Master of Science (MSc) in Cyber Security

Programme Objectives

- A Master of Science in Cyber Security aims to equip students with the knowledge and skills necessary to protect information systems and networks.
- This programme provides a comprehensive understanding of various types of cyber threats, including malware, phishing, ransomware, and advanced persistent threats (APTs).
- This programme develops technical skills using relevant software tools in areas such as network security, cryptography, intrusion detection systems, and secure software development.
- Students are trained to identify, assess, and mitigate cybersecurity risks, thereby enabled to implement effective risk management strategies.
- This programme familiarizes students with relevant laws, regulations, and standards that govern information security practices.
- Programme equips students with the skills to respond to and recover from cyber incidents, including developing incident response plans and conducting forensic investigations.
- By completion of this programme the students will be enabled to design and implement secure system architectures, ensuring the confidentiality, integrity, and availability of information systems.
- Further this programme introduces the principles and techniques of ethical hacking to identify vulnerabilities and improve system security

Total Number of Credits: 270

Duration of the Programme: 2 Years

Entry Requirements for the Programme

- An undergraduate degree or equivalent from a recognised higher education institution or alternative qualifications acceptable to the Amity Institute of Higher Education.
- AIHE may also consider applications for mature students meeting its own strict Rules and Regulations taking the appropriate minimum basic qualification into account by adhering to the mature student's policy of AIHE.

Modules
Year: 1
Semester: 1
Module Code: IT491
Module Name: NETWORK SECURITY AND CRYPTOGRAPHY

Credits: 20
Module Brief:
This module equips students with advanced knowledge on cryptography, such as encryption, digital signatures and secure hashes. Module learning further empowers students to select appropriate techniques and apply them to solve a given security threat problem. Students could also design and evaluate security network protocols appropriate for a given situation. Students will bew able to demonstrate an understanding of the mathematical underpinning of cryptography. Further the module aims to develop skills in students to demonstrate an understanding of Network monitoring, implementing security measures and cryptographic techniques.

Year: 1
Semester: 1
Module Code: IT492
Module Name: INFORMATION SYSTEMS SECURITY
Credits: 20
Module Brief:
The objectives of the module equips students with skills and knowledge to develop Information security triad, to identify and understand the high-level concepts surrounding information security tools inorder to secure company digitally, master the system architecture and security design of a system. Students will learn to identify, analyze, and assess risks associated with information systems, including potential threats and vulnerabilities. Students will gain skills in identifying security incidents, responding to breaches, and implementing incident response plans. This module further aims to develop skills in students to different access control models and their application in protecting information systems. Topics such as business continuity and disaster recovery, legal regulations, investigations and compliance, risk management.

Year: 1
Semester: 1
Module Code: MGT412
Module Name: BUSINESS RESEARCH METHODS
Credits: 20
Module Brief:
The module will build the foundation for research. The students will learn to compare and contrast the new knowledge, farmulate and design research methodology to criticaly define the management problem and investigate the cause. Hence the student would become acquainted with the scientific research methodology and reporting in dynamic business domain. They would also become analytically skillful.

Year: 1
Semester: 2
Module Code: IT493
Module Name: INFORMATION RISKS AND CONTROL

Credits: 20
Module Brief:
This module learning will equip students with skills to identify and quantify risk at both the strategic and project levels, to develop and apply systems and tools for the management of risks, to develop and justify contingency and disaster recovery plans and apply an integrated risk management approach to project development and evaluation to further communicate the findings in a clear and coherent manner. Students learn to design. implement and monitor effective controls to mitigate identified risks, including technical, administrative, and physical controls. Moreover, students develop skills in creating and managing incident response plans to address information security breaches and minimize impact.

Year: 1
Semester: 2
Module Code: IT494
Module Name: DIGITAL FORENSICS & INVESTIGATION 1
Credits: 20
Module Brief:
This module equips students with skills to use Forensic methodologies to investigate , master different types of abuse of computer networks. Students get familiarized with commonly used forensic tools and software for data recovery, analysis, and reporting, understand privacy and security issues on computer networks, and the law as it applies to computer networks. The module provides a thorough explanation of how computers and networks function, how they can be involved in crimes, and how they can be used as a source of evidence. Students develop skills in implementing techniques for the proper collection, preservation, and documentation of digital evidence from various sources, such as computers, mobile devices, and networks. Module further aims to make students understand of the abuse of computer network's privacy and security issues on computer networks. Further, students are made aware of laws and legislations with regards to ICT in Mauritius. Students master the ways to manage forensic investigations, including documentation, reporting, and presenting findings to stakeholders. Students engage in practical exercises and labs to apply theoretical knowledge and develop skills in real-world forensic scenarios.

Year: 1
Semester: 2
Module Code: IT495
Module Name: ETHICAL HACKING & TOOLS
Credits: 20
Module Brief:
This module engages students in practical exercises and labs to apply theoretical knowledge and develop skills in setting up Hacking Lab using Kali Linux and virtual machines, create Trojans, viruses, keyloggers for Ethical Hacking. Students learn to explore the different types of hackers (white hat, black hat, gray hat) and various attack vectors, including social engineering, malware,

and network attacks. Students are equipped with practical knowledge and hands-on experience on essential ethical hacking tools and software used for reconnaissance, scanning, exploitation, and reporting (e.g., Nmap, Metasploit, Wireshark). Students learn to gain access to any type of machine: Windows/Linux/MacOS and crack Wireless Access Point passwords. This module promotes students to master SQL Injection, XSS, Command Injection, and engages students to learn how to bypass Firewalls & Intrusion Detection System with Advanced Scanning.

Year: 1
Semester: 3
Module Code: IT561
Module Name: INTRUSION DETECTION SYSTEMS
Credits: 20
Module Brief:

On learning this module, students can achieve advanced knowledge on different types of IDS, such as network-based IDS (NIDS) and host-based IDS (HIDS), and their specific functions, and can evaluate exterior and interior sensor placement effectiveness. Students are practically trained to use several IDS to monitor and secure security in organizations. This module learning motivates the students towards exploring various detection methodologies, including signature-based, anomaly-based, and hybrid detection techniques. Students understand the architecture of intrusion detection systems, including deployment models, components, and data flow. Module learning further aims to develop skills in students in configuring, managing, and maintaining IDS to ensure optimal performance and effectiveness. Students are trained on IDS integration with other security measures, such as firewalls, and SIEM systems. Students are engaged in practical labs to perform incident response process, including detection, containment, and remediation of security incidents. Students stay informed about emerging trends in intrusion detection, including the impact of machine learning and AI on detection capabilities. Students are further trained to use LOIC to performe DOS attack including Tear drop attack, Death of Ping, and securing data packet sniffers

Year: 1
Semester: 3
Module Code: IT561
Module Name: DIGITAL FORENSICS & INVESTIGATION 2
Credits: 20
Module Brief:

This module equips students with the specialized knowledge and skills necessary to conduct thorough and effective digital forensic investigations in advanced contexts. Through learning this module, students explore complex digital forensic methodologies for analyzing various types of data, including cloud environments, IoT devices, and mobile systems. Students perform file system analysis to examine different file systems (e.g., NTFS, EXT4) and recover deleted or hidden data. With regards to network forensics**,** students learn to analyze network traffic and log data to identify suspicious activities, including intrusion attempts and data exfiltration. Students

are trained to develop skills in dissecting and analyzing malware to understand its behavior, functionality, and potential impact on systems. Students are made to get familiarized with advanced incident response frameworks and methodologies, focusing on integrating forensic investigations into response plans. Students are informed about new developments in digital forensics, such as artificial intelligence, blockchain, and advanced encryption techniques.This module learning engages students in practical labs and simulations that allow students to apply advanced forensic techniques in realistic scenarios.

Year: 1
Semester: 3
Module Code: IT533
Module Name: CLOUD COMPUTING
Credits: 20
Module Brief:

This module aims to equip students with knowledge and training on various cloud platforms and technologies. Students develop an ability to design cloud patterns using use cases, design and Implement a Data Centre Architecture and Technologies, prepare a cloud strategy, and perform infrastructure security. Moreover, this module prepares students in knowing technical building blocks of IaaS thus enabling students to perform cloud capacity management. Students are trained to identify common cyber security threats and vulnerabilities associated with cloud computing, including data breaches, misconfigurations, and insider threats. This module further familiarizes students on cloud security frameworks and standards relevant to cloud computing, such as NIST, ISO 27001, and CSA Cloud Controls Matrix. Further students are engaged in practical labs to carry out Identity and Access Management (IAM) which includes cloud security, including authentication, authorization, and role-based access controls.

Year: 1
Semester: 4
Module Code: IT511
Module Name: MOBILE & WIRELESS NETWORK SECURITY
Credits: 20
Module Brief:
This module aims to equip students with skills to explore emerging wireless technologies, to identify associated security concerns, to investigate the various wireless LAN security standards and protocols including WEP, WPA and WPA2. On learning this module, students will be able to illustrate the concepts and provide practical insight by examining specific networking protocols and topologies related to mobile and wireless security. Students can elaborate on the security aspects of modern technologies including RFIDs, smart card technologies and public wireless hotspots, illustrate the security concepts related to M-Commerce and Mobile IP and Identify common security threats and vulnerabilities specific to mobile and wireless networks, such as eavesdropping, man-in-the-middle attacks, and rogue access points.

Year: 1
Semester: 4
Module Code: IT598
Module Name: CYBER OPERATIONS AND QUALITY MANAGEMENT
Credits: 20
Module Brief:

This module discusses the strategic role of Cyber operations management in organizations and engages students in examining ways to design operation systems to support the strategy of the organization and gain a competitive advantage in the marketplace. Details such as the importance of designing and managing effectively the organization's supply network are discussed in this module. This module engages the students in practical labs to examine the role and key decisions of the operations manager (forecasting demand, capacity management, inventory management, scheduling etc. Students are trained in managing effectively quality and performance in organizations and its implications. This module emphasizes the learning on assessment of roles of operations in an organization, formulation of suitable operations strategy to support the overall organization strategy, design an operations system to support a specific operation strategy, assessment on the key processes involved in operations planning and control and engages students to analyse an operation, identify its strengths and weaknesses and propose an improvement project to overcome its main weaknesses.