MASTER OF CYBER SECURITY

PROGRAMME SPECIFICATIONS

The Master of Cyber Security is offered on a full-time basis. The full-time mode is offered only at the UTM main campus in Johor Bahru. The duration of study for the full-time programme is 3 semesters (1.5 years), subjected to the student's entry qualifications with total number of credits is 45.

This programme bridges the gap between those cyber security aspects with the real world requirements. The aim of this programme is to support the global need in producing professional, dedicated and ethical cyber security experts who will effectively plan, design, manage and practice reliable cyber security mechanisms and technologies. The programme is designed based on top cyber security professional certifications such as CISSP (Certified Information Systems Security Professional), CPT (Certified Penetration Tester), CSAP (Certified Secure Application Professional), CDSP (Certified Data Security Professional) and CHFI (Computer Hacking and Forensic Investigation).

General Information

1. Awarding Institution			**Universiti Teknologi Malaysia**	
2. Teaching Institution			Universiti Teknologi Malaysia	
3. Programme Name			Master of Cyber Security	
4. Final Award			Master of Cyber Security	
5. Programme Code			MECRA1AJA	
6. Professional or Statutory Body of Accreditation			Ministry of Higher Education	
7. Language(s) of Instruction			English	
8. Mode of Study (Conventional, distance learning, etc)			Conventional, Open Distance Learning (ODL).	
9. Mode of operation (Franchise, self-govern, etc)			Self-governing	
10. Study Scheme (Full Time/Part Time)			Full Time	
11. Study Duration			**Full Time** Minimum : 1.5 years Maximum : 4 years	
Type of Semester	**No. of Minimum Semesters**		**No. of Maximum Semesters**	
	Full Time	**Part Time**	**Full Time**	**Part Time**
Normal	3	-	8	-
Short	-	-	-	-

Course Classification

No.	Classification	Credit Hours	Percentage
i.	University Common Elective Course	3	6%
ii.	Core Faculty Course	3	6%
iii.	Core Courses	18	41%
iv.	Elective Courses	9	20%
v.	Project (1 and 2)	12	27%
	Total	**45**	**100%**
Total Credit Hours to Graduate		**45 credit hours**	

COURSE MENU

Additional Courses (for Non CS backgroud)	
MECR 0013	Cryptography
MECR 0023	Computer Security

University Common Elective Courses (Choose 1 Only)	
UECS 6013	IT Project Management
UHIS 6013	Philosophy of Science and Civilization
UHLM 6013	Malay Language for Post Graduates
UHMS 6013	Seminar on Global Development, Economic and Social Issues
UHMZ 6023	Malaysian Society and Culture
UBSS 6013	Organization Behavior and Development
UBSS 6023	Business Ethics, Responsibility and Sustainability
UHPS 6013	Dynamics of Leadership
URTS 6013	Environmental Ethics
UECS 6023	Introduction to Technopreneurship
UMJJ 6013	Basic Japanese Language and Culture
Core Faculty Course (Compulsory)	
MECR 1013	Research Methodology
Core Courses (Compulsory)	
MECR 1023	Information Security Governance and Risk Management
MECR 1033	Digital Forensics
MECR 1043	Cloud Computing Security
MECR 1053	Secure Software Engineering
MECR 1063	Cryptographic Engineering
MECR 1073	Penetration Testing
Elective Courses (Choose 3 only)	
MECR 2113	Business Continuity Planning
MECR 2123	Security Audit & Assessment
MECR 2213	Cyber Threat Intelligence
MECR 2223	Security Data Exploration
MECR 2233	Security Data Analytics & Visualization
MECR 2313	Software Exploitation
MECR 2323	Malware Analysis

Projects (Compulsory)	
MECR 2415	Project 1
MECR 2427	Project 2

Programme Structure (Full Time)

SYLLABUS	SEMESTER 1	SEMESTER 2	SEMESTER 3	TOTAL CREDITS
University Common Elective Courses		**(Choose 1)** U*** 6**3		**3**
Core Faculty Course	MECR 1013			**3**
Core Courses	MECR 1023 MECR 1033 MECR 1043 MECR 1053	MECR 1063 MECR 1073		**18**
Elective Courses		**(Choose 1)** MECR 2113 MECR 2123 MECR 2213 MECR 2223 MECR 2233 MECR 2313 MECR 2323	**(Choose 2)** MECR 2113 MECR 2123 MECR 2213 MECR 2223 MECR 2233 MECR 2313 MECR 2323	**9**
Project 1		MECR 2415		**5**
Project 2			MECR 2427	**7**
Total Credits	**15**	**17**	**13**	**45**

Programme Educational Objectives (PEO)

After having exposed to 3 to 5 years working experience, our graduates should become professionals who demonstrate the following competencies:

Code	Intended Educational Objectives
PEO1	Mastery of knowledge and competency in advanced areas of Cyber Security field.
PEO2	Practice professionalism and high standards of ethical conducts within organization and society.
PEO3	Responsive to changing situations by continuously acquiring new knowledge and skills.

Programme Learning Outcomes (PLO)
At the end of studies, students have the competencies to:

Code	Intended Learning Outcomes
PLO1	Synthesize complex information, specialized concepts, theories, methods and practice independently in the field of Cyber Security. (Knowledge and Understanding)
PLO2	Solve complex problems critically and integratively using systematic approaches. (Cognitive Skills)
PLO3	Apply practical skills to solve problems in the field of Cyber Security. (Practical Skills)
PLO4	Demonstrate effective collaboration with stakeholders professionally. (Interpersonal Skills)
PLO5	Communicate effectively the knowledge, skills and ideas using appropriate methods to peers, experts and communities. (Communications Skills)
PLO6	Use digital technologies and appropriate softwares competently to enhance study and practice. (Digital Skills)
PLO7	Evaluate numerical and graphical data critically using quantitative or qualitative tools in solving problems. (Numeracy Skills)
PLO8	Demonstrate leadership, autonomy and responsibility in managing resources. (Leadership, Autonomy and Responsibility)
PLO9	Engage self-advancement through continuous learning or professional development. (Personal Skills)
PLO10	Initiate entrepreneurial projects supported by relevant knowledge and skills. (Entrepreneurial Skills)
PLO11	Demonstrate respectable ethical conducts and professionalism skills in an organization and society. (Ethics and Professionalism Skills)

GRADUATION CHECKLIST
To graduate, students must pass all the stated courses in this checklist. It is the responsibility of the students to ensure that all courses are taken and passed. Students who do not complete any of the course are not allowed to graduate.

***Please attach a copy of results for previous semesters and a copy of registration slip for current semester.**				
Courses		**Credit**	**Grade**	**Pass**
Additional Courses (for Non CS backgroud)				
MECR 0013	Cryptography	3		
MECR 0023	Computer Security	3		
University Common Elective Courses (Choose 1 only)				

UECS 6013	IT Project Management	3		
UHIS 6013	Philosophy of Science and Civilization	3		
UHLM 6013	Malay Language for Post Graduates	3		
UHMS 6013	Seminar on Global Development, Economic and Social Issues	3		
UHMZ 6023	Malaysian Society and Culture	3		
UBSS 6013	Organization Behavior and Development	3		
UBSS 6023	Business Ethics, Responsibility and Sustainability	3		
UHPS 6013	Dynamics of Leadership	3		
URTS 6013	Environmental Ethics	3		
UECS 6023	Introduction to Technopreneurship	3		
UMJJ 6013	Basic Japanese Language and Culture	3		
Core Faculty Course (Compulsory)				
MECR 1013	Research Methodology	3		
Core Courses (Compulsory)				
MECR 1023	Information Security Governance and Risk Management	3		
MECR 1033	Digital Forensics	3		
MECR 1043	Cloud Computing Security	3		
MECR 1053	Secure Software Engineering	3		
MECR 1063	Cryptographic Engineering	3		
MECR 1073	Penetration Testing	3		
Elective Courses (Choose 3 only)				
MECR 2113	Business Continuity Planning	3		
MECR 2123	Security Audit & Assessment	3		
MECR 2213	Cyber Threat Intelligence	3		
MECR 2223	Security Data Exploration	3		
MECR 2233	Security Data Analytics & Visualization	3		
MECR 2313	Software Exploitation	3		
MECR 2323	Malware Analysis	3		
Projects (Compulsory)				
MECR 2415	Project 1	5		
MECR 2427	Project 2	7		
	TOTAL CREDITS:			

CAREER OPPORTUNITIES

Security Specialist/ Administrator/ Architect/ Analyst/ Auditor/ Director/ Consultant/ Engineer/ Manager; Cryptographer; Cryptanalyst; Chief Information Security Officer; Vulnerability Assessor; Incident Responder; Forensic Expert; Penetration Tester; Source Code Auditor.

COURSE SYNOPSIS

ADDITIONAL COURSES:

MECR 0013 Cryptography

Cryptography addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity. This course provides the background for the application and implementation of security mechanisms covered in the other courses. It deals with both theoretical and practical aspects of cryptography, to give an insight to the problems that arise in cryptography and the tools used to solve them. It introduces both symmetric key cipher system and public key cryptography, covering methods of obtaining the objectives of CIA (Confidentiality, Integrity and Availability).

MECR 0023 Computer Security

This course covers the body of knowledge on technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. The types of computer security that will be covered are application security, network security, internet security, data security, information security and end user security.

CORE FACULTY COURSE:

MECR 1013 Research Methodology

This course covers the fundamental steps and implementation on developing the initial ideas to formal academic writing accordingly. Students will be given the mechanisms on how to transform and digest the literature reviews that leads to the proposed research title. This course helps students to prepare the research proposal for Projects. The theoretical and practical aspects of implementing the proposal will be the milestone of this course.

CORE COURSES:

MECR 1023 Information Security Governance and Risk Management

The course is aimed at imparting knowledge and skill sets required to assume the overall responsibilities of administration and management of security of an information system. This course covers issues related to administration, management and governance of security of information systems. Topics include auditing and data management, risk management (risk identification, risk analysis, risk control), contingency planning, incident handling and risk governance. The course will study in detail principles and tools related to these topics. The course will also cover security standards, evaluation and certification process, security planning, ethical and legal issues in information and privacy.

MECR 1033 Digital Forensics

This course takes a detailed approach to the use of computers and computer technology in the investigation of incidents, both criminal and civil, in which computer technology play a significant or interesting role. Students completing this course will be familiar with the core computer science theory and practical skills necessary to perform elementary computer/digital forensic investigations, understand the role of technology in investigating

computer based crime, and be prepared to deal with investigative bodies at an elementary level.

MECR 1043 Cloud Computing Security

In this course, we are going to learn about common cloud misconfigurations, how to perform a risk assessment and verify compliance for various Cloud Services. Further, we will delve deeper into identifying security risks in these cloud services and to implement best practices to mitigate the common cloud misconfigurations. Other topics include topics of data ownership, privacy protections, data mobility, quality of service and service levels, bandwidth costs, data protection, and support.

MECR 1053 Secure Software Engineering

This course provides the principles of Secure Software Engineering and practical methods to secure requirements, design, implementation, testing, deployment and maintenance in software development. Students will also review policy specific requirements necessary to implement a secure development program within enterprise organizations. The students will also be able to understand software vulnerability, and how to evaluate, and address security risks to software.

MECR 1063 Cryptographic Engineering

This course is a continuation from the introductory cryptography. All networked computers and devices must have cryptographic layers implemented, and must be able to access to cryptographic functions in order to provide security features. In this context, efficient (in terms of time, area, and power consumption) hardware and software structures will have to be designed, implemented, and deployed. Discussion and analysis on how to resist cryptanalytic attacks by protecting access to primary (communication) and secondary (power, electromagnetic, acoustic) channels. Learn the algorithms, methods, and techniques in order to create latest cryptographic embedded software and hardware using common platforms and technologies. In addition to that, ethical issues in cryptography is discussed as well.

MECR 1073 Penetration Testing

This course will discuss issues pertaining to penetration testing which covers areas like finding vulnerabilities in various computer systems, exploiting them in an ethical manner. Emphasis is given on the fundamental theory and as well as hands on practice. Topics covered include information reconnaissance, web application pentesting, wireless pentesting, network pentesting, and current issues in pentesting.

ELECTIVE COURSES:

MECR 2113 Business Continuity Planning

The course is aimed at imparting knowledge and skill sets required to prepare to respond to a disaster and restore normal operations afterward. This subject covers issues related to administration and management of disaster recovery program. The important plan for disaster recovery includes the contingency plans: i) the Incident Response Planning (IRP), ii) Disaster Recovery Planning (DRP), iii) Business Impact Analysis (BIA) and iv) Business Continuity Planning (BCP). Topics include preparing to develop disaster recovery plan, assessing risk, prioritizing system and functions for recovery, developing plans and

procedure and organizational relationships in disaster recovery. The subject will study in detail principles and tools related to these topics. The subject will also cover procedures to response to attacks on computer, implementing disaster recovery plans, testing and rehearsal, assessment of needs, threats and solutions and living through a disaster.

MECR 2123 Security Audit & Assessment

The aim of this course is to provide students with knowledge of how security audits and assessment are being performed against company's information security system. Security audits are often used to determine regulatory compliance, in the wake of legislation (such as HIPAA, the Sarbanes-Oxley Act or etc.) that specifies how organizations must deal with information. The purpose is to evaluate, assess and measure how well the security conforms to a set of established criteria. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits. Most commonly the controls being audited can be categorized to technical, physical (e.g. system's physical configuration) and administrative (e.g. information handling processes and user practices). Also, auditing information security covers topics from auditing the physical security of data centers to auditing the logical security of databases and highlights key components to look for and different methods for auditing these areas.

MECR 2213 Cyber Threat Intelligence

With the rapid increase of cyber attacks, accurate security information is becoming more difficult to obtain. This course exposes the students to a complete cycle of CTI which includes hunting, behavioral patterns extraction, clustering and correlation, threat actor attribution until taking it down. Besides, it also explains the Cyber Kill Chain process in launching an attack. Understanding CKC is important in detecting cyberthreat. CTI will be explained in 3 different levels; strategic, tactical and operational.

MECR 2223 Security Data Exploration

This course is essential to help the CTI analyst to dissect data to find clues in detecting the cyberthreats. It covers techniques commonly used to explore and understand data obtained from various sources. Exploratory Data Analysis in general is an approach to analyzing data sets to summarize their main characteristics, usually visual methods are used. Primarily, data is explored to see what the data can tell us beyond the formal modeling or hypothesis testing task. It ranges from pre-processing techniques for detection, validation, error correction, and filling up of missing or incorrect data. Emphasis on finding the relationship among variables and Clustering to find patterns and associations among groups of data is also covered.

MECR 2233 Security Data Analytics & Visualization

This course consists of security analytics and visual analytics. Security analytics is an approach to cybersecurity focused on the analysis of data to produce proactive security measures. For example, monitored network traffic could be used to identify indicators of compromise before an actual threat occurs. Classification, regression and clustering we will be explored in analysing security data. Model evaluation is also covered. Data visualization is the only approach that scales to the ever changing threat landscape and infrastructure configurations. Using data visualization techniques, we can gain a far deeper understanding of what's happening on our network. We can uncover

hidden patterns of data, identify emerging vulnerabilities and attacks, and respond decisively with countermeasures that are far more likely to succeed than conventional methods. Visual analytics and its concept and design will be covered. Security data will be visualized using selected visualization tool.

MECR 2313 Software Exploitation

This course will discuss issues pertaining to software exploitation, finding vulnerabilities in various computer programs and exploiting them in an ethical manner. Topics covered include vulnerability discovery, stack overflow exploitation, format string exploitation, head overflow exploitation, shellcoding, and current issues in exploitation.

MECR 2323 Malware Analysis

This course will discuss issues pertaining to analysis of malicious software code. Emphasis is given on the fundamental theory and as well as hands on practice. Topics covered include static analysis, dynamic analysis, defensive mechanism of malware, and some topics on malware research.

PROJECTS:

MECR 2415 Project 1

This is the initial part of a 2-parts Master project that every student must fulfil successfully. Students are required to propose a suitable research topic under the supervision of a lecturer as a supervisor. Students must meet regularly with supervisor who will monitor their continuous progress. At the end of this course, students are required to prepare a report to be evaluated and present their proposal.

MECR 2427 Project 2

This is the second part of a 2-parts Master project that every student must fulfil successfully. Students are required to execute the next phases of their development plan in Project 1. Students are now required to code and integrate the different modules that make up the proposed project. Students will test the developed modules and the final fully-integrated the project following software development and research testing practices. Students must meet regularly with supervisor(s) who will monitor their continuous progress. Students are required to prepare a report to be evaluated and present their final work. The corrected report will be printed as a Master's thesis.

UNIVERSITY COMMON ELECTIVE COURSES:

UECS 6013 IT Project Management

This course presents a hands-on perspective to Information Technology project management. This course will assist post-graduate students to plan and implement their post-graduate projects as well as other IT projects effectively. The subject is organized into three main sections, that covers: i) Basic concepts, life cycle and framework of project management, iiI) Detailed description of each project management knowledge areas under the Project Management Institute (PMI) Body of Knowledge (PMBOK) and its applications, and iii) Real Project Initiation, Planning, Executing, Monitoring and Closing. The Project Management areas include – project integration, scope, time, cost, quality, human resource, communications, risks and procurement management. Students will also be utilizing latest

tools for understanding, reviewing, communicating and developing Business Model for a project. Teams of students are expected to perform real projects and achieve agreed Key Performance Indicators (KPI).

UHIS 6013 Philosophy of Science and Civilization

This course discusses the meaning and nature of the philosophy of science and civilization. It seeks first to explore the different denotation, connotation, and cognitive substance of philosophy, science, and civilization, as independent concepts. It then seeks to understand these terminologies individually in their historical perspectives and their relationship to each other. Understanding the meaning and import of culture is necessary to our understanding of civilization. The study of the nature and meaning of religion is therefore significant in our appreciation of culture and civilization. Historically, Islam and the Muslims have always been intricately connected to the Western world. Thus, the discussion also includes comparative studies of Islamic and western philosophy and universal values. The final discussion is about the contribution of Islam to the world's civilization, education, culture and scientific development.

UHLM 6013 Malay Language for Post Graduates

This course is offered to international students of the Masters and PhD programmes, from Indonesia, Brunei, Southern Thailand and Singapore. In this course students are given exposure on how to write scientific works (in Malay). The focus of this course is the spelling aspect, punctuation, sentence variety, language adjustment, paragraph writing and writing style. In addition, students will be exposed on writing formats such as literature writing, citations, bibliographies, abstracts and editing.

UHMS 6013 Seminar on Global Development, Economic and Social Issues

This course focuses on different approaches to economic development with reference to economic growth. Discussion on this course also includes issues related to globalization, technology and digital divides as well as the social crisis that has become a global concern. It aims in developing skills in understanding and analyzing global issues and recommending relevant solutions. Issues will be discussed in detail.

UHMZ 6023 Malaysian Society and Culture

This course is designed for international postgraduates. This course discusses on the various aspects of the Malaysian culture and society. Topics on belief system, religious festivals, customs and etiquettes of different ethnic groups in Malaysia will be introduced to the students. In addition, students will also been introduced to the Malay Language. At the end of the course students should be able to understand the cultures practiced among Malaysians and adapt themselves to these new cultures.

UHPS 6013 Dynamics of Leadership

This course is intended to encourage students discover and develop their personal leadership qualities. Students will be exposed to leadership theories so that they could develop an insight that leadership itself is a dynamic relationship based on mutual influence and common purpose between leaders and followers. Topics covered include Introduction to Leadership, Leadership Traits & Ethics, Leadership Behaviour and Motivation, Influencing: Power, Politics, Networking and Negotiation, Contingency Leadership Theories, Communication, Coaching, and Conflict Skills, The LeaderFollower Relationship, Team Leadership, Leading Self-Managed Teams, Transformational and Level 5 Leadership. Students will be evaluated based on their class leadership role, short talk and personal learning portfolios.

URTS 6013 Environmental Ethics

Environmental ethics is the discipline in philosophy that studies the moral relationship of human beings to, and also the value and moral status of, the environment and its nonhuman contents. It covers the challenge of environmental ethics to the anthropocentrism (i.e., human-centeredness) embedded in traditional western ethical thinking; the early development of the discipline in the 1960s and 1970s; the connection of deep ecology, feminist environmental ethics, and social ecology to politics; and the attempt to apply traditional ethical theories, and virtue ethics, to support contemporary environmental concerns. It focus on environmental literature on wilderness, and possible future developments of the discipline.

UMJJ 6013 Basic Japanese Language and Culture

At this course, students will be introduced to a simple yet useful familiar everyday expressions and very basic phrases using basic grammars to develop oral communication skills for social purposes. This course is suitable for beginners who wish to develop basic conversational skills in a short period. E-learning will be introduced and students must complete some Kana and communication courses within the time frame by self-learning. After this course, students are expected to speak common phrases in different situations and make simple conversation in Japanese language.

UECS 6023 Introduction to Technopreneurship

This course provides an overview of the basic concepts on entrepreneurship focusing on the nature, environment, and risks of new venture formation and building of businesses with IT in the Malaysian context. Students will learn on how to analyse and evaluate the business opportunities using knowledge and skills taught in this course and suggest innovative business ideas, business planning, self-assessment and operating strategies required to start a new small business. Students will also be exposed to current case studies of existing companies involved in the IT business. Active participation by students during class discussions and activities is encouraged & expected so that students can gain hands on experience with conducting research, develop, write, evaluate, presenting and defending segments of a business plan.

UBSS 6023 Business Ethics, Responsibility and Sustainability

Business plays a significant role in societal and environmental well-being. Private and public organizations are no longer responsible to shareholders and those inside the organizations, but to external parties including consumers, politicians, regulators, communities and ordinary citizens. To fulfil the conflicting needs of these stakeholders, business leaders and managers often encounter complex situations that require them to make difficult decisions whereby the lines between right and wrong are blurry. This course aims to provide students the fundamental knowledge about the role of organizations in a society and to develop their skills to sustainably manage organizations that integrate legal, ethical, economic, environmental, and social dimensions into their decision-making. The course intends to develop responsible managers who have high integrity, professionalism and interpersonal skills. The course will also teach strategies on how managers can promote responsible conducts in their companies. The course objectives will be achieved through various teaching and learning methods specifically through critical examination of case studies involving ethical issues and dilemmas on complex and controversial business problems. This course is integrative in nature built upon the understanding and reflection of the main disciplines covered in the core courses in the MBA program.

UBSS 6013 Organization Behavior and Development

This course helps students integrate behavioural science theories, tools, concepts, and techniques learned in the lab to an OB application in a "real" organization. Students are expected to conceptualize and apply Organization Behaviour three-level of analysis and synthesize it with the theory and practice of Planned Change for individuals, groups and organizations. Throughout the course, participants are exposed to the important topics central to behaviours of organization and its holistic process for development and change. Some of the topics include multiple views of organizations that influence organizational change, the evolution of organizational development and its challenges. The course also covers the nature of planned change, theories and types of change, the role of values and ethics in organizational change, and the concept of emergent change to enable participants to have an overall view of how available approaches to planned change management can be applied in organizational settings.