Cyber Security

Programme Information

2022.01, Approved

Overview

Programme Code	35574
Programme Title	Cyber Security
Awarding Institution	Liverpool John Moores University
Programme Type	Masters

Awards

Award Type	Award Description	Award Learning Outcomes
Target Award	Master of Science - MS	N/A
Alternative Exit	Postgraduate Diploma - PD	For the award of Postgraduate Diploma, in addition to the outcomes for Postgraduate Certificate, students will be capable of taking an innovative and informed position in relation to Cyber Security. Students will be capable of identifying and applying appropriate research methodologies as well as plan relevant research and/or development projects. Students will also be able to demonstrate creativity in critical analysis, reflection and contextual awareness in a wide range of topics associated with Cyber Security.

Alternate Award Names	

External Benchmarks

Subject Benchmark Statement	

Accreditation

Programme Accredited by

PSRB Name	Type of Accreditation	Valid From Date	Valid To Date	Additional notes
BCS, the Chartered Institute for IT	Accredited by BCS, the Chartered Institute for IT for the purposes of fully meeting the further learning academic requirement for registration as a Chartered IT Professional.			

Programme Offering(s)

Mode of Study, Mode of Delivery	Intake Month	Teaching Institution	Programme Length Programme Length Unit
Full-Time, Face to Face	September	LJMU Taught	1 Years

Aims and Outcomes

Educational Aims of the Programme	The overall aim of the programme is to provide people of graduate status working, or planning to work, in a computing environment with the opportunity to enhance their skills relating to cyber security in terms of research, analysis and practice, as well as to enhance career prospects or to become cyber security professionals by gaining additional knowledge and skills in the areas of cyber security. The specific aims of the programme are as follows: -To provide students with a fuller, systematic understanding of current and emerging cyber security threats, vulnerabilities and attacks. -To provide students with advanced practical skills for cyber defence, including secure software engineering and network defence. -To enable students to explore the issues surrounding information security management in industrial/enterprise contexts, including risk management, legal issues, ethics and privacy. -To facilitate students in the development of expertise in their interested topic areas of cyber security. -To encourage students to become advanced autonomous learners. -To provide students with a comprehensive understanding, critical awareness and ability to conduct evaluation of current and emerging cyber security research issues. -To further develop students' originality in applying analytical, creative, problem solving and research skills. -To provide advanced, conceptual understanding, underpinning career development, innovation and further study such as PhD.

Learning Outcomes

Code	Number	Description
PLO1	1	Critically apply current and emerging principles and practices of cyber security technologies.
PLO2	2	Perform original modelling, requirements analysis, design and implementation of secure software systems/applications.
PLO3	3	Engage with complex debates around ethical, legal, social and professional issues regarding information security.
PLO4	4	Deploy appropriate methods and tools creatively for the protection of a complex networked system.
PLO5	5	Specify, design and construct programs to be used for the purpose of information security.
PLO6	6	Analyse evidence data for an investigation.

PLO7	7	Evaluate investigation methodologies in terms of general attributes.
PLO8	8	Work professionally on complex problems as a part member of a team.
PLO9	9	Identify appropriate tools and techniques to be used for an investigation.
PLO10	10	Conduct research into Cyber Security and related topics.
PLO11	11	Use information technology, e.g. Web and internet, for effective information retrieval.
PLO12	12	Demonstrate deep conceptual and practical knowledge and skills in the areas of cyber security and its applications.
PLO13	13	Apply numerical skills to cases involving a quantitative dimension.
PLO14	14	Communicate effectively by written or verbal means.
PLO15	15	Plan and manage learning and development.
PLO16	16	Critically select a range of tools and techniques currently being used in the development of secure complex networked applications/systems.
PLO17	17	Critically analyse and developed a major piece of work in the area of cyber security.
PLO18	18	Have deployed complex tools to effectively and creatively manage the security of a networked computer system.
PLO19	19	Contribute to complex discussions around issues such as ethics, IT security law, and privacy.
PLO20	20	Comprehensively and critically review current research issues in the relevant aspects of cyber security technologies.
PLO21	21	Study independently at an advanced level and have developed effective methodology skills for original research.
PLO22	22	Demonstrate systematic and comprehensive knowledge of cyber security concepts, principles and theories.

Course Structure

Programme Structure Description	For an MSc award, students are required to attain 180 credits at Level 7. 120 credits from taught modules, and 60 credits from the project dissertation; For a PG Diploma award, 120 credits of taught modules at Level 7 are required; For a PG Certificate award, 60 credits of taught modules at Level 7 are required. 7101COMP Research Methods must be passed prior to the submission of the Project Dissertation (7136COMP Project Dissertation).

Programme Structure - 180 credit points	
Level 7 - 180 credit points	
Level 7 Core - 180 credit points	CORE
[MODULE] 7101COMP Research Methods Approved 2022.01 - 20 credit points	
[MODULE] 7131COMP Computer Security Approved 2022.01 - 20 credit points	
[MODULE] 7133COMP Network Security Approved 2022.01 - 20 credit points	
[MODULE] 7136COMP Project Dissertation Approved 2022.01 - 60 credit points	
[MODULE] 7139COMP Information Security Management Approved 2022.01 - 20 credit points	
[MODULE] 7141COMP Ethical Hacking Approved 2022.01 - 20 credit points	
[MODULE] 7142COMP Secure Systems Approved 2022.01 - 20 credit points	
Level 7 Optional - No credit points	OPTIONAL

Teaching, Learning and Assessment

Teaching, Learning and Assessment	Acquisition of 1 - 8 is through a combination of lectures, tutorials, practical sessions and laboratory work. Throughout the learner is encouraged to undertake independent reading both to supplement and consolidate what is being taught/learnt and to broaden their individual knowledge and understanding of the subject. Assessment methods are specified in module specifications. Each module is assessed by examination and/or coursework. Specifically the assessment takes the form of written examinations, laboratory work, coursework reports and presentations. Skills 9 - 12 are taught through lectures and developed through tutorial and lab work throughout the course. Cognitive skills are partly assessed via formal examinations, but mainly through coursework assessment. The Level 7 projects allow a student to demonstrate his/her cognitive skills. Practical skills 13-18 are developed throughout the programme. Coursework and projects are designed to provide practical opportunities for students to work independently and in groups. Specialist software is available in School labs or from specified PCs in the Learning Resource Centres. Assessment is normally by coursework and projects. Key skills 19-22 are developed throughout the programme in a variety of forms. Specifically through a combination of research related coursework, guided independent study and projects, examinations, group work and presentations. Key skills are assessed as part of coursework, projects, written examinations and presentations

Opportunities for work related learning

Opportunities for work related learning
Self-knowledge: Students reflect on their strengths and skills to select their project. With support of project supervisor; Project and time management skills, during Coursework, including groupwork and Project Dissertation; Oral presentation skills, in seminars and project presentation; Professional networking skills, during school research seminars; Coursework based on real-world industrial case studies/applications; Industrial guest speakers; Learning about Intellectual Property and Copyright, during Research Methods; Application of a wide range of ICT tools and techniques; Learning statistical tools for data analysis; Development of Interpersonal skills and knowledge of group dynamics, during group coursework and workshops.

Entry Requirements

Type	Description
Alternative qualifications considered	Applicants should normally have one of the following qualifications: Degree, in Computing or a related subject, or Degree equivalent professional qualifications, e.g. BCS Professional Graduate Diploma in IT Students with non-standard entry qualifications, relevant industry experience or certification are also encouraged to apply. Admission for these candidates will be at the discretion of the Programme Leader. Applicants with non-standard qualifications may be required to submit a CV and references.
Other international requirements	Where candidate's first degree was not taught and assessed in English, a minimum IELTS 6 is required (with a minimum of 5.5 on each component) or equivalent.

Programme Contacts

Programme Leader

Contact Name
Rubem Pereira

Link Tutor

Contact Name