

Module Specifications

Year/Level: 6
Programme: CyberSecurity

Module: Network Protocols and Architectures

Module Code: 6FTC2204

Credits: 15

Module Description:

Mandatory

This module aims to enable students to explore current and emerging network protocols and architectures. Additionally, this module aims to enable students to use appropriate tools to conduct networking experiments.

Module: Information Security Management

Module Code: 6FTC2203

Credits: 15

Module Description:

Optional

This module aims to enable students to explore advanced principles in information security from a management perspective. Additionally, this module aims to enable students to further develop knowledge of the fundamental principles underlying information risk and security management, and gain an understanding of theoretical and organisational aspects of information security management and operations.

Module: Cyber Security

Module Code: 6FTC2200

Credits: 15

Module Description:

Mandatory

This module aims to enable students to explore advanced principles in cyber security from a systems perspective. Provide a further grounding in the fundamental principles underlying cyber security. Introduce both theoretical and practical aspects of cyber security and operations.

Module: Cyber Security and Networks Project

Module Code: 6FTC2201

Credits: 30

Module Description:

Mandatory

This module aims to enable students to undertake a complex individual project answering a real-world, Cyber Security and Networks related problem. As part of this module, students will plan, undertake, and evaluate a practical solution or solutions to a cyber security and networks problem, designed to extend and deepen their knowledge in this specific area relevant to their studies.

Students will also plan, produce, and refine a significant technical report describing and reflecting upon the program of work undertaken to solve a real-world problem.

Module: Digital Forensics and Incident Respo

Module Code: 6FTC2202

Credits: 15

Module Description:

Mandatory

This module aims to enable students to detect how and when a security breach occurs against an information environment, be able to identify compromised systems and perform damage assessments to determine the impact of the breach as well as to contain and remediate it. The module will provide students with the skillset required to be part of an incident response team in a Computer Network Operations (CNO) environment.

Module: Software Architecture

Module Code: 6FTC2084

Credits: 15

Module Description:

Mandatory

This module aims to enable students to understand the different ways to structure large software systems and be able to design systems using common architectural patterns.

Module: Responsible Computing

Module Code: 6FTC2087

Credits: 15

Module Description:

Mandatory

This module aims to enable students to articulate the social, ethical, and legal issues and commercial risks together with the opportunities inherent in the use of computing technologies and the deployment of computer-based systems. Have a detailed awareness of the professional issues around current computing and Information Technology (IT) practice. Be able to produce outputs and documentation that demonstrate compliance with legal, ethical, and professional standards and principles of ethical design.

Module: Machine Learning and Neural Compu

Module Code: 6FTC2090

Credits: 15

Module Description:

Optional

This module aims to enable students to understand and apply machine learning techniques and neural networks to analyse both labelled and unlabelled data. Understand and use data visualisation techniques to further analyse data. Understand how computational models can capture some aspects of brain function.