

MSc in Cybersecurity

Award Type: Master of Science (MSc)

Program Stream: Cybersecurity & Information Technology

Course Overview

The MSc in Cybersecurity is designed to develop advanced knowledge and skills in protecting digital systems, networks, and information assets from cyber threats. The program focuses on understanding security risks, threat intelligence, and defensive strategies within modern technological environments.

This program is ideal for professionals seeking careers in cybersecurity operations, information security management, risk analysis, and technology governance across public and private sector organizations.

Learning Outcomes

Upon completion of the program, students will be able to:

- Analyze cybersecurity threats, vulnerabilities, and risk landscapes
- Apply security principles to protect networks, systems, and data
- Design and evaluate cybersecurity risk management strategies
- Interpret cybersecurity policies, standards, and regulatory frameworks
- Support incident response planning and security decision-making

Course Content

Key areas covered in the MSc in Cybersecurity include:

- Cybersecurity Fundamentals and Threat Intelligence
- Network and Systems Security
- Information Assurance and Risk Management
- Cybersecurity Policies, Standards, and Compliance
- Incident Response and Business Continuity Planning
- Ethical, Legal, and Regulatory Issues in Cybersecurity
- Applied Cybersecurity Research

Credit Value

Total Credit Load: 60 credits

Progression & Application

Graduates are prepared for roles such as cybersecurity analysts, information security officers, risk and compliance specialists, and IT security consultants. The program also provides a strong foundation for doctoral study in cybersecurity or advanced professional certifications in information security and cyber risk management.

MSc in Information Technology Management

Award Type: Master of Science (MSc)

Program Stream: Cybersecurity & Information Technology

Course Overview

The MSc in Information Technology Management is designed to develop expertise in overseeing and optimizing IT operations within organizations. The program emphasizes strategic planning, IT governance, systems integration, and the application of technology to solve complex business challenges.

This program is ideal for professionals aiming for leadership roles in IT management, technology strategy, systems administration, and organizational digital transformation initiatives.

Learning Outcomes

Upon completion of the program, students will be able to:

- Manage IT operations and resources efficiently within an organizational context
- Develop IT governance frameworks and implement best practices
- Assess and integrate emerging technologies to meet business objectives
- Lead projects involving digital transformation and IT system implementation
- Ensure compliance with regulatory standards and data protection policies

Course Content

Key areas covered in the MSc in Information Technology Management include:

- IT Governance and Strategic Planning
- Enterprise Systems and Digital Transformation
- Project and Portfolio Management in IT
- IT Infrastructure and Cloud Management
- Data Management and Business Intelligence
- Cybersecurity Principles for IT Managers
- Applied Research in Information Technology Management

Credit Value

Total Credit Load: 60 credits

Progression & Application

Graduates are prepared for roles such as IT managers, systems analysts, technology consultants, and digital transformation specialists. The program also provides a foundation for doctoral study in IT management or professional certifications in IT governance, project management, and enterprise technology leadership.

MSc in Information Systems

Award Type: Master of Science (MSc)

Program Stream: Cybersecurity & Information Technology

Course Overview

The MSc in Information Systems is designed to equip students with advanced knowledge of designing, implementing, and managing information systems that support organizational goals. The program combines technical skills with strategic insights to optimize IT infrastructure and business processes.

This program is ideal for professionals seeking roles in systems analysis, IT strategy, business process management, and enterprise information solutions.

Learning Outcomes

Upon completion of the program, students will be able to:

- Design and implement robust information systems aligned with business objectives
- Analyze organizational processes to identify technology-driven improvements
- Manage databases, applications, and IT resources effectively
- Integrate emerging technologies to enhance operational efficiency
- Ensure information security, data integrity, and regulatory compliance

Course Content

Key areas covered in the MSc in Information Systems include:

- Information Systems Analysis and Design
- Database Management and Data Analytics
- Enterprise Architecture and Integration
- Business Process Modeling and Optimization
- Information Systems Security and Risk Management
- Emerging Technologies and Digital Innovation
- Applied Research in Information Systems

Credit Value

Total Credit Load: 60 credits

Progression & Application

Graduates are prepared for roles such as information systems managers, systems analysts, IT consultants, and enterprise technology specialists. The program also provides a strong foundation for doctoral study in information systems or professional certifications in data management, IT governance, and system design.

MSc in Network & Systems Security

Award Type: Master of Science (MSc)

Program Stream: Cybersecurity & Information Technology

Course Overview

The MSc in Network & Systems Security is designed to provide students with the skills and knowledge needed to secure and manage modern IT networks and systems. The program emphasizes threat detection, vulnerability management, and the implementation of robust security measures to protect organizational assets.

This program is ideal for professionals seeking careers in network security, cybersecurity operations, system administration, and IT infrastructure protection.

Learning Outcomes

Upon completion of the program, students will be able to:

- Design and maintain secure network architectures
- Identify, analyze, and mitigate cybersecurity threats and vulnerabilities
- Implement advanced security protocols and monitoring systems
- Develop and enforce organizational security policies and compliance measures
- Respond effectively to security incidents and breaches

Course Content

Key areas covered in the MSc in Network & Systems Security include:

- Network Architecture and Protocols
- Cybersecurity Fundamentals and Threat Intelligence
- Vulnerability Assessment and Penetration Testing
- System Hardening and Security Configuration
- Intrusion Detection and Incident Response
- Cryptography and Secure Communication
- Applied Research in Network Security

Credit Value

Total Credit Load: 60 credits

Progression & Application

Graduates are prepared for roles such as network security engineers, cybersecurity analysts, system administrators, and IT security consultants. The program also provides a foundation for advanced professional certifications in cybersecurity and network management, as well as pathways to doctoral study in information security.

MSc in Digital Infrastructure & Systems

Award Type: Master of Science (MSc)

Program Stream: Cybersecurity & Information Technology

Course Overview

The MSc in Digital Infrastructure & Systems focuses on designing, implementing, and managing robust digital infrastructures to support organizational operations. The program emphasizes cloud computing, network integration, and scalable IT systems that ensure high availability, performance, and security.

This program is ideal for professionals seeking roles in IT infrastructure management, cloud solutions, systems engineering, and enterprise technology administration.

Learning Outcomes

Upon completion of the program, students will be able to:

- Design and maintain scalable digital infrastructure solutions
- Implement cloud and virtualization technologies
- Manage enterprise networks and distributed systems effectively
- Monitor system performance and optimize IT resource utilization
- Ensure system reliability, security, and compliance with industry standards

Course Content

Key areas covered in the MSc in Digital Infrastructure & Systems include:

- Digital Infrastructure Architecture and Design
- Cloud Computing and Virtualization
- Enterprise Systems Integration
- Network Management and Security
- IT Resource Optimization and Performance Monitoring
- Disaster Recovery and Business Continuity
- Applied Research in Digital Systems

Credit Value

Total Credit Load: 60 credits

Progression & Application

Graduates are prepared for roles such as IT infrastructure managers, systems engineers, cloud architects, and enterprise systems administrators. The program also provides a foundation for advanced professional certifications in cloud computing, systems management, and network administration, as well as pathways to doctoral study in IT systems and infrastructure.

Postgraduate Diploma in Cybersecurity

Award Type: Postgraduate Diploma (PGD)

Program Stream: Cybersecurity & Information Technology

Course Overview

The Postgraduate Diploma in Cybersecurity provides students with practical and theoretical knowledge required to protect digital assets and manage security risks in organizational environments. The program emphasizes hands-on experience with threat detection, vulnerability management, and cybersecurity policy implementation.

This program is ideal for professionals aiming to build a career in cybersecurity operations, IT security management, and network protection.

Learning Outcomes

Upon completion of the program, students will be able to:

- Identify and analyze cybersecurity threats and vulnerabilities
- Implement security measures to protect networks, systems, and data
- Apply cybersecurity policies, standards, and regulatory compliance
- Perform risk assessments and respond to security incidents
- Utilize security tools and technologies effectively in organizational settings

Course Content

Key areas covered in the Postgraduate Diploma in Cybersecurity include:

- Cybersecurity Fundamentals and Threat Intelligence
- Network Security and System Hardening
- Vulnerability Assessment and Penetration Testing
- Incident Detection and Response
- Security Policies, Compliance, and Risk Management
- Applied Cybersecurity Practices

Credit Value

Total Credit Load: 30 credits

Progression & Application

Graduates are prepared for roles such as cybersecurity analysts, IT security officers, network protection specialists, and systems security consultants. The program also provides a strong foundation for further studies at the master's level or for professional cybersecurity certifications.

Postgraduate Diploma in Information Technology

Award Type: Postgraduate Diploma (PGD)

Program Stream: Cybersecurity & Information Technology

Course Overview

The Postgraduate Diploma in Information Technology equips students with advanced skills in IT systems, software management, and technology integration in professional environments. The program combines theoretical knowledge with hands-on practice, enabling students to implement IT solutions that enhance organizational efficiency and security.

This program is suitable for professionals seeking careers in IT administration, systems management, and technology support roles.

Learning Outcomes

Upon completion of the program, students will be able to:

- Design, implement, and maintain IT systems in organizational settings
- Analyze and troubleshoot hardware, software, and network issues
- Apply best practices in IT governance and project management
- Evaluate and integrate emerging technologies into existing IT infrastructures
- Ensure compliance with security and operational standards

Course Content

Key areas covered in the Postgraduate Diploma in Information Technology include:

- IT Systems Design and Management
- Network and Database Administration
- Cloud Computing Fundamentals
- IT Project Management
- Information Security Principles
- Emerging IT Trends and Applications

Credit Value

Total Credit Load: 30 credits

Progression & Application

Graduates are prepared for roles such as IT support specialists, systems administrators, network coordinators, and IT project assistants. This diploma also provides a strong foundation for pursuing a master's degree in IT, cybersecurity, or related technology fields.

Postgraduate Diploma in Network Administration

Award Type: Postgraduate Diploma (PGD)

Program Stream: Cybersecurity & Information Technology

Course Overview

The Postgraduate Diploma in Network Administration focuses on the design, implementation, and management of organizational networks. Students gain practical skills in maintaining secure, efficient, and reliable network systems, preparing them for critical roles in IT infrastructure management.

This program is ideal for professionals seeking careers as network administrators, IT support specialists, or system operations coordinators.

Learning Outcomes

Upon completion of the program, students will be able to:

- Configure, manage, and monitor local and wide-area networks (LAN/WAN)
- Implement network security measures to protect organizational data
- Troubleshoot and resolve connectivity, hardware, and software issues
- Optimize network performance and ensure high availability
- Apply best practices in network documentation, monitoring, and governance

Course Content

Key areas covered in the Postgraduate Diploma in Network Administration include:

- Network Architecture and Design
- Routing and Switching
- Network Security Fundamentals
- Server and Infrastructure Management
- Troubleshooting and Network Optimization
- Emerging Trends in Network Technology

Credit Value

Total Credit Load: 30 credits

Progression & Application

Graduates are prepared for roles such as network administrators, IT operations coordinators, network support engineers, and infrastructure specialists. This program also provides a pathway to advanced studies in IT management, cybersecurity, and network systems at the master's level.

Postgraduate Diploma in Information Systems Security

Award Type: Postgraduate Diploma (PGD)

Program Stream: Cybersecurity & Information Technology

Course Overview

The Postgraduate Diploma in Information Systems Security equips students with the knowledge and skills to protect organizational information assets. The program emphasizes practical approaches to safeguarding networks, systems, and data against emerging cyber threats.

This program is suitable for professionals aspiring to careers in information security, IT auditing, or cybersecurity operations.

Learning Outcomes

Upon completion of the program, students will be able to:

- Assess and manage security risks for IT systems
- Implement policies and procedures for information security governance
- Design and enforce network and system access controls
- Detect, respond to, and mitigate cyber threats and vulnerabilities
- Apply industry standards and legal frameworks for information security

Course Content

Key areas covered in the Postgraduate Diploma in Information Systems Security include:

- Principles of Information Security
- Network Security and Intrusion Detection
- Secure Systems Design and Architecture
- Cybersecurity Policies and Compliance
- Incident Response and Disaster Recovery
- Emerging Threats and Advanced Security Techniques

Credit Value

Total Credit Load: 30 credits

Progression & Application

Graduates are prepared for roles such as information security analysts, IT security officers, cybersecurity consultants, and system auditors. The program also provides a foundation for further studies in cybersecurity, network security, or IT management at the master's level.

Postgraduate Diploma in IT Support & Infrastructure

Award Type: Postgraduate Diploma (PGD)

Program Stream: Cybersecurity & Information Technology

Course Overview

The Postgraduate Diploma in IT Support & Infrastructure provides students with the skills to design, implement, and maintain IT systems and support services. Emphasis is placed on troubleshooting, system administration, and infrastructure management to ensure reliable and efficient organizational operations.

This program is ideal for individuals pursuing careers as IT support specialists, system administrators, or infrastructure technicians.

Learning Outcomes

Upon completion of the program, students will be able to:

- Configure, manage, and maintain IT systems and networks
- Provide technical support for end-users and organizational systems
- Monitor and optimize IT infrastructure performance
- Apply best practices for system security and data protection
- Troubleshoot hardware, software, and network issues efficiently

Course Content

Key areas covered in the Postgraduate Diploma in IT Support & Infrastructure include:

- IT Systems Administration
- Network Configuration and Management
- Hardware and Software Troubleshooting
- User Support and Help Desk Management
- Cloud and Virtualization Technologies
- IT Infrastructure Security and Maintenance

Credit Value

Total Credit Load: 30 credits

Progression & Application

Graduates are prepared for roles such as IT support specialists, system administrators, infrastructure technicians, and help desk managers. The program also provides a pathway for further study in advanced IT management or cybersecurity programs.

Graduate Certificate in Cyber Risk Management

Award Type: Graduate Certificate

Program Stream: Cybersecurity & Information Technology

Course Overview

The Graduate Certificate in Cyber Risk Management equips students with the knowledge and skills to identify, assess, and mitigate cyber threats in organizational environments. The program emphasizes proactive risk assessment, regulatory compliance, and strategic management of cybersecurity risks.

This certificate is ideal for professionals seeking to enhance their expertise in protecting digital assets, managing information security risks, and supporting organizational resilience.

Learning Outcomes

Upon completion of the program, students will be able to:

- Assess organizational cyber risk and vulnerability
- Develop and implement risk mitigation strategies
- Apply cybersecurity frameworks and standards
- Conduct incident response and business continuity planning
- Evaluate regulatory compliance and ethical considerations in cyber risk management

Course Content

Key areas covered in the Graduate Certificate in Cyber Risk Management include:

- Principles of Cyber Risk and Governance
- Threat Analysis and Vulnerability Assessment
- Information Security Policies and Standards
- Risk Mitigation and Control Measures
- Incident Response and Business Continuity
- Compliance, Legal, and Ethical Considerations

Credit Value

Total Credit Load: 15 credits

Progression & Application

Graduates are prepared for roles such as cyber risk analysts, information security officers, compliance specialists, and IT security consultants. The program also serves as a foundation for further study in postgraduate diplomas or master's programs in cybersecurity and IT management.

Graduate Certificate in Network Security

Award Type: Graduate Certificate

Program Stream: Cybersecurity & Information Technology

Course Overview

The Graduate Certificate in Network Security provides students with practical and theoretical knowledge to protect, monitor, and maintain secure network infrastructures. The program emphasizes identifying vulnerabilities, implementing security protocols, and ensuring the integrity and confidentiality of data across organizational networks.

This certificate is ideal for professionals seeking to advance their expertise in network protection, cybersecurity operations, and IT infrastructure security.

Learning Outcomes

Upon completion of the program, students will be able to:

- Design and implement secure network architectures
- Monitor networks for vulnerabilities and threats
- Apply firewalls, intrusion detection systems, and encryption methods
- Conduct risk assessments for network security
- Develop policies and procedures for ongoing network protection

Course Content

Key areas covered in the Graduate Certificate in Network Security include:

- Network Security Fundamentals
- Threat Analysis and Intrusion Detection
- Firewall and Encryption Technologies
- Wireless and Cloud Network Security
- Risk Assessment and Incident Response
- Network Security Policies and Compliance

Credit Value

Total Credit Load: 15 credits

Progression & Application

Graduates are prepared for roles such as network security analysts, IT security administrators, network protection specialists, and cybersecurity consultants. The program also serves as a foundation for further study in postgraduate diplomas or master's programs in cybersecurity and IT management.

Graduate Certificate in Information Systems Administration

Award Type: Graduate Certificate

Program Stream: Cybersecurity & Information Technology

Course Overview

The Graduate Certificate in Information Systems Administration equips students with the skills to manage, maintain, and optimize enterprise information systems. Emphasis is placed on system administration, database management, network integration, and ensuring operational efficiency in organizational IT environments.

This program is suitable for professionals seeking to advance their careers as IT administrators, system managers, or information systems coordinators.

Learning Outcomes

Upon completion of the program, students will be able to:

- Configure and manage enterprise information systems
- Maintain secure and efficient database systems
- Integrate and monitor networked systems for optimal performance
- Apply troubleshooting and problem-solving techniques for IT systems
- Develop policies and procedures for system maintenance and security

Course Content

Key areas covered in the Graduate Certificate in Information Systems Administration include:

- System Administration Fundamentals
- Database Management and Optimization
- Network Integration and Management
- IT Infrastructure Maintenance
- Troubleshooting and Performance Monitoring
- Security and Compliance in Information Systems

Credit Value

Total Credit Load: 15 credits

Progression & Application

Graduates are prepared for roles such as systems administrators, IT support managers, network administrators, and information systems coordinators. This certificate also provides a pathway to postgraduate diplomas or master's programs in IT management and cybersecurity.

Professional Certificate in Ethical Hacking Fundamentals

Award Type: Professional Certificate

Program Stream: Cybersecurity & Information Technology

Course Overview

The Professional Certificate in Ethical Hacking Fundamentals introduces students to the principles and practices of ethical hacking, penetration testing, and vulnerability assessment. The program focuses on equipping learners with the skills to identify, analyze, and mitigate security threats in IT systems.

This program is ideal for IT professionals, security enthusiasts, and anyone seeking foundational knowledge in cybersecurity defense and ethical hacking practices.

Learning Outcomes

Upon completion of the program, students will be able to:

- Understand ethical hacking methodologies and legal considerations
- Perform vulnerability assessments and penetration testing
- Identify security threats and system weaknesses
- Apply defensive strategies to secure IT environments
- Use common tools and techniques for network and system security

Course Content

Key areas covered in the Professional Certificate in Ethical Hacking Fundamentals include:

- Introduction to Ethical Hacking
- Network and System Vulnerability Assessment
- Penetration Testing Techniques
- Security Tools and Software
- Legal and Ethical Considerations
- Incident Response and Mitigation

Credit Value

Total Credit Load: 10 credits

Progression & Application

Graduates are prepared for roles such as ethical hackers, junior penetration testers, cybersecurity analysts, and IT security support specialists. This certificate also serves as a foundation for more advanced certifications or postgraduate study in cybersecurity.

Professional Certificate in Cloud & Systems Security

Award Type: Professional Certificate

Program Stream: Cybersecurity & Information Technology

Course Overview

The Professional Certificate in Cloud & Systems Security provides students with the skills to secure cloud environments, networks, and IT systems. The program emphasizes practical knowledge in cloud security frameworks, system hardening, and protection against emerging cyber threats.

This program is ideal for IT professionals, system administrators, and security practitioners seeking specialized skills in safeguarding cloud and enterprise systems.

Learning Outcomes

Upon completion of the program, students will be able to:

- Implement security measures in cloud and on-premises systems
- Identify and mitigate threats targeting networks and cloud infrastructure
- Apply encryption, authentication, and access control techniques
- Monitor systems for potential breaches and vulnerabilities
- Understand compliance and regulatory considerations for cloud environments

Course Content

Key areas covered in the Professional Certificate in Cloud & Systems Security include:

- Cloud Security Principles and Architecture
- Network Security and Firewalls
- System Hardening and Secure Configurations
- Identity and Access Management
- Threat Detection and Incident Response
- Regulatory Compliance and Risk Management

Credit Value

Total Credit Load: 10 credits

Progression & Application

Graduates are prepared for roles such as cloud security specialists, systems security analysts, IT security administrators, and network security professionals. This certificate also provides a foundation for further studies or advanced certifications in cloud and systems security.

Professional Certificate in IT Service Management

Award Type: Professional Certificate

Program Stream: Cybersecurity & Information Technology

Course Overview

The Professional Certificate in IT Service Management equips students with the skills to effectively manage IT services, align IT operations with business needs, and optimize service delivery. The program emphasizes frameworks such as ITIL and best practices for maintaining reliable, efficient, and secure IT environments.

This program is ideal for IT managers, service desk coordinators, system administrators, and professionals responsible for delivering high-quality IT services.

Learning Outcomes

Upon completion of the program, students will be able to:

- Implement IT service management frameworks and best practices
- Design and manage service catalogs, workflows, and processes
- Monitor and optimize IT service performance
- Apply incident, problem, and change management procedures
- Align IT services with organizational goals and compliance requirements

Course Content

Key areas covered in the Professional Certificate in IT Service Management include:

- IT Service Management Principles and Frameworks (e.g., ITIL)
- Service Lifecycle Management
- Incident, Problem, and Change Management
- Service Level Agreements and Performance Metrics
- Continuous Improvement and Service Optimization
- Risk and Compliance in IT Services

Credit Value

Total Credit Load: 10 credits

Progression & Application

Graduates are prepared for roles such as IT service managers, service desk supervisors, IT operations coordinators, and IT governance officers. This certificate also provides a foundation for advanced IT service management certifications and leadership roles in IT operations.