city college plymouth

UNIVERSITY OF PLYMOUTH

PROGRAMME QUALITY HANDBOOK 2025/26

FdSc Applied Cyber Security

Welcome and Introduction to FdSc Applied Cyber Security

Welcome to FdSc Applied Cyber Security delivered at City College Plymouth.

This programme has been designed to equip you with the skills and knowledge base required to work in your chosen specialism or other graduate opportunities. It is also a platform from which you can undertake additional vocational and academic qualifications.

This Programme Quality handbook contains important information including:

- The approved programme specification
- Module records

Note: The information in this handbook should be read in conjunction with the current edition of:

- Your Programme Institution & University Student Handbook which contains student support based information on issues such as finance and studying at HE
    - available in your Google Classroom
  - Your Module, Teaching, Learning and Assessment Guide
    - available in your Google Classroom
- University of Plymouth's Student Handbook
  - available at: https://www.plymouth.ac.uk/your-university/governance/student-handbook

1. **Final Award Title: FdSc Applied Cyber Security**

   Named Exit Award: N/A UCAS

   code: FCYB

   HECOS code: 100376 (Computer and Information Security)

2. **Awarding Institution:** University of Plymouth

   Teaching institution(s): City College Plymouth

3. **Accrediting body**: N/A

4. Distinctive Features of the Programme and the Student Experience

The course has been designed in response to the increasing demand regionally, nationally and internationally for Cyber Security specialists. The threat of cyber attacks and unauthorised access to information grew exponentially during the Covid-19 pandemic as many companies moved to remote working, leading to increased sharing and storage of data online.

A Graduate of the FdSc Applied Cyber Security is someone who has studied the fundamental technical aspects of computing. They have chosen an academic pathway that enables them to develop further their understanding of the systems, networks, laws, risks and solutions involved in Cyber Security.

City College Plymouth has developed strong links with the local digital industry in which most graduates will eventually be seeking employment. The College encourages active participation of its industry partners in both the development and delivery of its programmes, which enhances the experience and employability of its graduates. Industry selected problems are incorporated into assessments where possible to allow students to gain real-life experience.

This award has been designed to meet the current needs of the South West Digital Sector and their component employers, both large scale as well as small and medium-sized enterprises (SMEs). A design principle is that this award can flex in both method delivery and content as the needs of the sectors, the region or the technology involved evolve.

Now part of the South West Institute of Technology (SWIoT), City College Plymouth have developed dedicated computing classrooms that are; computer networking, cyber security and Artificial Intelligence (AI) labs. Labs includes Cisco and Juniper equipment including routers, switches, hardware firewalls and VoIP. Also, the labs include several servers on which we have installed various operating systems such as MS Windows Server 2012, FreeBSD, ESXI and a few Linux distributions. One of the workstations in the lab once held the designation of "Super Computer" and contains over 40 thousand NVidia GPU cores. This computer will be used to build and research AI applications for cyber security.

This programme gives the student a broad knowledge of the sector, covering essential topics such as cryptography, systems analysis, threat intelligence, software engineering and machine learning. The programme will culminate in a team project, where students will bring together their knowledge and skills to solve a problem set by an industrial collaborator. Groups will have to work together within well defined targets and timescales to achieve completion.

The FdSc Applied Cyber Security program is also designed to equip students with the skills and knowledge necessary to combat modern cyber adversarial. The program is unique in that it focuses not only on traditional cyber security principles but also incorporates Artificial Intelligence (AI) and Machine Learning (ML) techniques to enhance cyber security strategies and understand, analyse and develop threat intelligence and threat modelling strategies. Students will learn to analyse data and develop algorithms to detect, prevent, and respond to cyber-attacks.

One of the distinctive features of this program is its emphasis on ethical hacking, with the importance of understanding ethics and legal concerns protecting privacy and confidentiality, avoiding legal liability, and maintaining trust with clients. Ethical hackers must operate within legal and ethical boundaries to effectively perform their work and provide value to their clients.

Students will learn to think like a hacker and be trained to identify vulnerabilities in systems and networks to secure them. The program provides students with hands-on experience using industry-standard tools and techniques to simulate real-world scenarios, giving them a solid foundation in the practical skills needed for a career in cyber security.

5. Relevant QAA Subject Benchmark Group(s)

This programme has been designed inline with the following subject benchmark statement for Computing (March 2022) which defines the academic standard expected of graduates with a Computing degree.
https://www.qaa.ac.uk/the-quality-code/subject-benchmark-statements/computing

SEEC Credit Level Descriptors for Higher Education (2021) has been integral in the writing of both the programme and module level outcomes in regard of scope and level. https://seec.org.uk/wp-content/uploads/2021/03/SEEC-Credit-Level-Descriptors-2021.pdf

The Characteristics Statement for Foundation Degrees (February 2022) describes the distinctive features of a Foundation Degree delivered in the UK. This strongly supports the importance of work based learning (WBL) within foundation degree qualifications. Please see appendix 2 for further detail regarding how WBL has been embedded in the course. https://www.qaa.ac.uk/docs/qaa/quality-code/foundation-degree-characteristics-statement-2020.pdf

6. Programme Structure:

Programme Structure for the Foundation Degree in Applied Cyber Security (full-time)

Year 1 (Level 4)					Year 2 (Level 5)				
Module Code	**Module Title**	**Credits**	**Semester**	**C / O**	**Module Code**	**Module Title**	**Credits**	**Semester**	**C / O**
CITY1142	Applied Cryptography	20	1	Core	CITY2160	Advanced Software Engineering	20	1	Core
CITY1143	Computer Systems and Operating Systems	20	1	Core	CITY2161	Data Modelling and Machine Learning for Cyber Security	20	1	Core
CITY1144	Introduction to Software Engineering	20	1	Core	CITY2162	Ethics, Legal and Management	20	1	Core
CITY1145	Security Fundamentals with Computer Networks	20	2	Core	CITY2163	Offensive and Defensive Security	20	2	Core
CITY1146	Systems Analysis	20	2	Core	CITY2164	Penetration Testing	20	2	Core
CITY1147	Threat Modelling and Intelligence	20	2	Core	CITY2165	Team Project	20	2	Core

Programme Structure for the Foundation Degree in Applied Cyber Security (Part-time)

Year 1
80 Level 4 Credits

Semester 1

Module Code	Module Title	Credits	C/O
CITY1142	Applied Cryptography	20	C
CITY1143	Computer Systems and Operating Systems	20	C

Semester 2

Module Code	Module Title	Credits	C/O
CITY1146	Systems Analysis	20	C
CITY1147	Threat Modelling and Intelligence	20	C

Year 2
40 Level 4 Credits and 40 Level 5 Credits

Semester 1

Module Code	Module Title	Credits	C/O
CITY1144 (L4)	Introduction to Software Engineering	20	C
CITY2161 (L5)	Data Modelling and Machine Learning for Cyber Security	20	C

Semester 2

Module Code	Module Title	Credits	C/O
CITY1145 (L4)	Security Fundamentals with Computer Networks	20	C
CITY2163 (L5)	Offensive and Defensive Security	20	C

Year 3
80 Level 5 Credits

Semester 1

Module Code	Module Title	Credits	C/O
CITY2160	Advanced Software Engineering	20	**C**
CITY2162	Ethics, Legal and Management	20	C

Semester 2

Module Code	Module Title	No. of Credits	C/O
CITY2164	Penetration Testing	20	C
CITY2165	Team Project	20	C

7. Programme Aims

The FdSc Applied Cyber Security programme is intended to:

- Provide learners with the knowledge, skills, and critical understanding of the role of cyber security principles, particularly ethical hacking and AI for cyber security.
- Furnish graduates with the knowledge, understanding and skills to be professionals in cyber security careers.
- Enable learners to continue in education or training in order to further develop existing skills or develop new competencies in cyber security or any other discipline.
- Enable learners to use their knowledge and skills in cyber security to collaborate on computing projects to develop their understanding of the nature of collaborative work in the context of Computing and the skills required for it to succeed.
- Enable learners to make a contribution to the digital community in the region and beyond, both during and upon completing the course.
- Provide quality HE within an FE environment to support widening participation and to provide learners with the best opportunity to achieve their potential.

8. Programme Intended Learning Outcomes (PILOs)

8.1. Knowledge and understanding

On successful completion graduates should have developed:

1) A deep understanding of the computing discipline and its practical applications, which is crucial for securing computer systems and networks. This includes knowledge of computer architecture, operating systems, programming languages, and databases essential for identifying and addressing security vulnerabilities.
2) A critical understanding of cyber security principles and various paradigms, such as access control, encryption, intrusion detection, and incident response. This understanding is essential for developing effective security strategies to mitigate current and future threats.
3) A strong knowledge and skills in modelling and systems analysis, which are vital in designing and developing secure systems, including the ability to create models, perform analyses, identify potential threats, evaluate security controls, and test the effectiveness of security measures.
4) An awareness of legal and ethical responsibilities in cyber security. This includes knowledge of relevant laws and regulations, such as data protection and privacy laws, and the ability to conduct security operations ethically and responsibly. This knowledge ensures that security measures are effective and implemented with integrity.

8.2 Cognitive and intellectual skills

On successful completion graduates should have developed:

1) Their ability to learn independently from a range of academic and industry sources and apply that learning to new problems. They will stay up-to-date with the latest industry developments and apply that knowledge to address new cyber security challenges.
2) The ability to analyse complex cybersecurity problems and evaluate and recommend solutions using professional judgement regarding risks, costs, benefits, and codes of practice. They will consider the broader context of cyber security and balance the need for protection against other organisational priorities.

8.2. Key and transferable skills

On successful completion graduates should have developed the ability to:

1) Communicate effectively in speaking, interviewing and interacting productively with a client, present and defend substantial work, engage with others and respond effectively to questions. They should be able to articulate complex cyber security concepts clearly and concisely and engage with stakeholders at all levels of the organisation.
2) Communicate effectively in writing, present a two-sided argument, expose technical information clearly, and comprehend and summarise resource material with proper citations of sources. They should be able to write clear and concise reports, document cybersecurity incidents and vulnerabilities, and communicate cyber security risks to senior management and other stakeholders.
3) Work autonomously and as part of a team as appropriate. They should be able to take ownership of tasks, work independently when required, and collaborate with others in a team environment to achieve common goals. They should also be able to adapt to different team dynamics and work effectively in various organisational structures.

8.3. Employment related skills

On successful completion graduates should have developed:

1) The ability to demonstrate personal initiative, self-motivation, self-learning and problem-solving skills. They should be able to identify and tackle cybersecurity challenges independently and continuously improve their knowledge and skills to stay ahead of emerging threats.
2) The ability to research, develop, and complete a practical problem-solving challenge regarding appropriate industry standards. They should be able to apply their knowledge and skills to real-world cybersecurity challenges and create solutions aligned with industry best practices.

3) A critical understanding of the role of cyber security, computer systems, software, and algorithms in various industry and public contexts. They should be able to appreciate the importance of cyber security in protecting critical infrastructure, financial systems, and personal data and be able to apply cyber security principles to a range of industry and public contexts.

8.4. Practical skills

On successful completion graduates should have developed:

1) The ability to analyse requirements and implement solutions to cyber security problems. They should be able to understand an organisation's security requirements and develop and implement security solutions that address those needs.
2) Skills to troubleshoot computer systems for operational faults and ensure the security of the systems. They should be able to identify and mitigate security vulnerabilities and apply appropriate security measures to protect the systems.
3) The ability to select and apply various cyber security solutions to business problems, including commercial, off-the-shelf, and bespoke solutions. They should be able to align these solutions with the organisational goals and requirements.
4) The skills to design, build, and test cyber security systems (software) in various contexts using different paradigms. They should be able to apply appropriate security controls and measures throughout the development process and ensure that the systems are resilient to attacks.

9. Admissions Criteria, including RPL and Disability Service arrangements NB The following table is a draft exemplar for an undergraduate programme

All applicants must have GCSE (or equivalent) Maths and English at Grade C/Level 4 or above.

Entry Requirements for FdSc Applied Cyber Security	
A-level/AS-level	Normal minimum entry requirements are 96 UCAS Points to include a relevant subject such as Computing
BTEC National Diploma/QCF Extended Diploma	Normal minimum entry requirements are 96 UCAS Points (Extended Diploma MMM) to include a relevant subject such as Computing
Access to Higher Education at level 3	Normal minimum entry requirements are 96 UCAS Points (45 M credits or 15 D, 15 M, 15 P) Access to HE Diploma in a relevant subject such as Computing
T-Levels	Normal minimum entry requirements are 96 UCAS Points (P-C or above on the core) in a relevant subject such as Computing

Welsh Baccalaureate	Normal minimum entry requirements are an equivalent of 96 UCAS Points from the successful completion of a Welsh Baccalaureate Advanced Diploma
Scottish Credit and Qualifications Authority (SCQF)	Normal minimum entry requirements are an equivalent of 96 UCAS Points (SCQF level 6) to include a relevant subject such as Computing
Irish Leaving Certificate	Normal minimum entry requirements are an equivalent of 96 UCAS Points to include a relevant subject such as Computing at Higher Level
International Baccalaureate	Normal minimum entry requirements are an equivalent of 96 UCAS Points to include a relevant subject such as Computing at Higher Level
English Language Requirements	Normal minimum entry requirements for International students are IELTS 5.5 overall with 5.0 minimum in all elements.
Other Qualifications and/or Experience	Non-traditional candidates with alternative equivalent qualifications or demonstrable experience will be considered and may be subject to an interview.
Direct Entry to Stage 2 (Level 5)	Students may enter at level 5 with a relevant HNC made up of 120 level 4 module credits subject to the University of Plymouth APL regulations.

10. Progression criteria for Final Awards

Students, who successfully complete the FdSc may progress to:

- Level 6 of BSc (Hons) Computer Science (Cyber Security) based at UoP
- Level 6 of BSc (Hons) Applied Computer Science based at CCP

11. Non Standard Regulations (NB: all non-standard regulations must be approved by QSSC)

None

12. Transitional Arrangements for existing students looking to progress onto the programme

No transitional arrangements are required as this is a new programme.

Appendix 1: (UG) Mapping table that reflects which core modules contribute to the Programme Intended Learning Outcomes (PILOs)
Tick those Programme Learning Outcomes the module contributes to through its assessed learning outcomes. Insert rows and columns as required.

Core modules	Programme Intended Learning Outcomes contributed to (for more information see Section 8)																Compensation Y/N	Assessment Element(s) and weightings 01 (online open book assessment) E1 (exam), E2 (clinical exam), T1 (test), C1 (coursework), A1 (generic assessment), P1 (practical)
	8.1 Knowledge and understanding				8.2 Cognitive and intellectual skills		8.3 Key and transferable skills			8.4 Employment related skills			8.5 Practical skills					
	1	2	3	4	1	2	1	2	3	1	2	3	1	2	3	4		
PILOs met at Level 4																		
CITY1142 Applied Cryptography	x	x	x		x			x	x	x	x	x	x	x	x	x	Y	C1 (50%) P1 (50%)
CITY1143 Computer Systems and Operating Systems	x	x	x		x	x			x	x	x	x	x		x	x	Y	C1 (50%) P1 (50%)
CITY1144 Introduction to Software Engineering	x				x	x	x	x	x	x	x					x	Y	C1 (40%) P1 (60%)
CITY1145 Security Fundamentals with Computer Networks	x	x	x		x			x	x	x	x	x	x	x	x		Y	C1 (50%) P1 (50%)
CITY1146 Systems Analysis	x		x		x			x	x	x	x	x	x				Y	C1 (100%)
CITY1147 Threat Modelling and Intelligence	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	Y	C1 (40%) P1 (60%)
PILOs met at Level 5																		
CITY2160 Advanced Software Engineering	x				x			x	x	x	x					x	Y	C1 (50%) P1 (50%)

CITY2161 Data Modelling and Machine Learning for cyber security	x	x	x		x			x	x	x	x	x	x		x		Y	C1 (40%) P1 (60%)
CITY2162 Ethics, Legal and Management		x		x	x	x	x	x	x	x	x	x	x		x		Y	C1 (100%)
CITY2163 Offensive and Defensive Security	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	Y	C1 (50%) P1 (50%)
CITY2164 Penetration Testing	x	x	x	x	x		x		x	x	x	x	x	x	x		Y	C1 (50%) P1 (50%)
CITY2165 Team Project	x				x		x		x	x							Y	C1 (100%)

Appendix 2: Work Based Learning

WBL is an essential element of Foundation Degrees and therefore needs to be detailed here and added to the programme specification.

FHEQ level: 4				
WBL Activity	**Prog Intended LO**	**Related Modules**	**Assessed LO**	**Range of Assessments**
Practical Skills	LO3. Design and implement cryptographic solution(s) for client needs. LO2 Apply good programming practice by producing an object oriented structured design as a programming solution. LO3. Design and implement computer and network security systems. LO4. Manage and troubleshoot networks and cyber security systems. LO4. Design, plan and implement mitigation measures.	CITY1142 CITY1144 CITY1145 CITY1147	8.5.1, 8.5.2, 8.5.3	Implementation of software, networks, cyber security applications and presenting data in a human-friendly manner. Creation of materials to present findings, including screencasts and practical demonstrations.
Problem Based Learning / Project Management	All LOs	All modules		Development of software and hardware solutions.
Presentations	LO1 LO2 LO3 LO4 LO1 Demonstrate an understanding of the principles of procedural and object oriented programming. LO3. Evaluate modelling notations and their cyber security application to business problems LO3. Identify and analyse vulnerable systems, resources; and identify risks. LO4. Design, plan and implement mitigation measures.	CITY1143 CITY1144 CITY1146 CITY1147	8.2.2, 8.3.1, 8.3.2, 8.3.3, 8.5.1, 8.5.2, 8.5.3, 8.5.4	Individual and group presentations, screencasts, demonstrations of cyber security policies, issues and applications.

Site/off site visits. Industry and academic events. Guest Speakers	Visits are more likely to relate to all modules: Speakers can be invited to cover any topic, both academic and industry-based and will be determined by availability.	All modules	8.4.3	This is not formally assessed as part of the programme.

An explanation of this map:

- Practical skills are fundamental to the programme, and students will be taught in labs for almost all of their sessions.
- A number of coursework assignments include the development of hardware or software systems. These will require adequate planning and management of time and resources.
- A number of units have a practical assignment that includes either a presentation or demonstration of practical work.
- A number of industry events are held in the region throughout the year that staff and students attend. We also arrange a number of external speakers from industry to come and speak to our students. Visiting IT organisations within the region to see facilities and meet employees.

FHEQ level: 5				
WBL Activity	**Prog Intended LO**	**Related Modules**	**Assessed LO**	**Range of Assessments**
Practical Skills	LO3 Optimise code(s) to perform on IT and OT environments. LO4 Implement and test architecture and designs in software. LO4 Design and implement one supervised and one unsupervised cyber security application. LO3. Design and implement from basic to advanced security systems based on needs. LO4. Manage, test and troubleshoot various cyber security	CITY2160 CITY2161 CITY2163 CITY2164	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.3.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.4.3, 8.5.1, 8.5.2, 8.5.3, 8.5.4	Implementation of software, networks, cyber security applications and presenting data in a human-friendly manner. Creation of materials to present findings, including screencasts and practical demonstrations.

	applications, systems and rules. LO1 LO2 LO3 LO4			
Problem Based Learning / Project Management	All LOs	All modules		Development of software and hardware solutions.
Presentations	LO2 Demonstrate the ability to capture and validate software requirements. LO3 Critically evaluate AI and ML paradigms for cyber security applications. L03 Demonstrate an understanding of the repercussions of failure to comply with regulations within industry L04 Illustrate an understanding of the ethical issues related to failure to comply to cyber security LO4 Evaluate and present the findings of a project to the client/sponsor.	CITY2160 CITY2161 CITY2162 CITY2165	8.1.1, 8.2.1, 8.3.1, 8.3.2, 8.3.3, 8.4.2, 8.4.1, 8.5.1 8.1.2, 8.1.4, 8.2.2, 8.3.1, 8.5.1, 8.5.3	Individual and group presentations, screencasts, demonstrations of cyber security policies, issues and applications.
Site/off site visits. Industry and academic events. Guest Speakers	Visits are more likely to relate to all modules: Speakers can be invited to cover any topic, both academic and industry-based and will be determined by availability.	All modules	8.4.3	This is not formally assessed as part of the programme.

An explanation of this map:

- Practical skills are fundamental to the programme, and students will be taught in labs for almost all of their sessions.
- A number of coursework assignments include the development of hardware or software systems. These will require adequate planning and management of time and resources.
- A number of units have a practical assignment that includes either a presentation or demonstration of practical work.
- A number of industry events are held in the region throughout the year that staff and students attend. We also arrange a number of external speakers from industry to come and speak to our students. Visiting IT organisations within the region to see facilities and meet employees.

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY1142 **MODULE TITLE: Applied Cryptography**

CREDITS: 20 **FHEQ LEVEL: 4** **HECOS CODE: 100376 Computer and Information Security**

PRE-REQUISITES: N/A **CO-REQUISITES: N/A** **COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module will develop the student's understanding and analytical skills of the cryptography algorithms and protocols and their applications. Students will learn how cryptographic algorithms are used in practical solutions.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*

E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	50%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To understand cryptography's role in the digital world.
- To understand and analyse cryptographic algorithms, procedures and protocols.
- To understand privacy and the role of algorithms.
- To understand and analyse symmetric and asymmetric algorithms.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module, the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	Programme Intended Learning Outcomes (PILOs) contributed to
1. Discuss and analyse the role of cryptographic systems in the modern digital world.	8.1.1, 8.1.3, 8.3.2, 8.4.3
2. Discuss and analyse a variety of algorithms, procedures and protocols.	8.2.1, 8.1.2, 8.1.3, 8.3.2, 8.4.3, 8.5.3, 8.5.4
3. Design and implement the cryptographic solution(s) for client needs.	8.1.1, 8.1.2, 8.3.3, 8.4.1, 8.4.2, 8.5.1, 8.5.2, 8.5.3, 8.5.4

4. Analyse Case Studies and Systematic Reviews of Cryptographic solutions	8.2.1, 8.3.2, 8.4.1, 8.4.2, 8.5.1

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: September 2023	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 1**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026 **NATIONAL COST CENTRE: 121**
MODULE LEADER: Tomek Bergier **OTHER MODULE STAFF:**

Summary of Module Content

- Cryptography history.
- Cryptography today and the future.
- Cryptography algorithms, procedures, and protocols.
- Private and public algorithms.
- Symmetric and asymmetric algorithms.
- Prime numbers in cryptography.
- Cryptography applications.
- Elliptic-Curve Cryptography (ECC).

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	Report on cryptography principles. LO1 LO2 LO4	100%
Practical	Design and implement cryptography solutions. LO3	100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Report on cryptography principles. (new/different). LO1 LO2 LO4	100%
Coursework in lieu of practical	Design and implement cryptography solutions (new/different). LO3	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD. ***Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.***

MODULE CODE: CITY1143 **MODULE TITLE: Computer Systems and Operating Systems**

CREDITS: 20 **FHEQ LEVEL: 4** **HECOS CODE: 100376 Computer and Information Security**

PRE-REQUISITES: N/A **CO-REQUISITES: N/A** **COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module will help learners to understand the fundamental components used in modern computers. The module will provide an overview of different types of computer systems and identify various operating systems that are used in different environments. Learners will gain knowledge of how various operating systems and software manage the hardware, processes etc.

ELEMENTS OF ASSESSMENT- *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	50%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:
The module aims to provide learners with the fundamentals of the key components of a computer, including understanding how computers represent numbering systems and an introduction to the role of a kernel in an operating system. The module will also identify the various types of computers and different operating systems as well as investigate computer systems advances and their cyber security advantages and disadvantages. In addition, inverse engineering will be introduced as a useful tool to understand how the hardware and software of a computer system are constructed.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant award/ programme Learning Outcomes)

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Demonstrate knowledge of the main components of a computer and its role in various environments.	8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.4.3

2. Demonstrate an understanding of computer systems that are used for business and individual needs.	8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.3.3, 8.4.3
3. Demonstrate knowledge of computer systems and operating systems used today for cyber security.	8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2, 8.4.1, 8.4.2, 8.4.3, 8.5.1, 8.5.3, 8.5.4
4. Demonstrate the analysis of diverse computer system infrastructures used as a result of modern world needs, which includes cyber security issues and solutions.	8.1.1, 8.1.2, 8.1.3, 8.2.2, 8.4.1, 8.4.2, 8.5.1, 8.5.3, 8.5.4

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2023**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 1**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026 **NATIONAL COST CENTRE: 121**
MODULE LEADERS: Grant Sewell **OTHER MODULE STAFF: Tomek Bergier**

Summary of Module Content

- History and the future of computing.
- Number systems, computing logic and proof methods.
- Computer components and architectures.
- Operating systems principles.
- Network OS, Server OS, Desktop OS.
- UNIX-Like and MS OS.
- Virtualisation.
- High-performance computing, parallel computing, supercomputing, datacentres, server farms etc.
- Computing at home and from small offices to large institutions and organisations.
- Hardware and software firewalls.
- Smart homes.

The module will begin with the history of computing, hardware, and operating system design, covering but not limited to such subjects as number systems and computing logic, and continue on to discuss the current state of computing, including the different types and categories of operating systems in use today, and move on to subjects such as virtualisation, high-performance computing, and the future of computing.

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name & associated ALO**	**Component Weighting**
Coursework	Report covering principles and components. LO1 LO2	100%
Practical	Design and implement security systems for two different computer systems. LO3 LO4	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Report covering principles and components (new/different). LO1 LO2	100%

Coursework in lieu of practical	Design and implement security systems for two different computer systems. (new/different). LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODUEL RECORD

SECTION A: DEFINITIVE MODULE RECORD. ***Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.***

MODULE CODE: CITY1144 **MODULE TITLE: Introduction to Software Engineering**

CREDITS: 20 **FHEQ LEVEL: 4** **HECOS CODE: 100376 Computer and Information Security**

PRE-REQUISITES: None **CO-REQUISITES:None** **COMPENSATABLE:**

Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*

The object oriented programming paradigm requires a programmer to *design* and *develop* code by considering what *objects* may exist in some system, how these are related to each other and how these may interact with each other. It is a proven method for developing reliable modular programs and encourages reuse which shortens development time.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	40%	**P1** (Practical)	60%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:

The module aims to provide learners with a deep introduction to Computer Programming, starting with an introduction to procedural programming and then moving to the fundamentals of object-oriented programming. It introduces concepts such as syntax, iteration, conditional statements (incl. logical operators), classes and objects, inheritance, aggregation, abstract classes and polymorphism in order that the learner may apply these correctly to object oriented programs. It will introduce the benefits of using an object oriented approach to software development, such as shorter development cycles, adaptable code, and ability to interact with differing systems using common platforms, but also initially introduce procedural programming (with a focus on related Cyber Security scripting/coding within hardware / BIOS / OS protection).

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Demonstrate an understanding of the principles of various computer programming.	8.1.1, 8.2.1, 8.2.2

2. Design computer programs in an object-oriented and aspect-oriented structure.	8.3.3, 8.4.1 , 8.4.2, 8.5.4
3. Implement an object-oriented programming solution.	8.4.1 , 8.4.2, 8.5.4
4. Test, verify and document the resulting object- oriented software.	8.2.2, 8.3.2, 8.3.1, 8.4.1, 8.5.4

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2023**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 1**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026 **NATIONAL COST CENTRE:**
121 MODULE LEADER: Dr Christopher Ford **OTHER MODULE STAFF:**

Summary of Module Content

- Classes, Abstract Classes, Interfaces/Pure Virtual Functions
- Constructors/destructors
- Encapsulation and public, private and protected scope
- Inheritance
- Association
- Composition
- Aggregation
- Polymorphism, Method Overloading, Method Overriding
- Libraries
- Design principles
    - coherence and (de-)coupling between the classes
    - identification of dependencies, aggregation, inheritances, data and file structures
    - class diagrams, sequence diagrams
- IDE - source code editor, compiler, interpreter, build automation tools, debugger
- Error and exception handling
- Testing, Verifying, Validating, Documentation

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	Report on design and theory of OOP. LO1	100%
Practical	Implement and test an OOP application. LO2 LO3 LO4	100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Report on design and theory of OOP. (new/different) LO1	100%
Coursework in lieu of practical	Implement and test an OOP application. (new/different) LO2 LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY1145	**MODULE TITLE: Security Fundamentals with Computer Networks**	
CREDITS: 20	**FHEQ LEVEL: 4**	**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: N/A	**CO-REQUISITES: N/A**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module will develop the student's analytical ability and provide a foundation for computer security. Students will learn different computer systems and networking attacks and study the techniques and methods for designing secure computer systems and networked systems.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	50%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:
The aim of this module is to provide learners with an understanding of the fundamental principles and techniques of computer systems and networks, threats and attacks, and to design and implement security rules. Besides, the module provides students with an introduction to computer networks, design, implementation and troubleshooting allowing students to develop computer networks, cloud and cyber security for small to medium businesses.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understand computer network components, types of network systems and protocols, and their security implications.	8.1.1, 8.1.2, 8.1.3, 8.4.1, 8.4.3
2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks.	8.1.1, 8.1.2, 8.1.3, 8.4.1, 8.4.3
3. Design and implement computer and network security systems.	8.2.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.5.1, 8.5.2
4. Manage and troubleshoot networks and cybersecurity systems.	8.2.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.5.1, 8.5.2, 8.5.3

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2023**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 2**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026 **NATIONAL COST CENTRE: 121**
MODULE LEADER: Grant Sewell **OTHER MODULE STAFF: Tomek Bergier**

Summary of Module Content
The module will begin by looking at the different network types (e.g. LAN, WAN, PAN, etc), components (e.g. servers, routers, firewalls, etc) and their functions. The curriculum will then focus on an overview of cyber security knowledge areas relevant to those networks and component functions. Module content will include sessions on protocols and layers, routing and switching, addressing and name resolution, physical security, logical security including authentication and cryptography, and policies. Practical sessions will provide hands-on experience of working with networking components with various functions, establishing the security of them, and analysing potential threats to that security.

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	Written report on computer and network cybersecurity design and management. LO1 LO2	100%
Practical	Design and implementation of cyber security for an organisational scenario. LO3 LO4	100%

REFERRAL ASSESSMENT (Same)

Element Category	Component Name	Component Weighting
Coursework	Written report on computer and network cybersecurity design and management. (New/Different) LO1 LO2	100%
Coursework in lieu of practical	Design and implementation of cyber security for an organisational scenario. (New/Different) LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD. ***Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.***

MODULE CODE: CITY1146	**MODULE TITLE: Systems Analysis**	
CREDITS: 20	**FHEQ LEVEL: 4**	**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: N/A	**CO-REQUISITES: N/A**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
Understanding the conceptual models of the software they create is necessary for software developers, and they must record this in both code and UML (Unified Modeling Language) diagrams. This module examines the modelling of an organisation using UML and the transition from the Business Model into the Cyber Security (Software) Model.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical)	
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:
This module aims to provide students with an understanding of the role and practicalities of systems analysis and the modelling of business systems. It also aims to help students understand the relationship between business models and cyber security using standard notations and modelling languages.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understand the process of analysing business requirements for cyber security.	8.1.1, 8.1.3, 8.2.1, 8.4.2, 8.4.3
2. Analyse and accurately apply cyber security models to the analysis of a business requirement	8.1.1, 8.1.3, 8.2.1, 8.3.3, 8.4.1, 8.4.2, 8.4.3, 8.5.1

3. Evaluate modelling notations and their cyber security application to business problems	8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.4.3

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2023**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 2**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026 **NATIONAL COST CENTRE: 121**

MODULE LEADER: Dr Andrew Watson **OTHER MODULE STAFF: Tomek Bergier Summary of Module Content**

Modelling notations

- UML; BPMN
- Object Constraint

Language Diagrams

- Use Cases
- Class diagram
- Workflow Diagrams
- Interaction Diagrams
- State Diagrams
- Activity

Diagrams UML tools

- Drawing vs Modelling
- Visual Paradigm
- Rational Architect
- MS Visio
- Cloud based

tools Transition to Software

- Implementation of Class diagrams
- O/R Mapping

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	C1 Report on an application of business modelling and the transition to cyber security (software) models. LO1 LO2	50%
	C2 Design and implement cyber security applications for business/organisation needs. LO3	50%
		100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework 1	Report on an application of business modelling and the transition to cyber security (software) models. Design and implement cyber security applications for business/organisation needs (new/different). LO1 LO2 LO3	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY1147	**MODULE TITLE: Threat Modelling and Intelligence**	
CREDITS: 20	**FHEQ LEVEL: 4**	**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: N/A	**CO-REQUISITES: N/A**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*

This module will develop the student's understanding of various threats in modern organisations and institutions. In addition, learners will develop the knowledge to prevent and mitigate cyber-attacks. Also, students will identify and analyse the requirements needed to provide cybersecurity solutions for systems.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	40%	**P1** (Practical)	60%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A
MODULE AIMS:

- To understand business model(s), infrastructures and security threats in organisations and institutions.
- To analyse and identify resources that may be attacked.
- To identify risks and mitigation measures.
- To understand threat modelling and threat intelligence processes.
- To design and plan mitigation measures.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understand the organisational structures and models; and security threats.	8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.4.1, 8.4.2, 8.4.3
2. Understand threat modelling and threat intelligence processes.	8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2, 8.4.1, 8.4.2, 8.4.3
3. Identify and analyse vulnerable systems, resources; and identify risks.	8.2.2, 8.3.1, 8.3.2, 8.3.3, 8.5.1, 8.5.2, 8.5.3, 8.5.4

4. Design, plan and implement mitigation measures.	8.3.1, 8.3.2, 8.3.3, 8.5.1, 8.5.2, 8.5.3, 8.5.4

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2023**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 2**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026 **NATIONAL COST CENTRE: 121**
MODULE LEADER: Tomek Bergier **OTHER MODULE STAFF:**

Summary of Module Content

- Business model(s)
- Business infrastructure(s)
- Threats, risks and mitigation measures.
- Threat modelling systems and software.
- Threat modelling processes and cycles.
- Threat intelligence systems and software.
- Threat intelligence processes and cycles.
- Plan mitigation measures.

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name & associated ALO**	**Component Weighting**
Coursework	Report on threat modelling in a modern organisation(s). LO1 LO2	100%
Practical	Design and implement a threat modelling system. LO3 LO4	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Report on threat modelling in a modern organisation(s). (New/different) LO1 LO2	100%
Coursework in lieu of practical	Design and implement a threat modelling system. (New/different) LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY2160 **MODULE TITLE: Advanced Software Engineering**

CREDITS: 20 **FHEQ LEVEL: 5** **HECOS CODE: 100376 Computer and Information Security**

PRE-REQUISITES: None **CO-REQUISITES: None** **COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module explores the principles and techniques of software development. The learners will understand analysis, design, software construction and testing in independent and collaborative development. Further, Functional and Aspect-Oriented Programming will be introduced (to add to the procedural and OOP paradigms already taught), focusing on its common usage within Cyber Security frameworks.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	50%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:

This module aims to develop an understanding of the analysis, design, software construction and testing processes and consolidate the learners' initial experiences of programming and the resulting development of software. The focus is the development of skills such as functional programming, OOP, AOP and procedural. In addition, it aims to extend their understanding of more complex ideas in software development, such as collaborative design and integration and a focus on programming for Cyber Security requirements.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understand software development architectures' differences, advantages and disadvantages (and Procedural, OOP, AOP and Functional programming styles).	8.1.1, 8.4.1, 8.4.2
2. Demonstrate the ability to capture and validate software requirements.	8.1.1, 8.4.1, 8.4.2

3. Optimise code(s) to perform on IT and OT environments.	8.2.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.5.4
4. Implement and test architecture and designs in software.	8.2.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.5.4

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2024**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 1**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/26 **NATIONAL COST CENTRE: 121**

MODULE LEADER: Tomek Bergier **OTHER MODULE STAFF: Dr Andrew Watson**

Summary of Module Content

1. Software Development Methodologies
    a. Values and principles
    b. Iteration, increments and evolution
    c. Communication and quality
    d. Development practices
    e. Pitfalls
2. Implementation in Object Oriented Programming, Aspect-Oriented Programming, Procedural and Functional Languages
3. Collaborative design and Integration testing
4. Creating test cases, analysis of test cases
5. Code optimisation

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name & associated ALO**	**Component Weighting**
Coursework	Implement and demonstrate code optimisation for a given scenario. LO1 LO2	100%
Practical	Test and troubleshoot code from scenario. LO3 LO4	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Implement and demonstrate code optimisation for a given scenario. LO1 LO2 (new/different).	100%
Coursework in lieu practical	Test and troubleshoot code from scenario. LO3 LO4 (new/different).	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY2161	**MODULE TITLE: Security**	**Data Modelling and Machine Learning for Cyber**	
CREDITS: 20	**FHEQ LEVEL: 5**		**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: None	**CO-REQUISITES:**	**None**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*

This module will introduce Machine Learning (ML) and Artificial Intelligence (AI) principles and practical methods for cyber security applications. In addition, the module introduces graphical and statistical representations for data modelling from cyber security datasets as well as real data.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	40%	**P1** (Practical)	60%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:

This module aims to provide students with the knowledge and skills to design and implement intruder detection and prevention software using supervised, unsupervised and semi-supervised algorithms. This will include statistical methods, artificial neural networks, deep learning, and research for new ML and AI methods for cyber security applications (both passive and active firewall types). The students will use readily available real-world datasets to achieve this. There is scope for project work within the public and private sectors/organisations willing to provide datasets for students to work with.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understanding of data modelling and statistical principles for computing.	8.1.1, 8.1.2, 8.1.3, 8.4.2
2. Understanding of the AI and ML principles.	8.1.1 8.1.2 8.1.3, 8.4.3
3. Critically evaluate AI and ML paradigms for cyber security applications.	8.2.1, 8.3.2, 8.3.3, 8.4.1, 8.5.1

4. Design and implement supervised and unsupervised cyber security applications.	8.2.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.5.3

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2024**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 1**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/26 **NATIONAL COST CENTRE: 121**
MODULE LEADER: Tomek Bergier **OTHER MODULE STAFF:**

Summary of Module Content

- Mathematics - statistical and probability principles.
- Database principles and SQL programming.
- Data modelling - physical, conceptual and logical data models.
- Supervised, unsupervised and semi-supervised paradigms.
- AI and ML principles.
- AI and ML for cyber security applications.

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name & associated ALO**	**Component Weighting**
Coursework	Report on state-of-art for AI in cyber security applications. LO1 LO2	100%
Practical	Design and implement AI cyber security applications. LO3 LO4	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Report on state-of-art for AI in cyber security applications. (new/different) LO1 LO2	100%
Coursework in lieu of practical	Design and implement AI cyber security application (new/different) LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD. ***Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.***

MODULE CODE: CITY2162	**MODULE TITLE: Ethics, Legal and Management**	
CREDITS: 20	**FHEQ LEVEL: 5**	**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: None	**CO-REQUISITES: None**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module explores the ethics and management of laws and policies in computing. The learners will acquire an understanding of different government acts and laws within the United Kingdom alongside the wider effects of breaches in security on individuals and institutions. In addition, an understanding of the management of reducing risks, enforcing policies and the procedures that ensue, will be introduced.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical)	
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:
The aim of this module is to provide learners with a fundamental understanding of the different laws, regulations and ethical implications surrounding digital storage and the security thereof. This will include gaining knowledge of items such as the following; Computer Misuse Act, the Data Protection Act (DPA) and General Data Protection Regulation (GDPR), Intellectual Property Act, and Equality Act. In addition, cyber crime, cyber security measures, and health and safety laws and regulations that employers and employees set out in company policies will be explored.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understand the laws and regulations to be followed by companies that store information digitally	8.1.2, 8.1.4, 8.4.1, 8.4.2, 8.4.3

2. Understand the legal implications related to failure to comply with regulations and the law surrounding cyber security	8.1.2, 8.1.4, 8.4.1, 8.4.2, 8.4.3
3. Demonstrate an understanding of the repercussions of failure to comply with regulations within industry	8.1.2, 8.1.4, 8.2.1, 8.2.2, 8.3.1, 8.3.2, 8.3.3, 8.5.1, 8.5.3
4. Illustrate an understanding of the ethical issues related to failure to comply to cyber security	8.1.2, 8.1.4, 8.2.1, 8.2.2, 8.3.1, 8.3.2, 8.3.3,

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2024**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 1**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/26 **NATIONAL COST CENTRE: 121**
MODULE LEADER: Gemma Lane **OTHER MODULE STAFF:**
Summary of Module Content

Laws relating to the digital storage of information:

- Computer Misuse Act
- The Data Protection Act (DPA)
- General Data Protection Regulation (GDPR),
- Intellectual Property Act
- Equality Act
- Copyright, Designs and Patents Act.

Regulations

- Network and Information Systems Regulations
- Employer regulations
- Employee regulations

Cyber crime

- Spoofing and Phishing scams
- Identity Theft scams
- Online Harassment
- Cyberstalking
- Invasion of privacy

Cybersecurity measures

- Anti-virus
- Firewalls
- Company policies
- Password security
- Data backups
- Multi factor identification
- Anti malware

Management

- Risk Assessment
- ISO Standards e.g. ISO27001
- IT Governance Cyber Risk

Assessment Health and safety

- Display screen equipment (DSE)
- Repetitive Strain Injury (RSI)
- Musculo-skeletal disorders (MSDs)

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	C1 Report on legal and regulatory requirements to be followed and the implications of failure to comply. LO1 LO2 C2 Report on the ethical impact and repercussions. Design and implement cyber risk assessment. LO3 LO4	50% 50% 100%

REFERRAL ASSESSMENT (Same)

Element Category	Component Name	Component Weighting
Coursework	Report on legal, ethical and regulatory requirements to be followed and the implications of failure to comply (New/different). LO1 LO2 LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY2163	**MODULE TITLE: Offensive and Defensive Security**	
CREDITS: 20	**FHEQ LEVEL: 5**	**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: None	**CO-REQUISITES: None**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module will develop the student's understanding and analytical skills of the cyber security applications. Students will learn how to design, implement and test Intruder Detection Systems (IDS) and Intruder Prevention Systems (IPS). Students will also gain skills to test various passive and active firewalls.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	50%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:
The aim of this module is to provide learners with an understanding of the advanced principles and techniques of the threats and potential attacks impacting computer systems and networks, in order to design and implement cyber security rules and applications.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Understand the complexity of organisational aspects of cyber security applications and the types and sources and computer systems and computer network attacks.	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.4.1, 8.4.2, 8.4.3
2. Understand and analyse cyber security policies and rules that are applied in various systems.	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.2.2, 8.4.1, 8.4.2, 8.4.3
3. Design and implement from basic to advanced security systems based on needs.	8.5.1, 8.5.2, 8.5.3, 8.5.4
4. Manage, test and troubleshoot various cyber security applications, systems and rules.	8.5.1, 8.5.2, 8.5.3, 8.5.4

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**

DATE OF IMPLEMENTATION: **September 2024**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 2**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/26	**NATIONAL COST CENTRE: 121**
MODULE LEADER: Tomek Bergier	**OTHER MODULE STAFF:**

Summary of Module Content

- Organisational aspects of computer systems and network security i.e. threats, client needs, etc.
- Cyber Security policies and rules.
- User/Admin access and rights.
- Design and implement various security systems.
- Border systems.
- Cyber security applications - implementing and testing the following: IDS and IPS, Firewall, IPtables, ACL, VPN, NAT, etc.
- Physical security - locks, sign-in/out systems, biometrics, etc.
- Smart homes, IoT, IIoT, etc.
- Security management systems Cisco vs. Juniper and others.
- Security Information and Event Management (SIEM).

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name & associated ALO**	**Component Weighting**
Coursework	Design and implement a cyber security application for given needs. LO1 LO2	100%
Practical	Testing and troubleshooting cyber security for given needs. LO3 LO4	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Design and implement a cyber security application for given needs. LO1 LO2 (new/different)	100%
Coursework in lieu of practical	Testing and troubleshooting cyber security for given needs. LO3 LO4 (new/different)	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD*. Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.*

MODULE CODE: CITY2164	**MODULE TITLE: Penetration Testing**	
CREDITS: 20	**FHEQ LEVEL: 5**	**HECOS CODE: 100376 Computer and Information Security**
PRE-REQUISITES: None	**CO-REQUISITES: None**	**COMPENSATABLE: Yes**

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module will help learners to understand security vulnerabilities in IT and OT as well as various computer systems. The module will provide penetration testing knowledge and skills. Students will learn how to use both active and passive penetration testing methods and software.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	50%
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing
Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To understand and analyse various penetration testing methods and software.
- To understand and test vulnerabilities in UNIX-Like and MS Windows operating systems.
- To understand and test vulnerabilities in computer systems and networks.
- To understand and test vulnerabilities in the cloud and hosting, etc.
- To use and understand sniffing and scanning tools.
- To understand the role and techniques of red, purple and blue teams in cyber security.
- To understand the typical stages of hacking.
- To understand commonly used custom vulnerability attack tools.
- To understand adversarial motives.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Demonstrate an understanding and analysis of penetration testing methods and techniques.	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.3.1, 8.3.3, 8.4.1, 8.4.2, 8.4.3,

2. Demonstrate hacking phases in a computing LAB environment.	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.2.1, 8.3.1, 8.3.3, 8.5.1, 8.5.2, 8.5.3
3. Use your knowledge and skills and apply them to penetration and testing of vulnerabilities in computing systems.	8.2.1, 8.4.1, 8.4.2, 8.4.3, 8.5.1, 8.5.2, 8.5.3
4. Analyse and log the results from the various penetration testing methods and techniques.	8.5.1, 8.5.2, 8.5.3

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2024**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 2**

Notes:

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/2026	**NATIONAL COST CENTRE: 121**
MODULE LEADER: Tomek Bergier	**OTHER MODULE STAFF: Grant Sewell**

Summary of Module Content

- UNIX-Like (includes BSD family OS) and MS Windows desktop and server OSes vulnerabilities and bugs.
- Computer networks include wireless (i.e. air-crack), vulnerabilities testing.
- Metasploit.
- Clouds and hosting cyber-attacks and defence systems.
- Security policies vulnerabilities.
- Sniffing tools i.e. Wireshark, TCPDump, air tools, net-tools, nload, nmap etc.
- Role of the following teams: red, purple, and blue.
- Various security attacks i.e. DDoS, Injections, Brute force, IP spoofing, ping of death, flooding attacks etc.
- Penetration Testing Execution Standard (PTES).
- Mobile vulnerabilities and penetration testing.
- Open Web Application Security Project (OWASP)
- Information Systems Security Assessment Framework (ISSAF)
- Backdoors techniques and analysis.
- Malwares, trojans and other viruses analysis.

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	Plan and implement the penetration testing. LO1 LO2	100%
Practical	Document and analyse the penetration testing. LO3 LO4	100%

REFERRAL ASSESSMENT (Same)

Element Category	Component Name	Component Weighting
Coursework	Plan and implement the penetration testing. (New/different). LO1 LO2	100%
Coursework in lieu of practical	Document and analyse the penetration testing (New/different). LO3 LO4	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025

UNIVERSITY OF PLYMOUTH MODULE RECORD

SECTION A: DEFINITIVE MODULE RECORD. ***Proposed changes must be submitted via Faculty/AP Quality Procedures for approval and issue of new module code.***

MODULE CODE: CITY2165 **MODULE TITLE: Team Project**

CREDITS: 20 **FHEQ LEVEL: 5** **HECOS CODE: 100376 Computer and Information Security**

PRE-REQUISITES: None **CO-REQUISITES:None** **COMPENSATABLE:**

Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*

This practical take on systems engineering introduces this as a means of facilitating and assuring the development of a complex computer related technical product. Focusing predominantly on introducing tools and techniques that can be applied at different stages of the product development cycle. It will cover relevant system analysis processes that support project management and will focus on the CyberDevOps model.

ELEMENTS OF ASSESSMENT - *see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical)	
E2 (Clinical Examination)		**A1** (Generic assessment)			
T1 (Test)		**O1** (online open book assessment)			

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

1. To introduce students to specifying and solving computing problems as part of a team.
2. To give students the opportunity to implement a project using a CyberDevOps approach to project management.
3. To develop students' ability to experiment with project management tools and techniques.
4. To allow students to learn how to demonstrate their ability to work as part of a team to find a solution to a problem.
5. To allow students to reflect and evaluate the skills required within a work based project.

ASSESSED LEARNING OUTCOMES: (additional guidance below; please refer to the Programme Specification for relevant Programme Intended Learning Outcomes).

At the end of the module the learner will be expected to be able to:

Assessed Module Learning Outcomes (ALOs)	**Programme Intended Learning Outcomes (PILOs) contributed to**
1. Select an appropriate project, preparing an appropriately detailed project proposal.	8.1.1, 8.3.1, 8.3.2, 8.3.3, 8.4.1
2. Demonstrate the application of	8.1.1, 8.3.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.4.3

CyberDevOps project management to a group project.	
3. Demonstrate the ability to work in a team project.	8.3.1, 8.3.2, 8.3.3, 8.4.1, 8.4.2, 8.4.3
4. Evaluate and present the findings of a project to the client/sponsor.	8.2.1, 8.3.1, 8.3.2, 8.3.3, 8.5.1

DATE OF APPROVAL: **09/05/2023**	**FACULTY/OFFICE: Academic Partnerships**
DATE OF IMPLEMENTATION: **September 2024**	**SCHOOL/PARTNER: City College Plymouth**
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER: Semester 2**

Notes:

The assessment is a group project with a minimum of 3 students in each group. Each group will receive a group mark which contributes 50% of the student's marks and 50% of the mark based on their individual contribution to the project.
The group will present their final projects to their peers, client/Sponsor and assessor.
The students will be taught project management principles and systems lifecycle models but will be required to use the agile or CyberDevOps development model.
Each student must chair at least one group meeting and also minute at least one meeting.
Students will be required to liaise with employers/clients to produce solutions to real world problems.

Additional Guidance for Learning Outcomes:

To ensure that the module is pitched at the right level check your intended learning outcomes against the following nationally agreed standards

- Office for Students, Sector-recognised Standards
- Office for Students, Quality and Standards Conditions of Registration
- Subject benchmark statements
- Professional, regulatory and statutory (PSRB) accreditation requirements (where necessary e.g. health and social care, medicine, engineering, psychology, architecture, teaching, law)

SECTION B: DETAILS OF TEACHING, LEARNING AND ASSESSMENT

Items in this section must be considered annually and amended as appropriate, in conjunction with the Module Review Process. Some parts of this page may be published on the website as a guide for prospective students. Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2025/26 **NATIONAL COST CENTRE: 121**
MODULE LEADER: Dr Andrew Watson **OTHER MODULE STAFF: Tomek Bergier**

Summary of Module Content

This module will initially cover the theory behind project management and different systems analysis lifecycles. The students will then undertake a group computing software project documenting all stages of development. Students will use the CyberDevOps model for software development.

SUMMARY OF TEACHING AND LEARNING		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	30	Combined lecture/lab sessions
Directed Study	30	Combined lecture/lab sessions
Student Self Study	140	Google classroom is the starting point for guidance in directed study with direction from the module leader.
Total	200	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name & associated ALO	Component Weighting
Coursework	C1 Project Proposal, Documentation and Reflection on skills developed for WBL. LO1 LO2 C2 Presentation of findings and evaluation to peers and assessor(s). LO3	70% 30% 100%

REFERRAL ASSESSMENT (Same)

Element Category	Component Name	Component Weighting
Coursework	Project proposal and documentation, slideshow with notes and supporting material to present findings and evaluation. LO1 LO2 LO3	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: June 2025	**Approved by**: Hollie Galpin-Mitchell Date: August 2025