Study Scheme for Master of Information Security
(FullTime)

Course Code	Course Name	Credit Hour	Status
First Semester			
CCS5090	Research Methods in Computer Science	3(3+0)	Core (YW)
CCS5500	Security in Computing	3(3+0)	Core (YW)
CCS5207	Cyber Ethics and Law	3(3+0)	Core (YW)
CCS5505	Internet and Cloud Computing Security	3(3+0)	Core (YW)
CCS5508	Computer Forensics and Investigations	3(3+0)	Core (YW)
Total credits for First Semester Year 1		**15**	
Second Semester			
CCS5506	Information Security Management	3(3+0)	Core (YW)
CCS5503	Cryptography and Security Protocol	3(3+0)	Core (YW)
	Elective Course	3(3+0)	Elective (ELF)
	Elective Course	3(3+0)	Elective (ELF)
CCS5991	Project**	2(0+2)	Core (YW)
Total credits for Second Semester Year 1		**14**	
First Semester			
	Elective Course	3(3+0)	Elective (ELF)
CCS5991	Project	8(0+8)	Core (YW)
Total credits for First Semester Year 2		**11**	
	TOTAL CREDITS	**40**	

Note: **The Project Course (CCS5991) for 2 credit hours in year 1, second semester is for registration purposes only and does not count towards total credits and continues in year 2, first semester.

Study Scheme for Master of Information Security
(Part-Time)

YEAR 1					
First Semester			Second Semester		
Course Code	**Course Name**	**Credit Hour**	**Course Code**	**Course Name**	**Credit Hour**
CCS5207	Cyber Ethics and Law	3(3+0)	CCS5090	Research Methods in Computer Science	3(3+0)
CCS5508	Computer Forensics and Investigations	3(3+0)	CCS5506	Information Security Management	3(3+0)
CCS5500	Security in Computing	3(3+0)	CCS5503	Cryptography and Security Protocol	3(3+0)
				Elective	3(3+0)
Total credits for First Semester Year 1		**9**	**Total credits for Second Semester Year 1**		**12**
YEAR 2					
First Semester			**Second Semester**		
Course Code	**Course Name**	**Credit Hour**	**Course Code**	**Course Name**	**Credit Hour**
CCS5505	Internet and Cloud Computing Security	3(3+0)		Elective Course	3(3+0)
	Elective	3(3+0)	CCS5991	Project	8(0+8)
CCS5991	Project**	2(0+2)			
Total credits for First Semester Year 2		**8**	**Total credits for Second Semester Year 2**		**11**
TOTAL CREDIT					**40**

Note: ** The Project Course (CCS5991) for 2 credit hours in year 2, first semester is for registration purposes only and does not count towards total credits and continues in year 2, second semester.

List of Courses and Study Scheme Master of Information Security
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia

Core Course

No	Course Code	Course Name	Credit	Course Synopsis
1	CCS5090	Research Methods in Computer Science	3(3+0)	This course introduces students to the research methods in computer science and gives ideas on how to plan, organize and use the available resources efficiently in helping them in their research.
2	CCS5207	Cyber Ethics and Law	3(3+0)	This course provides students with comprehensive understanding of the legal, ethical, and societal issues surrounding cyberspace, enabling them to critically evaluate and navigate the complexities of the digital world with integrity and responsibility.
3	CCS5500	Security in Computing	3(3+0)	This course covers protection methods against various attacks on legitimate users, including necessary actions to track, document, and prevent the threats. Awareness on security threats and vulnerabilities as well as best practices in computer security are discussed.
4	CCS5506	Information Security Management	3(3+0)	This course covers the techniques being used in managing information security. A pragmatic approach that manages the entire information security process within a large organisation shall be introduced.
5	CCS5505	Internet and Cloud Computing Security	3(3+0)	This course covers advanced topics in cloud network security that emphasizes the network security practices and practical applications that have been adopted to ensure the security of the Internet and cloud is guaranteed. Secure design ensuring the confidentiality, integrity, and availability of digital assets in the face of evolving cyber threats are also discussed.

6	CCS5503	Cryptography and Security Protocol	3(3+0)	This course covers the concept of cryptography and its applications. Two categories of cryptography techniques, namely symmetric ciphers and public-key are discussed. Message authentication and appropriate cryptography techniques are used in constructing security protocol for application systems.
7	CCS5508	Computer Forensics and Investigations	3(3+0)	This course covers the principles of forensic evidence, criminal investigations, evidence collection and handling procedures that can be admissible in court. The search methods, documentations, forensic toolkits, acquisition and data analysis methods, data examination, evidence collection, fraud and forensic accounting, writing computer forensic reports, as well as legal, ethical and policies are also discussed.
8	CCS5991	Project	10(0+10)	The student will carry out a detailed study to evaluate the significant method and develop a research project related to information security under a supervision of a lecturer. Students will perform the study according to a suitable methodology for the project that will be implemented. A proposal report needs to be prepared at the beginning of the study. At the end of the project, the student will submit a complete project report for evaluation. The student will also be required to present the project in a seminar organised by the department.

Elective Course

No	Course Code	Course Name	Credit	Course Synopsis
1	CCS5502	Penetration Testing	3(3+0)	This course includes supporting theory in understanding the ways in which computer systems can be attacked and invaded by bypassing security or exploiting system vulnerabilities. Several principles and methods are used to ethically assess and evaluate computer security.
2	CCS5509	Trusted Computing	3(3+0)	This course covers the underlying mechanisms and technologies needed for trusted computing, which include hardware and trust models, attestation protocols such as Direct Anonymous Attestation and Single Sign-On to make authorization decisions. Some of the applications discussed include certificate management, conditional access for mobile recipients and peer-to-peer (P2P) networks in protecting the security and privacy of information providers and end users.
3	CCS5511	Software Security	3(3+0)	This course covers the common software security problems, their underlying causes, and solutions to the problems. Techniques to prevent and detect the software security level shall be discussed in this course.
4	CCS5512	Steganography and Digital Watermarking	3(3+0)	This course covers steganography and digital watermarking technics that can be adapted for information security problems in industry or specific domains. Emphasis on current trends and practices in the real world also discussed.
5	CCS5513	Public Key Cryptography	3(3+0)	This course covers cryptographic techniques and algorithms with their implementations in different situations. Limitations of cryptography will be identified before implementation of the cryptosystems.
6	CCS5514	Intrusion Detection System	3(3+0)	This course focuses on the concepts and issues related to intrusion detection system (IDS). IDS functions, detection approaches, analysis schemes and deployment of IDS are also discussed.

7	CCS5529	Cryptanalysis	3(3+0)	This course covers various techniques of cryptanalysis starting from cryptanalysis for classic ciphers, linear cryptanalysis, differential cryptanalysis and current cryptanalysis. Limitation of cryptanalysis will be identified before execution.
8	CCS5537	Blockchain Technology	3(3+0)	This course covers the concepts, technologies, and impacts of blockchain technology in society. The architecture, consensus, application and security of decentralized blockchain by maintaining transparency, anonymity, security, variability, and history in the open domain are also discussed.
9	CCS5800	Special Topic in Information Security	3(3+0)	This course focuses on selected issues and trends related to the field of information security. Exploration of key issues and new direction is conducted through analysis of critical issues and problems to recommend solutions.