國立台灣科技大學 114學年 第2學期　課程大綱

Spring 2026 NTUST Course Outline

授課教師：鄭欣明

Instructor:Shin-Ming Cheng

課程名稱：資通安全政策、法規與技術

Course Title：Cybersecurity Policy, Regulations, and Technology

2026/11/3

課程代號：CS3058701 Course Code	必選修：選修/半學年 Required/Electve:Elective/Half Yr.
學分數：3 Credits	先修課程： Prerequisites

節次教室：R4(TR-514) R5(TR-514) T5(TR-514)
Time/Location

專業核心能力：
Core Professional Competencies

具備數理與邏輯推演能力、具備發掘與解決問題能力、熟悉資訊專業基礎理論、具備產業實作應用與系統整合能力、增進溝通協調與團隊合作能力、具備外語閱讀能力與國際觀、理解科技趨勢與社會責任、具備專業倫理與人文素養

課程網址：
Course Website

課程宗旨：
Course Objectives

在當前資通安全威脅高度多元化、跨域化的時代，單一技術防禦已不足以支撐國家與企業的安全韌性。技術的有效運用，必須建構在政策與法規的可持續治理框架上。

本課程以「技術驅動的資安治理」為核心精神，兼顧理論、政策與實作。課程設計涵蓋三個層面：

1. 政策層（Governance Layer）：介紹我國《資通安全管理法》與國家資通安全發展方案，並與美國《National Cybersecurity Strategy》、歐盟《NIS2 Directive》對照，讓學生理解政策設計如何影響技術落實與防護標準。
2. 法規層（Regulatory Layer）：深入探討資安合規、漏洞通報、個資保護與供應鏈安全等制度如何映射到實際技術規範（如ISO 27001、NIST CSF 2.0、零信任架構）。
3. 技術層（Technical Layer）：以NIST CSF的五大功能（Identify、Protect、Detect、Respond、Recover）為主軸，結合實際案例與演算法探討，如資產識別演算法、入侵偵測模型、AI防禦技術、事件回應自動化（SOAR）與災後復原演練等。

此外，本課程特別強調AI技術在資安中的雙重角色：

- 一方面探討AI在威脅分析、異常偵測與決策支援中的應用（AI for Security）；
- 另一方面檢視AI本身的安全風險與治理挑戰（Security of AI），包括模型攻擊、資料中毒、AI RMF、與AI Act等議題。

最終目標是培養兼具系統開發思維與政策視野的資安人才，能夠設計「可被法規驗證、可被技術實現」的資安解決方案。

課程大綱：
Outline of Lectures

一：資安基礎與政策架構
1. 資通安全概念與威脅模型：資安需求分析、威脅建模（STRIDE、MITRE ATT&CK）、風險管理概論
2. 國家資安政策發展：我國國家資通安全發展方案與防護四階架構；NIST CSF 2.0 五大功能簡介
3. 全球資安戰略比較：美國National Cybersecurity Strategy與歐盟NIS2對照
二：法規與治理實務
4. 資通安全管理法架構與修法趨勢：資安法修法草案（2026版）解析、公私協力機制、主管機關職權
5. 資安子法與標準：施行細則、防護基準、應辦事項、稽核與通報制度
6. 國際法規比較：歐盟、日本、以色列、新加坡
三：資安技術框架與實作
7. 辨識（Identify）：資產管理與風險辨識之技術
8. 防護（Protect）：防護技術與零信任設計之技術
9. 偵測（Detect）：偵測技術與異常分析之技術
10. 回應（Respond）：事件回應與自動化之技術
11. 復原（Recover）：復原機制與災難復建之技術
四：AI 與新興技術之資安挑戰
12. AI導入的資安風險與治理：NIST AI RMF、EU AI Act、模型風險管理、資料外洩與偏誤
13. AI幫助資安的技術應用：LLM輔助防禦、攻防模擬、威脅偵測模型、藍隊自動化
14. AI本身的安全性：對抗樣本、模型中毒、Prompt Injection、資料洩漏防護
15. 期末專題

授課方式：
Method of Instruction

講授 Lecture：%

分組討論 Group discussion：%

案例研討 Case study：%

操做練習 Practical exercises：%

講授 Lecture：%

教科書：
Textbooks

參考書目：
References

修課須知：
Notice

評量方式：
Grading

備註說明：
Notes