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** | COM481 |
| **Module Title** | Network Defence |
| **Level** | 4 |
| **Credit value** | 20 |
| **Faculty** | FACE |
| **HECoS Code** | 100376 |
| **Cost Code** | GACP |
| **Pre-requisite module** | N/A |

## Programmes in which module to be offered

| Programme title | Core/Optional/Standalone |
|---|---|
| BSc (Hons) Cyber Security | Core |
| BSc (Hons) Cyber Security with Industrial Placement | Core |
| Stand-alone module aligned to BSc (Hons) Cyber Security for QA and assessment | Option |
| BSc (Hons) Computing for Business | Core |

## Breakdown of module hours

| | |
|---|---|
| Learning and teaching hours | 24 hrs |
| Placement tutor support hours | 0 hrs |
| Supervised learning hours e.g. practical classes, workshops | 12 hrs |
| Project supervision hours | 0 hrs |
| **Active learning and teaching hours total** | **36 hrs** |
| Placement hours | 0 hrs |
| Guided independent study hours | 164 hrs |
| **Module duration (Total hours)** | **200 hrs** |

## Module aims

The module provides students with a comprehensive understanding of network security concepts, strategies, and techniques. Its primary objective is to equip students with the knowledge and skills to identify, analyse, and mitigate network security vulnerabilities. Students will learn about different types of threats, explore best practices for securing networks, and develop critical thinking through hands-on exercises and simulations. By the end

of the module, students will possess a strong foundation in network defence, enabling them to safeguard network resources effectively. The module aligns with industry best practices and prepares students for industry certifications, enhancing their career prospects and demonstrating their expertise in network defence.

## Module Learning Outcomes

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

| | |
|---|---|
| **1** | Demonstrate the fundamental concepts in information security and network defence. |
| **2** | Make informed decisions on the suitability of administrative, physical and technical controls within a network. |
| **3** | Identify, analyse and evaluate a range of network and data security vulnerabilities within an organisational context |
| **4** | Analyse and develop network and data security controls. |

## 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.

Assessment One will look at network defence from an organisational context allowing students to demonstrate an understanding of network defence concepts within an organisation context. This demonstration may take place through written submissions, practical demonstrations or video submissions.

Assessment Two is a 2-hr in-class test that is aligned with industry qualifications.

| Assessment number | Learning Outcomes to be met | Type of assessment | Duration/Word Count | Weighting (%) | Alternative assessment, if applicable |
|---|---|---|---|---|---|
| 1 | 1, 3 | Coursework | 1200 Words or Equivalent | 30 | |
| 2 | 2, 4 | In-class test | 2 hours | 70 | |

## Derogations

N/A

## Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework, the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE) and an online community. Students will have the flexibility to access course materials both synchronously and asynchronously. 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

Indicative syllabus includes topic areas that may include:

- Network Security Fundamentals
- Identity, Authorisation and Accounting
- Administrative Controls
- Physical & Technical Controls
- Wireless, Mobile & IoT
- Data Security
- Network Traffic Monitoring
- Cryptography and the Public Key Infrastructure
- Virtualisation and Cloud Computing Essentials

## Indicative Bibliography

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

**Essential Reads:**
N/A

**Other indicative reading:**

Easton, C. (2018). Network Defence and Countermeasures: Principles and Practices. Pearson.

Williams, S. (2022). Cryptography and Network Security: Principles and Practice. Pearson.

## Administrative Information

| **For office use only** | |
|---|---|
| Initial approval date | 08/11/2023 |
| With effect from date | Sept 2026 |
| Date and details of revision | March 26 – Addition of BSc (Hons) Computing for Business programme title |
| Version number | 2 |