

淡江大學 110 學年度第 2 學期課程教學計畫表

課程名稱	資訊安全概論	授課 教師	李鴻璋 LEE HUNG-CHANG
	INTRODUCTION TO INFORMATION SECURIT		
開課系級	資管三 P	開課 資料	實體課程 選修 單學期 2學分
	TLMXB3P		
課程與SDGs 關聯性	SDG4 優質教育		
系（ 所 ） 教 育 目 標			
一、精進資訊管理知能。 二、提升資訊科技專業。 三、獨立思考邏輯分析。 四、強化團隊合作能力。 五、重視企業資訊倫理。 六、培育全球化世界觀。			
本課程對應院、系(所)核心能力之項目與比重			
C. 資訊系統運用。(比重：50.00) G. 資訊系統分析、設計與整合。(比重：50.00)			
本課程對應校級基本素養之項目與比重			
2. 資訊運用。(比重：50.00) 5. 獨立思考。(比重：50.00)			
課程簡介	本課程介紹資通安全重要觀念與常用之安全技術。 資通安全重要觀念如資訊中心安全管理與實體安全，使用者身分鑑別，作業系統安全等 常用之安全技術如傳統秘密金鑰系統、現代公開金鑰系統、雜湊與亂數演算法、認證協定與系統與公鑰基礎架構等		

	This course introduces the essential concept of information security and technologies on Information/Network security. Information security concept includes information center management and physical security, user authentication, Operating Security, etc. Technologies on Information/Network security includes the traditional symmetric system, modern public key system, hashing function, and authentication protocols etc.
--	---

本課程教學目標與認知、情意、技能目標之對應

將課程教學目標分別對應「認知 (Cognitive)」、「情意 (Affective)」與「技能 (Psychomotor)」的各目標類型。

- 一、認知 (Cognitive)：著重在該科目的事實、概念、程序、後設認知等各類知識之學習。
- 二、情意 (Affective)：著重在該科目的興趣、倫理、態度、信念、價值觀等之學習。
- 三、技能 (Psychomotor)：著重在該科目的肢體動作或技術操作之學習。

序號	教學目標(中文)	教學目標(英文)
1	資訊安全威脅與架構	Information Security Threat and Framework
2	使用者身分鑑別	User Authentication
3	作業中系統安全	System Security in Operating processing
4	秘密金鑰系統	Secret Key Cryptosystem
5	認證協定與系統與公鑰基礎架構	authentication protocols and PKI
6	電子商務與資料庫安全	Electronic Commerce security and Database security

教學目標之目標類型、核心能力、基本素養教學方法與評量方式

序號	目標類型	院、系(所) 核心能力	校級 基本素養	教學方法	評量方式
1	技能	C	2	講述、實作	作業
2	認知	G	5	講述、討論	作業、討論(含課堂、線上)
3	情意	C	2	講述、討論	作業、討論(含課堂、線上)
4	情意	CG	25	講述、討論	作業、討論(含課堂、線上)
5	情意	C	25	講述、討論	作業、討論(含課堂、線上)、報告(含口頭、書面)
6	技能	CG	25	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)

授課進度表

週次	日期起訖	內容 (Subject/Topics)	備註

1	111/02/21~ 111/02/25	課程簡介與資通安全概論	
2	111/02/28~ 111/03/04	資訊安全技術-傳統秘密金鑰系統-DES	
3	111/03/07~ 111/03/11	資訊安全技術-3DES, RC5	
4	111/03/14~ 111/03/18	資訊安全技術-AES	
5	111/03/21~ 111/03/25	資訊安全技術-AES operation mode	
6	111/03/28~ 111/04/01	離散數論基礎	
7	111/04/04~ 111/04/08	現代公開金鑰系統-RSA	
8	111/04/11~ 111/04/15	現代公開金鑰系統-ElGaMal, DSS	
9	111/04/18~ 111/04/22	現代公開金鑰系統-ECC	
10	111/04/25~ 111/04/29	期中考試週	
11	111/05/02~ 111/05/06	資訊安全管理專題與報告1	
12	111/05/09~ 111/05/13	資訊安全管理專題與報告2	
13	111/05/16~ 111/05/20	資訊安全管理專題與報告3	
14	111/05/23~ 111/05/27	資訊安全管理專題與報告4	
15	111/05/30~ 111/06/03	資訊安全管理專題與報告5	
16	111/06/06~ 111/06/10	資訊安全管理專題與報告6	
17	111/06/13~ 111/06/17	資訊安全管理專題與報告7	
18	111/06/20~ 111/06/24	期末考試週	
修課應 注意事項		堅持才會成功。基本要點是不遲到及不缺席。	
教學設備		電腦、投影機、其它(專題報告與分享)	
教科書與 教材		1. 講義集成冊 (必備) 2. 資訊與網路安全概論 黃明祥、林詠章著 高立圖書 3. 資訊安全概論與實務(第三版) 潘天佑 碁峰書局 4. 資訊安全管理認證實戰寶典(第二版) 林文恭等 碁峰書局 5. 資訊安全 Merkow&Breithaut 柳望君譯 滄海書局	
參考文獻		1. 資訊與網路安全技術 粘添壽、吳順欲著 旗標出版 2. 近代密碼學及其應用 賴溪松等編著 松崗書局	

批改作業 篇數	3 篇（本欄位僅適用於所授課程需批改作業之課程教師填寫）
學期成績 計算方式	◆出席率： 10.0 % ◆平時評量：10.0 % ◆期中評量：30.0 % ◆期末評量：30.0 % ◆其他〈專題資安報告〉：20.0 %
備 考	「教學計畫表管理系統」網址： https://info.ais.tku.edu.tw/csp 或由教務處 首頁→教務資訊「教學計畫表管理系統」進入。 ※不法影印是違法的行為。請使用正版教科書，勿不法影印他人著作，以免觸法。