Prifysgol **Wrecsam**
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM760
Module Title	Secure Computing
Level	7
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP
Pre-requisite module	None

Programmes in which module to be offered

Programme title	**Core/Optional/Standalone**
MSc Cyber Security	Core
MSc Cyber Security with Advanced Practice	Core
MSc Computer Science	Core
MSc Computer Science with Advanced Practice	Core
MSc Computing for Business	Core

Breakdown of module hours

Learning and teaching hours	11 hrs
Placement tutor support hours	0 hrs
Supervised learning hours e.g. practical classes, workshops	10 hrs
Project supervision hours	0 hrs
Active learning and teaching hours total	**21 hrs**
Placement hours	0 hrs
Guided independent study hours	179 hrs
Module duration (Total hours)	**200 hrs**

Module aims

This module offers students a holistic understanding of key topics in computer security these may include:

- Risks & Threats
- Cryptography

- Secure software development principles
- Access control & Authentication
- Information security governance
- Security policy and risk management.

Students will explore various aspects such as identifying vulnerabilities, encryption algorithms, secure coding practices, user authentication methods, establishing security policies, and effectively managing risks and incidents. This module equips students with the knowledge and skills necessary to navigate the complex field of computer security and to implement robust security measures in diverse technological environments.

Module Learning Outcomes

At the end of this module, students will be able to:

1	Demonstrate the concepts, principles, and goals of secure computing.
2	Critically evaluate the risks and threats in the digital environment, implementing appropriate countermeasures.
3	Apply cryptographic techniques to ensure data confidentiality, integrity, and authenticity.
4	Implement secure software development principles and practices, mitigating common vulnerabilities and ensuring the creation of robust and secure applications.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The portfolio could assess tasks such as designing or implementing a cryptographic solution for a specific scenario, ensuring data confidentiality, integrity, and authenticity. Students will provide a detailed explanation of the cryptographic techniques employed and evaluate their effectiveness in safeguarding sensitive information.

Students may also be required to develop a secure software application following best practices and secure coding principles, mitigating common vulnerabilities such as injection attacks and cross-site scripting, and providing evidence of robust testing and validation.

Assessment number	Learning Outcomes to be met	Type of assessment	Duration/Word Count	Weighting (%)	Alternative assessment, if applicable
1	1,2,3,4	Portfolio	5000 Words or Equivalent	100%	

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience.

Welsh Elements

This module is designed to support Welsh-speaking students in line with the Welsh Language Standards. While the primary delivery will be in English, students will have the opportunity to submit assessments, including coursework and projects, in Welsh if preferred. Relevant module materials, such as reading lists, key texts, and guidance, will be available bilingually upon request, ensuring accessibility for all students. Additionally, where possible, guest speakers, case studies, or examples may include references to the Welsh business context, especially in areas such as data use in local industries and Welsh public sector organisations.

The department encourages students to develop bilingual digital skills by incorporating Welsh-language datasets, tools, and resources where appropriate, offering an inclusive learning environment. We also support the development of bilingual visualisation techniques, enabling students to create digital outputs that reflect the Welsh language, should they wish to do so.

Indicative Syllabus Outline

Risks and Threats

- Identification and classification of risks
- Risk assessment methodologies and frameworks
- Understanding the impact and likelihood of various threats
- Developing risk mitigation strategies and incident response plans

Cryptography

- Symmetric and asymmetric encryption algorithms
- Hash functions and digital signatures
- Key management

Secure Software Development Principles

- Input validation and secure error handling
- Mitigating common vulnerabilities
- Security-focused development methodologies

Access Control and Authentication

- Authentication mechanisms and access control
- Identity and access management

Information Security Governance and Risk Management

Indicative Bibliography

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads:

- Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, and Dwayne Williams. *Principles of Computer Security, CompTIA Security+ and Beyond*. McGraw-Hill Education, 2021.

Other indicative reading:

- W. Stallings., & L .Brown, *Computer Security: Principles and Practice*. Pearson, 2018.
- R Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2021
- B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley,2017.
- C. Kaufman, R. Perlman, & M. Speciner, *Network Security: Private Communication in a Public World*. Pearson, 2022.

Administrative Information

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2026
Date and details of revision	March 2026 Addition of MSc Computing for Business programme title
Version number	2