MSc Network Security & Management (Part-Time) - IC501

1. Context and Objectives

Growth in the field of communication has been phenomenal over the last ten years. In this context, the MSc Network Security and Management programme has been designed to provide graduates with an adequate coverage of Computer Networks, Network Security, Cryptography, Computer Forensics, Cyber Laws and an in-depth knowledge to design and protect reliable network connectivity.

This programme has been developed in consultation with leading players in the ICT sector and is tailor made to the current needs of the industry. Graduates will have the necessary skills to develop and perform in this rapidly changing environment. The aim of this programme is to impart students with the necessary skills in network security solutions, secure digital services and secure infrastructures for computer systems.

Objectives

The objectives of the programme are to:

- Provide in-depth knowledge in Network Security and Management;
- Provide an understanding in Cyber Laws, Computer Forensics and Complex Cryptographic Algorithms;
- Provide skills to operate a secure infrastructure;
- Provide necessary background knowledge to pursue further studies in the field;

Competencies

After successful completion of this programme, graduates should be equipped with competencies to pursue a career in Network Security and Management;

2. Learning Outcomes:

Graduates of the MSc Network Security & Management programme should be able to:

- Apply the concepts of IoT, Enterprise Networking, Cryptography, Cloud Security, Computer Forensics and Cyber Law;
- Apply the acquired knowledge for writing research papers;
- Apply the acquired knowledge in a creative, innovative and critical manner;
- Contribute in the advancement of the field;

3. Teaching and Learning Methods

The MSc Network Security & Management programme consists of teaching contact hours, Self-Study and other learning activities. Teaching methods may include face-to-face lectures, online delivery, tutorials or practical sessions.

Other learning activities may comprise of the following:
- Working on assignments;
- Sitting for class test and preparation time for same;
- Sitting for examination and preparation time for same;
- Group work;
- Attending Workshops/Conferences recommended by the Department / Faculty;
- Fieldwork;
- Site Visits/Trips;
- Additional Practicals;
- Presentation among Peers;
- Experimental Learning;
- Guest Lectures;

4. Entry Requirements

(i) General

Successful completion of an undergraduate degree with at least a Second Class or 50%, whichever is applicable, or a GPA not less than 2.5 out of 4 or equivalent, from a recognised Higher Education Institution, or alternative qualifications acceptable to the University of Mauritius.

(ii) Programme Specific

For enrolment in this postgraduate programme applicants should possess an undergraduate degree in Computer Science, ICT or other related areas.

5. Programme Duration

The normal duration of the programme is as detailed below.

	Part Time (years)
Minimum	2
Maximum	4

6. Minimum LCCS Credits Required:

(i) Postgraduate Degree Award

For the Postgraduate degree award in MSc Network Security & Management, the student must obtain at least 72 LCCS credits including:

Modules	LCCS Credits
Minimum LCCS Credits for Core Modules	48
Final Year Project	24
TOTAL	**72**

(ii) Post Graduate Diploma Award

The Postgraduate Diploma is provided as a possible exit point in the programme. To be able to exit with a Postgraduate Diploma in Network Security & Management, a student must have attained 48 LCCS credits, and completing a minimum of 36 LCCS credits of taught modules. A student may also opt to complete a Postgraduate Diploma Project worth 12 LCCS credits to attain the 48 LCCS credits in lieu of 2 modules of level 2 to a maximum of 12 LCCS credits. The assessment of the Postgraduate Diploma Project will be based on project report, presentation and software/system demo. Written requests to exit with Postgraduate Diploma should be made to the Dean of Faculty.

(iii) LCCS Credits per Year

Students may register for a minimum of 12 and a maximum of 48 LCCS credits, per year.

7. Assessment and Deadlines

The assessment mode for each module will be based on one or a combination of the following:
- Examination
- Continuous Assessment
- Software Evaluation
- Portfolio evaluation

Students will be assessed by continuous assessment (CA) and/or formal examination for taught modules. The weight of the CA will be at least 40%, while examination may carry up to 60% of the total marks. The specific details and/or formula for the calculation of the final mark are provided in the Module Catalogue for each module.

Information regarding the classification of award and student grading is provided in the university regulations.

Students are required to register for modules which they intend to follow in a given semester on date(s) specified by the Faculty.

Submission deadlines for Project:

	Part Time
Start	January – Level 2
Submission	Last working day of August – Post Level 2

8. List of Modules

Module Code CORE	Module Name	L*/T*/P* Contact Hours/Week	Self-Study/ Week	Other Learning Hours/ Week	LCCS Credits
ICT 6001	Internet of Things	2+0+1	6	9	6
ICT 6002	Enterprise Networking	2+0+1	6	9	6
ICDT 6037	Research Methodology	2+1+0	6	9	6
ICT 6004	Cryptography	2+0+1	6	9	6
ICT 6005	Information Security Management	2+1+0	6	9	6
ICT 6006	Network & Cloud Security	2+0+1	6	9	6
ICT 6007	Computer Forensics	2+0+1	6	9	6
ICT 6008	Cyber Laws	2+1+0	6	9	6
ICT 6000	Project	-	6	9	24

Note: Contact Hours = L : Lectures+ T* : Tutorials+ P* : Practicals*

9. Programme Plan

Year 1 - Semester 1			
Module Code CORE	**Module Name**	**L*/T*/P* Contact Hours/Week**	**LCCS Credits**
ICT 6001	Internet of Things	2+0+1	6
ICT 6002	Enterprise Networking	2+0+1	6
ICDT 6037	Research Methodology	2+1+0	6
	SubTotal		**18**
Year 1 - Semester 2			
Module Code CORE	**Module Name**	**L*/T*/P* Contact Hours/Week**	**LCCS Credits**
ICT 6004	Cryptography	2+0+1	6
ICT 6005	Information Security Management	2+1+0	6
ICT 6006	Network & Cloud Security	2+0+1	6
	SubTotal		**18**
Year 2 - Semester 1			
Module Code CORE	**Module Name**	**L*/T*/P* Contact Hours/Week**	**LCCS Credits**
ICT 6007	Computer Forensics	2+0+1	6
ICT 6008	Cyber Laws	2+1+0	6
	SubTotal		**12**
Year 2 - Semester 1 & 2			
Module Code CORE	**Module Name**	**L*/T*/P* Contact Hours/Week**	**LCCS Credits**
ICT 6000	Project	-	24
	Sub Total		**24**
	Grand Total		**72**

25.07.19