園資安與個資的防護，也需謹慎處理資訊作業委外的安全，強化校園的資安防護，減少遭受攻擊的威脅和系統弱點。

本次課程安排從資訊委外安全管理以及校園資安與個資防護等面向出發，幫助教育機構了解法規修正重點與方向，進而因應與強化現有的資安管控作為。課程介紹如下：

- 一、「政府資訊作業委外安全管理」專業分工的潮流帶動資訊作業委外比例的提升，藉由委外供應商的專業技能，組織得以在短時間內獲取更為穩定的資訊系統與服務，卻容易忽略其過程中帶來的資安風險。本課程將分析近期資訊委外作業發生的資安事件案例，並參照政府資訊作業委外服務參考原則，針對資訊委外不同階段的注意事項與要求，進行介紹及剖析，進而加強學員對資訊作業委外服務安全管理的掌握。
- 二、「校園資安與個資防護」隨著 114 年 9 月資通安全管理法及相關子法的陸續修正，無獨有偶，個人資料保護法即將迎來母法修正及新子法上路的動作，這代表資安與個資議題依舊是我國政府聚焦的重點。面對法規異動帶來的可能衝擊，各級教育機構必須積極瞭解及適應相關規範要求，期能有效降低發生資安與個資事件的風險。本課程將以近期公務機關常見資安事件為出發，並說明相關法規修正的方向與重點，分析後續應注意的校園防護重點項目，協助學員掌握法規內容和提升校園資安及個資保護，進而維護機關形象並保護教職員工生的個人權益。

貳、參加資格

- 一、資格：教育單位資訊或資安人員
- 二、人數：每場 130 人；名額有限，採優先報名順序參加，額滿為止。

參、課程資訊

二場課程相同實體與視訊同步進行，請擇一報名參加，如課程前需異動參加場次，均以候補登記。

場次	課程日期	實體課程名額	視訊課程名額
第一場	115 年 7 月 21 日(二) 上午 09:20 至 16:40	30 名	100 名
第二場	115 年 8 月 11 日(二) 上午 09:20 至 16:40	30 名	100 名

◆實體課程地點：國科會資安暨智慧科技研發大樓 5 樓-國網中心
(臺南市歸仁區歸仁十三路一段 6 號 5 樓)

◆視訊課程系統：Microsoft Teams 系統

肆、報名資訊

- 一、報名網址：<https://forms.cloud.microsoft/r/XG4AuHb8r4>
- 二、報名時間：7 月 7 日(二)上午 10:00 起至額滿截止。



指導單位



教育部

主辦單位



NCHC 國家實驗研究院

國家高速網路與計算中心
National Center for High-performance Computing

教育部 115 年教育體系資安專業課程
校園資安與個資防護暨教育機構資訊作業委外安全(通識)

伍、課程議程

時 間	課 程 內 容
09：10～09：30	實體報到 / 視訊連線報到
09：30～12：30	政府資訊作業委外安全管理 1. 資訊委外介紹 2. 資通安全管理法委外規範說明 3. 資訊委外各階段資安要求與注意事項
12：30～13：30	午餐休息及交流
13：30～16：30	校園資安與個資防護 1. 資安攻擊趨勢 2. 資安與個資法規修正方向與重點 3. 教育機構常見的資安與個資議題

陸、課程師資

鍾沛原 先生

柒、注意事項

- 一、依報名單位和姓名實際全程參與課程，並於課程結束後完成課程問卷和線上測驗，將提供課程時數共 6 小時。
- 二、講義/簡報電子檔，徵詢講師同意後提供，若涉及版權因素或機敏資料於課程結束後則不對外公開。
- 三、主辦單位保有最終修改、變更、活動解釋及取消本活動之權利，若有相關異動將另行通知。
- 四、課程聯繫 E-mail：asoc_support@niar.org.tw

捌、個資保護聲明

辦理「教育部 115 年教育體系資安專業課程」蒐集之個人資訊，僅於課程相關作業使用，非經當事人同意，不轉做其他用途，亦不會公佈任何資訊；如必填欄位提供資料不完整或不確實，將無法提供本次課程時數。

指導單位



教育部

主辦單位



NIEER 國家實驗研究院

國家高速網路與計算中心
National Center for High-performance Computing