Study Plan and Course Descriptions of Master of Science (MSc) in Cybersecurity Engineering – MCSE

Ref: UC/ P 770/2025

As approved by University Council Decision No. UC/2584/11/2024-25 of meeting No. UC/11/2024-25 held on Tuesday the 15th of July 2025.

This Study Plan supersedes the previous version of the MCSE study plan, as outlined in the document approved by the University Council under reference number UC/P 668/2023, and will take effect upon approval by the Higher Education Commission (HEC) for the commencement of admissions to the programme.

M.Sc. in Cybersecurity Engineering
Program Structure

FOUNDATION COURSES

Course	Code	Course Title	Lec	Lab	Cre	Pre-Requisites
ITFN	500	Object Oriented Programming	3	0	3	
ITFN	502	System Architecture	3	0	3	

CORE COURSES(18 Credits)

Course	Code	Course Title	Lec	Lab	Cre	Pre-Requisites
ITCY	511	Cryptographic and Authentication Techniques	2	2	3	
ITCY	512	Cybersecurity architecture and design	3	0	3	
ITCS	527	Advanced Networking	3	0	3	
ITCY	522	Security Management	3	0	3	
ITCY	521	Software Security and Testing	2	2	3	
ITCS	550	Research Methods & Modeling	3	0	3	Completion of at least 9 credits

ELECTIVE COURSES (6 Credits: two courses to chosen from the following list of elective courses)

Course	Code	Course Title	Lec	Lab	Cre	Pre-Requisites
ITCS	539	Digital Forensics	3	0	3	
ITCS	509	Artificial Intelligence	3	0	3	
ITCS	526	Cloud Computing	3	0	3	
ITCY	526	Ethical Hacking	3	0	3	
ITCY	531	Malware Analysis and Engineering	3	0	3	ITCY512
ITCY	549	Selected Topics in Cyber Security	3	0	3	

DISSERTATION

Course	Code	Course Title	Lec	Lab	Cre	Pre-Requisites
ITCY	599	Dissertation in Cybersecurity Engineering	0	24	12	ITCS 550
	A student can register in the dissertation course ITCY 599 if the following conditions are satisfied: the student (1) completed successfully at least 21 credit hours including ITCS 550 - Research Methods & Modeling, (2) received a grade of B or more in ITCS 550, and (3) attained a CGPA of at least 3.0.					

Course Descriptions

ITCY 511	This course provides modern cryptographic and authentication techniques and covers essential concepts of cryptographic standards that users need to understand to achieve intended cybersecurity goals. This course also introduces the mathematical principles required for encryption/decryption, and public-key schemes. Students will be able to learn code-breaking techniques, awareness on hacking, and the design of cryptographic and authentication protocols. Students will gain practical skills through hands-on exercises and case studies, learning to implement and evaluate various cryptography and authentication mechanisms and digital signature algorithms.
ITCY 512	Cybersecurity Architecture and Design is a comprehensive course that delves into the critical aspects of designing and implementing secure IT systems. Students will demonstrate a detailed understanding of the principles of cybersecurity, apply principles and concepts to identify vulnerabilities in system architecture, and develop strategies to mitigate potential threats. This course explores the latest trends and challenges in the field, providing students with the skills needed to design robust security architectures and stay ahead in the rapidly evolving cybersecurity landscape. Students will engage with case studies, conduct research, and participate in projects that simulate real-world scenarios.
ITCY 520	The course is designed to provide advanced knowledge and professional-level skills in the areas of database management systems (DBMS) with a particular focus on database security. The course explores core and specialized theories, principles, and practices involved in the design, implementation, and management of complex database systems with a strong emphasis on security considerations. The course also studies critical security considerations, including database confidentiality, integrity, availability, access control, auditing, and reliability. Students will engage with contemporary challenges and cutting-edge solutions in enterprise database environments, applying both standard and specialised research methods.
ITCY 521	This course provides a comprehensive and critical study of software security and testing practices. It equips students with specialized theoretical and applied knowledge to address complex security challenges in modern software development. Students will engage with both static and dynamic security analysis, penetration testing, and secure coding practices. Emphasis is placed on critical thinking, creativity, and professional responsibility through problem-solving and project-based learning.
ITCY522	This course provides in-depth analysis in the development and management of information security systems. It equips students with the skills needed to assess and manage security risks across organizational and technical environments. The course covers key activities such as information systems asset valuation, threat and vulnerability assessment, cybersecurity risk management, incident response planning, and disaster recovery strategies. Students will be able to design and evaluate security solutions, recommend response strategies for incidents and breaches, and align security practices with organizational objectives and stakeholder requirements.
ITCY 526	The course provides an in-depth understanding of tools and techniques that are used by hackers and penetration testers and covers three main topics in general, namely Ethical Hacking, Website Hacking & Security and Mobile & Wireless Security. Students will be able to analyze and identify systems' vulnerabilities in order to design security measures to prevent cyber-attacks.
ITCY 527	The course aims to provide students with a comprehensive understanding of security challenges in mobile technologies. It covers the specialized concept of securing devices, applications, and networks while raising awareness about potential threats. This course also brings students up to date on developing technologies and covers encryption protocol and secure mobile application development, allowing them to effectively contribute to secure wireless and mobile networks.
ITCY 531	This course provides an in-depth understanding of malware, vulnerabilities and its workings, malicious analysis programs, and delving into engineering principles. Encourage discussion on malware core topics which include malware types, infection mechanisms, static and dynamic analysis, reverse engineering, malware forensics, cyber-attack response, software security and defensive strategies.
ITCY 549	This course explores specialized and emerging topics within the field of cyber security engineering. It focuses on specialized areas such as secure systems design, cryptographic methods, threat intelligence, and cutting-edge technologies for combating cyber threats. Students will engage with recent research and case studies to understand the challenges and innovations shaping the future of cyber-security.

ITCY 599	A structured supervised in-depth study on a pre-approved topic in the field of cyber security engineering can entail one of three methodologies: (1) a literature-focused study which aims to critically discuss the literature within a specified topic area; (2) a research focused study which aims to draw on practical data to assess critically a specified area or topic; or (3) a practical software development study which aims to explore an area or ideas, or demonstrate a concept through appropriate software development testing and critical analysis. The dissertation engages the student in a progressive course of intellectual discourse involving problem identification, methodology, research, evaluation and recommendation that culminates in the production of manuscript subject to public defense.