Programme Regulations: 2021/22

Programme Title: Degree of Master of Science in Cyber Security - Code: 5144 F/P

Notes:

(i) *These programme regulations should be read in conjunction with the University's Taught Programme Regulations.*

(ii) *A compulsory module is a module which a student must take.*

(iii) *All modules are delivered in Linear mode unless stated otherwise as Block, eLearning or distance learning.*

(iv) *All optional modules are offered subject to the constraints of the timetable and to any restrictions on the number of students who may be taught on a particular module. Not all modules may be offered in all years and they are listed subject to availability.*

1. Programme structure

(a) The programme is available for study in both full-time and part-time modes.

(b) The period of study for full-time mode shall be 1 year starting in September. The period of study for part-time mode shall normally be 2 years starting in September.

(c) The programme comprises modules to a credit value of 180.

(d) All candidates shall take the following compulsory modules:

Code	*Descriptive title*	*Total Credits*	*Credits Sem 1*	*Credits Sem 2*	*Credits Sem 3*	*Level*	*Mode*	*Type*
CSC8102	System Security	10	10			7	Block	Core
CSC8202	Information Security and Trust	10	10			7	Block	Core
CSC8207	Security Analysis of Complex Systems	10		10		7	Block	Core
CSC8208	Research Methods and Group Project in Security and Resilience	20		20		7	Block	Core
CSC8209	Project and Dissertation in Cyber Security	60		20	40	7		Core
CSC8411	The Challenge of Dependable Systems	10	10			7	Block	Core
CSC8414	Security Tools and Analysis	20	20			7	Block	Core
CSC8415	Strategic Case Studies	20		10	10	7	Block	
CSC8611	Human-Artificial Intelligence (AI) Interaction & Futures	10		10		7	Block	
CSC8635	Machine Learning with Project	10	10			7	Block	

2. Assessment methods

Details of the assessment pattern for each module are explained in the module outline.

3. Other

This programme is designed to produce graduates who will be expected to be equally capable in theoretical and practical aspects of their subject and it is essential that only students of equally high calibre in both aspects of the programme are eligible for merit and distinction awards. Therefore the regulations are as follows:

Course Requirements

A number of areas in which specific regulations have been defined for this programme, and approved by the Faculty Learning, Teaching and Student Experience Committee, are documented below, and in these areas these provisions take precedence over other University regulations.

Progression within the MSc degree in Cyber Security

Three assessed components comprise the MSc degree in Cyber Security:

- Component 1: Six 10-credit modules, two 20 credits modules, in Semester 1 and 2
- Component 2: 60-credit individual project with dissertation module, in Semester 2 and 3
- Component 3: 20-credit module in Semester 2 and 3.

In order to be permitted to start Component 2 a candidate must

- obtain a weighted average mark for Component 1 of at least 50,
- and have failed no more than 20 credits,

and have not failed any core module.

Award of the MSc degree in Cyber Security

To obtain the MSc degree, candidates must satisfy the examiners in both assessed components as follows.

- A student will be recommended for the *award of MSc with Distinction* if they have achieved a pass mark in 180 credits with a weighted average mark across all 180 credits of at least 70 and have a Component 2 mark of at least 70.
- A student will be recommended for the *award of MSc with Merit* if they have achieved a pass mark in 180 credits with a weighted average mark across all 180 credits of at least 60 and have a Component 2 mark of at least 60.
- A student will be recommended for the *award of MSc* if they have achieved a pass mark in at least 160 credits with a weighted average mark across all 180 credits of at least 50.