Helsinki Metropolia University of Applied Sciences

HRMI

www.hrmi.lk

Master´s
in Information Technology
Cyber Security

Awarded by Helsinki Metropolia
University of Applied Sciences – Finland
The Largest University of Applied Sciences in Finland

UGC SRI LANKA RECOGNISED

Entry Requirements :

- 4 years Bachelor's Degree with 3 years post qualifying experience OR
- 3 years Bachelor's Degree with a Master's Degree and 3 years post qualifying experience.
- Knowledge of IT is required.

HUMAN RESOURCE MANAGEMENT INSTITUTE
A : No 23, Vijaya Kumaranathunga Mawatha (Polhengoda Rd), Colombo 05.
T : (0 11) 2811822, 5335986, 5335987, 7203334 **E :** info@hrmi.lk

For Enquiries & Commencement Dates : 077 2204101, 071 2724425

Master´s in Information Technology
Cyber Security

Helsinki Metropolia University of Applied Sciences in Finland is the biggest university for Applied Sciences in Finland and ranked amongst the best in Europe for professional education in Engineering, Information Technology, Business, Health Business Management and Health Care. Helsinki Metropolia is the recipient of The Finnish Education Evaluation Centre Award, The European Commission Mark of Distinction- The ECTS Label and many other academic honors. The The ECTS (European Credit Transfer and Accumulation System) enables a student to transfer credits amongst all European Universities, which signifies the standards and recognition of Helsinki Metropolia. Finnish education standards are considered amongst the best in the world.

1: Security and Risk Management

- Security Governance Principles
- Compliance
- Professional Ethics
- Security Documentation
- Risk Management
- Threat Modeling
- Business Continuity Plan Fundamentals
- Acquisition Strategy and Practice
- Personnel Security Policies
- Security Awareness and Training

2: Asset Security

- Asset Classification
- Privacy Protection
- Asset Retention
- Data Security Controls
- Secure Data Handling

3: Security Engineering

- Security in the Engineering Lifecycle
- System Component Security
- Security Models
- Controls and Countermeasures in Enterprise Security
- Information System Security Capabilities
- Design and Architecture Vulnerability Mitigation
- Vulnerability Mitigation in Embedded, Mobile, and Web-Based Systems
- Cryptography Concepts
- Cryptography Techniques
- Site and Facility Design for Physical Security
- Physical Security Implementation in Sites and Facilities

4: Communications and Network Security

- Network Protocol Security
- Network Components Security
- Communication Channel Security
- Network Attack Mitigation

5: Identity and Access Management

- Physical and Logical Access Control
- Identification, Authentication, and Authorization
- Identity as a Service
- Authorization Mechanisms
- Access Control Attack Mitigation

6: Security Assessment and Testing

- System Security Control Testing
- Software Security Control Testing
- Security Process Data Collection
- Audits

7: Security Operations

- Security Operations Concepts
- Physical Security
- Personnel Security
- Logging and Monitoring
- Preventative Measures
- Resource Provisioning and Protection
- Patch and Vulnerability Management
- Change Management
- Incident Response
- Investigations
- Disaster Recovery Planning
- Disaster Recovery Strategies
- Disaster Recovery Implementation

8: Software Development Security

- Security Principles in the System Lifecycle
- Security Principles in the Software Development Lifecycle
- Database Security in Software Development
- Security Controls in the Development Environment
- Software Security Effectiveness Assessment

9: Ethical Hacking

- Introduction to ethical hacking
- Foot printing and reconnaissance
- Scanning networks
- Enumeration
- Sniffing
- System hacking
- Malware threats
- Social engineering
- Denial of service
- Session hijacking
- Hacking web applications
- SQL injection
- Hacking wireless networks
- Hacking web servers
- Hacking mobile platforms
- Evading IDS, Firewalls, and Honeypot
- Cloud computing
- Cryptography

10: Security Solutions

- Implement access controls on files and folders
- Configure password policies and logon restrictions
- Create and manage user accounts
- Encrypt files and folders
- Implement virtual LANs for network security
- Configure network packet filters to restrict network traffic
- Open and close firewall ports
- Configure and secure remote access connections
- Create and secure VPN connections
- Configure web authentication and encryption
- Manage Internet browser security
- Disable unused network services
- Configure system auditing

11: Research

Mode of Delivery:

- Coursework - Delivered online by European Experts
- Research Guidance by HRMI

Duration: 1 year

Course Fees: € 3,200 (payable in 2 installments)

Registration Fees: Rs. 25,000