Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Department of Computing

Course: Postgraduate Diploma in Computing in Cybersecurity

Module Title: Cryptography and Forensic Analysis

Credits:	10
Credit Level:	9
Prerequisite Modules:	None

Description:

To provide the student with a solid understanding of the role cryptography, authentication and key exchange play in the security of computer systems. The module will also address the issues of wireless security, block chain and the applications of block chain technology. In addition, students will gain familiarity with post attack forensic analysis.

Module Learning Outcomes:

On successful completion of this module the learner will be able to:

1. Synthesise cryptography, authentication and key exchange to form a coherent understanding of the role of cryptography in wired and wireless systems
2. Apply experience with cryptographic attacks and their mitigation.
3. Produce original research based texts to communicate ideas concisely and effectively in written work which shows clear expression and coherent structure.
4. Forensically analyse and critically review a RAM based attack.
5. Defend a position on a selected aspect of cryptographic security.
6. Perform mathematical calculations that show deep understanding of cryptographic primitives.

Indicative Content:

1. Protocol Building Blocks
2. Mobile & Wireless Security
3. Cryptography & Blockchain
4. Advanced Forensics

Module Assessment:

Coursework	*100%*
End of Semester Final Exam	*0%*

Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Department of Computing

Course: Postgraduate Diploma in Computing in Cybersecurity

Module Title: Secure Infrastructure

Credits:	10
Credit Level:	9
Prerequisite Modules:	None

Description:

To provide the student with a solid understanding of infrastructure (cabling, networks, servers and services, security devices) both from the theoretical perspective and as an applied discipline. This module will analyse vulnerabilities in infrastructure and consider strategies to remediate them.

Module Learning Outcomes:

On successful completion of this module the learner will be able to:

1. Design and audit the necessary ICT infrastructure appropriate to particular business requirements.
2. Devise and implement solutions to particular service requirements in terms of services, servers and supporting infrastructure.
3. Critically analyse the possible attack vectors to an infrastructure.
4. Devise and formulate detection and response systems focussed on protecting critical infrastructure.
5. Evaluate and mitigate against techniques for detection avoidance and concealment.
6. Research and defend strategies using appropriate academic and industry sources.

Indicative Content:

1. Securing Enterprise Data Communications Infrastructure
2. Securing Operating Systems & Services
3. Securing the Perimeter Network
4. Securing the Internet Connection

Module Assessment:

Coursework	*100%*
End of Semester Final Exam	*0%*

Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Department of Computing

Course: Postgraduate Diploma in Computing in Cybersecurity

Module Title: Information Security Management 1

Credits:	10
Credit Level:	9
Prerequisite Modules:	None

Description:

To provide the student with a practitioner's understanding of information security from the view of various stakeholders, roles and process that interact with data at rest or data in transit. This module will cover the core competencies and lead the learner to investigate further new areas as they arise.

Module Learning Outcomes:

On successful completion of this module the learner will be able to:

1. Audit the necessary Information Systems appropriate to particular business requirements.
2. Critically analyse current best practice frameworks and methodologies for the implementation of security protocols for information systems.
3. Devise a scalable risk management plan including an appropriate risk response strategy based on risk analysis
4. Perform risk analysis to categorise and prioritize risk for communication to stakeholders and to enable directed response and monitoring for emerging risks
5. Devise a strategy for the left-shift of implementation of security protocols from the early stages of the SDLC to enhance the overall ALM
6. Research and defend strategies using appropriate academic and industry sources.

Indicative Content:

1. Introduction to Information Security
2. Legal & Mandatory Imperatives
3. Audit
4. Secure Application Lifecycle Management (ALM)
5. Risk

MODULE ASSESSMENT:

Coursework	*100%*
End of Semester Final Exam	*0%*

Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Department of Computing

Course: Postgraduate Diploma in Computing in Cybersecurity

Module Title: Software Compliance

Credits:	10
Credit Level:	9
Prerequisite Modules:	None

Description:

To provide the student with a significant level of comprehension both of the theoretical concepts underpinning vulnerabilities and also how to implement remediation strategies in modern object oriented programming languages.

Module Learning Outcomes:

On successful completion of this module the learner will be able to:

1. Critically analyse relevant topics in advanced secure programming.
2. Evaluate memory management problems and discuss strategies and practical solutions to these issues in a modern object oriented programming language.
3. Develop and evaluate software with security vulnerabilities and propose solutions for security-conscious environments.
4. Produce original texts to communicate ideas concisely and effectively in written work which shows clear expression and coherent structure.
5. Research and evaluate the impact of software security application.
6. Apply and categorise mitigations for various forms of software based attacks.

Indicative Content:

1. Code Vulnerabilities
2. Pernicious Kingdoms
3. Memory Management & Profiling
4. Evaluation of Applications & Future Trends

Module Assessment:

Coursework	*100%*
End of Semester Final Exam	*0%*

Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Department of Computing

Course: Postgraduate Diploma in Computing in Cybersecurity
Module Title: Information Security Management 2

Credits:	10
Credit Level:	9
Prerequisite Modules:	None

Description:

To provide the student with a solid background to information security management in projects and services from the governance level. As part of this module learners are encouraged to contribute to the leadership of their group by displaying critical thinking, analytical skills and judgement particularly when reviewing the impact of their decisions within the wider context.

Module Learning Outcomes:

On successful completion of this module the learner will be able to:

1. Critically assess the governance of IT security, evaluating the wider business and strategic environments within which the project resides.
2. Determine issues relating to the management of large scale complex projects and services including diverse underlying architectures.
3. Examine dynamic problems in an abstract form, analyse them and present a concrete controlled solution.
4. Devise and execute a comprehensive management project plan which incorporates a high level of personal autonomy and accountability.
5. Research and defend strategies in a professional manner using appropriate academic and industry sources.
6. Develop competencies in the determination, integration and management of communication and documentation needs over a project or service lifecycle.

Indicative Content:

1. Governance & Management of Systems
2. Project Lifecycle
3. Operations, Maintenance, Service Management
4. Incident Management
5. Information Security for Services
6. Applied Secure Product Lifecycle Techniques

MODULE ASSESSMENT:

Coursework	*100%*
End of Semester Final Exam	*0%*

Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Department of Computing

Course: Postgraduate Diploma in Computing in Cybersecurity

Module Title: Web Application Security and Software Standards

Credits:	10
Credit Level:	9
Prerequisite Modules:	None

Description:

To provide the student with a significant level of comprehension both Web Application security and relevant software compliance standards.

Module Learning Outcomes:

On successful completion of this module the learner will be able to:

1. Critically analyse selected topics in Web Application and software security.
2. Develop and evaluate applications with security vulnerabilities and propose solutions for security-conscious environments.
3. Produce original texts to communicate ideas concisely and effectively in written work which shows clear expression and coherent structure.
4. Appraise, review and critically and reflexively formulate issues involved in designing, developing and implementing a secure application from both a legal and ethical point of view.
5. Research and evaluate future trends in the field of application security and standards.
6. Revise and document the security of applications using various analysis techniques.

Indicative Content:

3. Application Vulnerabilities
4. Secure Document Exchange
3. Compliance & Standards
4. Evaluation of Applications & Future Trends

Module Assessment:

Coursework	*100%*
End of Semester Final Exam	*0%*