UNIVERSITY of TECHNOLOGY, MAURITIUS

School of Innovative Technologies & Engineering

Department of Business Informatics & Software Engineering

MSc Enterprise Security & Digital Forensics

PROGRAMME DOCUMENT

Version 1.1
MESDF v1.1
Jan 2015

University of Technology, Mauritius
La Tour Koenig, Pointe aux Sables, Mauritius
Tel: (230) 207 5250 *Fax:* (230) 234 1747 *Email:* site@umail.utm.ac.mu
website: www.utm.ac.mu

A. Programme Information

MSc in Enterprise Security and Digital Forensics is the fore runner to the MSc in Computer Security and Forensics that provides specialised study for those students with an interest in areas such as enterprise security, security management, cryptography, digital forensics, controls, cloud frameworks, law/regulations, security technologies and audit areas.

Most postgraduate courses are based upon a broad range of modules. However, we recognise the desire for some students to specialise in specific areas in order to increase employment prospects in their area of interest.

The MSc in Enterprise Security and Digital Forensics is designed for candidates wishing to gain employment in enterprise security and digital forensics related areas such as with public and private security agencies, computer companies, local police forces and other government agencies etc.

B. Programme Aims

This Programme will provide both theory and practice and will enable students to gain the skills to develop a management security policy for organisations, design a secure wireless or wired computer network, manage a forensic case and understand and perform detailed technical analyses of computer-based evidence as well as many other aspects of computer and data security. It will further provide extensive understanding of security-based architectures as well as developing skill in the use of tools to test and evaluate such systems.

C. Programme Objectives

After successful completion of the Programme, the graduates should:

- display a mastery of the principal skill required for work in security & forensics dept
- have achieved broad understanding and knowledge, and have an interest in and appreciation of risk assessment, major security issues, policies, securing software, cloud concepts-security etc
- be logical and analytical, and possess skill in security, biometrics, high level forensics research and investigation
- become knowledgeable on core security focusing on predictions and or potential threats and analysis and core practice and actions that are required

D. General Entry Requirements

As per UTM'S Admission Regulations, and 'Admission to Programmes of Study at Master's Degree Level'

E. Programme Entry Requirements

At least an Honours Degree with significant Information security, Networking or IT content.

For instance, BSc (Hons) Degree in Science, Engineering, Security or other qualifications (academic or professional) acceptable to the University of Technology, Mauritius

F. Programme Mode and Duration

Full Time: 1 Year (2 semesters)
Part Time: 1½ Years (3 semesters)

G. Teaching and Learning Strategies

- Lectures, Tutorials and Practicals
- Class Tests and Assignments
- Industrial Project
- Workshops / Seminars / Lab Sessions
- Structured Discussions & Self Directed Study
- Case Study material & scenarios centred on real world problems

H. Student Support and Guidance

Lecturer and student interactions are encouraged. Students can contact their lecturers in person or through different communication tools.

I. Attendance Requirements

As per UTM's Regulations and Policy

J. Credit System

1 module = 3 or 4 credits
Industrial Project = 12 credits

K. Student Progress and Assessment

The programme is delivered mainly through lectures, tutorials, and practical laboratory sessions. Students are expected to be as autonomous and research oriented as possible and activities may include reading research papers, delivering presentations, taking part in quizzes, case-studying amongst others.

Each module carries 100 marks and unless otherwise specified, will be assessed as follows:

Written examination, inclusive of reading time, of duration of 2 - 3 hours for 3 credits modules and not less than 3 hours for 4 credits modules and continuous assessment carrying up to 40% of total marks. Continuous assessment can be based on a combination of assignments, field study, workshops and class tests.

Project on an Industrial placement
The students will undergo a six months project in collaboration with the industry. This project will be jointly supervised by an internal academic staff and an external representative from the industry local or overseas through UTM linkages

L. Evaluation and Performance

The percentage mark contributes a 100 percent weighting towards the degree classification.

Maximum marks attainable: 1100

Module grading structure:

Grade	Marks x (%)
A	$70 \leq x$
B	$60 \leq x < 70$
C	$50 \leq x < 60$
D	$40 \leq x < 50$
F	$x < 40$
A-D	Pass
F	Fail

M. Award Classification

Overall weighted mark x (%)	Classification
$70 \leq x$	MSc with Distinction
$60 \leq x < 70$	MSc with Merit
$40 \leq x < 60$	MSc
$x < 40$	No Award

Minimum Credits Required for Award of:

Master's Degree:	42
Postgraduate Diploma:	30
Postgraduate Certificate:	18

N. Programme Organisation & Management

Programme Director and Coordinator: Dr. Shireen Panchoo

Contact Details:

- Telephone Number: (+230) 207 52 50
- Email: s.panchoo@umail.utm.ac.mu

Part II - Programme Structure

O. MSc Enterprise Security & Digital Forensics – Full Time (Version 1.0)

Semester 1				Semester 2			
Code	**Modules**	**Hrs/Wk L + P/T**	**Credits**	**Code**	**Modules**	**Hrs/Wk L + P/T**	**Credits**
SECU5111C	Information Warfare & Security Management	2 + 2	4	SECU5114C	Secure Infrastructure Design	2 + 2	4
ISM5120C	Digital Forensics & Investigation	2 + 2	4	ISM5122C	Information Risks & Controls	2 + 2	4
SECU5115C	Enterprise Cloud Security Concepts & Frameworks	2 + 2	4	SECU5117C	Mobile & Wireless Network Security	2 + 2	4
SECU5116C	Standards & Security Technologies	2 + 1	3	ISM5121C	Cybercrime & Law	2 + 1	3
PROJ5202C	Industrial Project						12

P. MSc Enterprise Security & Digital Forensics – Part Time (Version 1.0)

Semester 1				Semester 2			
Code	**Modules**	**Hrs/Wk L + P / T**	**Credits**	**Code**	**Modules**	**Hrs/Wk L + P / T**	**Credits**
SECU5111C	Information Warfare & Security Management	2 + 2	4	SECU5115C	Enterprise Cloud Security Concepts & Frameworks	2 + 2	4
ISM5120C	Digital Forensics & Investigation	2 + 2	4	SECU5114C	Secure Infrastructure Design	2 + 2	4
SECU5116C	Standards & Security Technologies	2 + 1	3	ISM5122C	Information Risks & Controls	2 + 2	4
				PROJ5202C	Industrial Project		

Semester 3			
Code	**Modules**	**Hrs/Wk L + P**	**Credits**
SECU5117C	Mobile & Wireless Network Security	2 + 2	4
ISM5121C	Cybercrime & Law	2 + 1	3
PROJ5202C	Industrial Project		12

Q. MODULE OUTLINE

ISMS5121C: CYBERCRIME & LAW

- Introduction to law
- Basic liability for online activities
- E-commerce and the law of contracts
- Dematerialization of documents
- Legal restrictions on the movement and use of cryptographic technology
- Digital signature and electronic signature law
- International e-commerce and the law
- Discussion: revisiting issues in a multinational context, and electronic 'money'.
- Types of computer crime, history, surveys, statistics and global connections
- Legal Measures: Computer Misuse, Criminal Damage,
- Software Piracy, Forgery, Investigative Powers
- Network Crimes: Hacking methodologies via the Internet and attacks to other networks Investigations, Incident Handling and Forensic Examination
- The Future: The expansion of the Internet, pornography and other unsuitable material
- Identity Theft and Fraud
- Government control of security technology; regulation of CAs/TTPs; data privacy legislation, and taxation of e-commerce

ISM5120C: DIGITAL FORENSICS & INVESTIGATION

- Database Forensics
- Network Forensics
- Mobile Device Forensics
- Computer Forensics
- Investigative tools
- Digital Evidence
- Forensics Process
- Development of Forensic tools
- Forensic Standards
- Search & Seizure
- Network, Cloud, e-Discovery and Mobile Forensics
- Creating Forensic Ready Infrastructure
- Evidence Collection
- Using Network Intelligence

SECU5115C: ENTERPRISE CLOUD SECURITY CONCEPTS & FRAMEWORKS

- Vulnerabilities & Cloud Risks
- Enterprise Cloud v/s open cloud
- Core cloud computing technologies
- Essential Characteristics
- Core-Technology Vulnerabilities
- Essential Cloud Characteristic Vulnerabilities
- Defects in Known Security controls vs. cloud implementations
- Prevalent Vulnerabilities in State of the Art cloud offerings
- Cloud Software Infrastructure & Environments
- Cloud Service Models – SaaS, PaaS, IaaS
- Computational resources – storage, communication, cloud web applications, Services & APIs
- Management Access – Identity, Authentication, Authorisation
- NIST & ISO Standards
- Virtualisation & Cloud Security – Security Threats to evolving Data Centers
- Cloud/Grid Computing – Principles, distributed architectures
- Data Grid & Semantics Web

- Cloud Grid applications
- Auditing Mechanisms

ISM5122C: INFORMATION RISKS & CONTROLS

- Identify, assess and evaluate risk
- Enterprise risk management strategy
- Development and implementation of risk responses
- Risk factors and Events Addressing adapting to cost-effectiveness alignment to business objectives.
- Monitoring of risk and communicate information
- Managing stakeholders to ensure continued effectiveness
- Developing, Measuring and Monitoring of KRIs & KPIs
- Designing and implementation of information systems controls
- Governance, risk and compliance (GRC) tools
- Control practices related to business processes and initiatives
- Business process review tools and techniques
- Standards, frameworks
- Plan, supervise and conduct testing
- Maturity model to identify the gaps
- Control objectives, activities and metrics related to architecture (platforms, networks, application, databases and operating systems)

SECU5111C: INFORMATION WARFARE & SECURITY MANAGEMENT

- IW Doctrine and the Single Integrated Picture,
- Information Assurance
- Defensive Information Operations,
- Offensive Information Operations
- Computer Network Attack,
- IW Support: Research & Development,
- Operational Planning
- Principles of Information Security and its Management
- Internal Control, Audit and Security
- Information Security & Governance
- ISO 27001 – Information Security Management for Business benefits
- Role of Risk Analysis and Management in Effective InfoSec
- Building a World-class Information Security Architecture
- Security Management – Systems, Models and Frameworks
- Business Continuity – the Wider Context of Information Security

SECU5117C: MOBILE & WIRELESS NETWORK SECURITY

- Wireless & Mobile IP Architecture, Standards, Interoperability Developments
- Cryptographic Tools for Wireless Network security
- Security Architectures & Protocols in Wireless LANs
- Security Architectures & Protocols in 3G Mobile Networks
- IP Roaming
- Quality of Service
- Broadband Wireless Access
- Secure M-Commerce
  - WPKI
  - RPKI

SECU5114C: SECURE INFRASTUCTURE DESIGN

- IPv6 - Transition techniques from IPv4 to IPv6

- Internet security models: IPv4/IPv6
- WLAN Security Technology and Solutions
- Network Infrastructure Design
- Network Infrastructure for Virtualization
- Change Management Structure for a Network
- Network & Routing Topology
- Network Devices
- Internet Connectivity and Perimeter Networks
- Routing Communications
- Network Performance
- Network Security Design
- Security Plan
- Defense-in-Depth Model
- End-end security
- PKI : WPKI,MPKI
  - Algorithms: DES, RSA. Encapsulation. Encryption principles

SECU5116C: STANDARDS & SECURITY TECHNOLOGIES

- Security service &mechanism
- OSI communications architecture
- Security frameworks for key management
- Access control and authentication
- Encryption algorithms
- Computer and Network Architectures
- Platform and Operating System Security
- User Authentication Mechanisms
- Security Models and Access Control Mechanisms
- Malicious Code
- Introduction to Security Protocols
- Network Security Threats and Countermeasures
- Web Security
- Wireless (WLAN and GSM/UMTS) Security
- Authentication and key agreement
- Modern security evaluation criteria
- Common Criteria framework for security evaluation

PROJ5202: INDUSTRIAL PROJECT

Students will undergo a six months project in collaboration with the industry. An internal academic staff and an external representative from the industry local or overseas through UTM linkages will jointly supervise this project. The Project would include a project write up and presentation.