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	COM466
Module title	Fundamentals of Information Security
Level	4
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Applied Cyber Security	Core
Standalone Module aligned to Applied Cyber Security for QA and assessment purposes	

Pre-requisites

None

Breakdown of module hours

Learning and teaching hours	36 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	36 hrs
Placement / work based learning	0 hrs
Guided independent study	164 hrs
Module duration (total hours)	200 hrs

For office use only	
Initial approval date	10 Nov 2021
With effect from date	Jan 2022
Date and details of revision	30/05/2024 APSC approval to offer module as a standalone module
Version number	2

Module aims

This course provides an introduction to the foundational concepts, principles, and practices of information security. Students will explore the fundamentals of protecting digital assets, mitigating risks, and safeguarding information systems against threats.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Analyse the impact of information systems on individuals and enterprises.
2	Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure
3	Compare and contrast the effectiveness of Tools, Techniques and Policies in Information Security
4	Evaluate the importance of security audits, testing, and monitoring in an IT infrastructure
5	Analyse the function of security controls in IT infrastructure.

Assessment

Indicative Assessment Tasks:

Assessment 1 is a portfolio, the portfolio will be reflect how the topics presented on the course are implemented / or could be in their working environment.

Assessment 2 is an In-class test, testing the students' knowledge and understanding of key principles.

Where practical assessment 1 will be related / carried out in the workplace.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	2,3,4	Portfolio	70%
2	1,5	In-class test	30%

Derogations

None

Learning and Teaching Strategies

The module is taught using a structured programme of lectures, online learning, mini-seminars, tutorials, practical exercises and student-centred learning specifically:

- Self-directed learning using on-line material and lectures to supplement on-line material

- On-line multiple choice tests to give formative feedback
- Web based research

Indicative Syllabus Outline

- Introduction to Information Security
- Security Principles and Models
- Network & Cyber Security
- Security Tools and Techniques
- Threats and Vulnerabilities
- Governance and Risk

Indicative Bibliography:

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

Essential Reads

Wills, M. (ISC)2 SSCP Systems Security Certified Practitioner Official Study Guide, Sybex; 2nd edition (7 Jun. 2019)

Other indicative reading

Gibson, D. CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide, 2014, ISBN 978-193913602

Smith, R E. Elementary Information Security, 2nd Edition, 2015, ISBN 978-1284055931

Goodman, M. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World Reprint Edition, 2016, ISBN 978-0804171458

Andress, J. The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice, 2nd Edition, 2014, ISBN 978-0128007440