PROGRAMME QUALITY HANDBOOK 2023/24

FdSc Applied Cyber Security

1. 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

- Your Module, Teaching, Learning and Assessment Guide
  - available on your programme VLE
- Plymouth University's Student Handbook
  - available at:
    https://www.plymouth.ac.uk/your-university/governance/student-handbook

1. Programme Specification

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

   Intermediate Award: N/A

   UCAS code: FCYB

   JACS code: N/A

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

   Teaching institution(s):   **City College Plymouth**

3. **Accrediting body**(ies)   **N/A**

4.   Distinctive Features of the Programme and the Student Experience

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 how reliable and secure software is developed. They will have developed software using a variety of different paradigms, using a range of languages and will have developed confidence in being able to use any new languages that they are required to use in the future. They will understand how to use models in the Applied Cyber Security process to model systems and organisations, and to solve complex Applied Cyber Security problems. They will also be able to program user interfaces that are fit for their intended purpose, allowing users to interact with systems securely and safely. They will have taken opportunities to meet with local businesses in the digital industries, and applied their knowledge and skills to developing software solutions to computing problems.

Graduates of the FdSc Applied Cyber Security are likely to go on to study on the BSc Computing at the University of Plymouth, but equally, they will have the confidence to seek a career, or to develop their own ideas into a business opportunity.

City College Plymouth has developed strong links with the local digital industry, the industry in which most Computing 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 the assessment which are then presented to the client/sponsor and the students are given the opportunity to reflect on work based learning skills gained from this experience.

Within Computing, the main method of delivery is to small groups of up to 20 students. As well as providing the core knowledge that students of computing require, there is a focus on project work and collaboration between students, not only within their group but across the range of Higher Education programmes delivered by the College, and with industry partners and clients. This provides a broader range of experiences for students and enhances their communication, collaboration and practical skills.

All of computing delivery is in the new STEM (Science, Technology, Engineering and Maths) Centre on Kings Road, providing a stimulating and comfortable learning environment where students can find all the hardware and software they need for their particular field of study, whilst sharing that environment with students studying in a range of science, creative and digital related subjects.

In addition to the new learning environment, Computing students have exclusive use of four dedicated computing labs, and a research space. Two of the labs offer their own dedicated networking environments to allow for experimentation in networking and security, whilst the software suites offer the student a range of open source and proprietary software to enhance the practical side of their education. Computing subscribes to Linux and Microsoft's Imagine programme, and is therefore able to provide students with fully licensed development software from Microsoft, as well as supporting the many open source options. This investment in resources continues on an annual basis ensuring that facilities are up to date and relevant.

All Computing programmes are delivered by a strong team with a depth and breadth to both academic and industry experience. Lecturers are here to teach, support and develop the knowledge and understanding of the subject that students have chosen

to study. The timetable will also be designed with students in mind and in most cases Computing students will benefit from a compact timetable that suits their needs, and that is consistent across the whole year, enabling them to plan the rest of their busy life around it.

The FdSc in Applied Cyber Security will allow students to make full use of the opportunities offered by the College and its Partnership with industry and the University, whilst focussing on the specific area of Applied Cyber Security. Students will study the underlying principles of Applied Cyber Security whilst enhancing their practical skills using the range of current industry tools and techniques. Students will have the opportunity to develop real systems, for real clients which may be either internal or external to the College and will have the opportunity to meet with, and learn from, industry partners. During their first year, students will share units with the other Computing Programmes, and can therefore make a more informed choice about the particular field of computing in which they ultimately wish to specialise. Dedicated students of the FdSc in Applied Cyber Security will graduate as highly employable individuals with a broad experience of the computing subject, along with a specialist knowledge, and practical skills in Applied Cyber Security.

5.   Relevant QAA Subject Benchmark Group(s)

The FdSc in Applied Cyber Security has been developed in consultation with various sources, both local and national, alongside our own significant experience. In particular, it considers the **QAA Subject Benchmark Statement for Computing**, the Department for Digital, Culture, Media and Sport's **UK Digital Strategy** policy paper, the **ACM/IEEE Computing Curricula Recommendations** and the **Foundation Degree Characteristics Statement**. In order to ensure delivery at the appropriate level, the Programme aligns learning outcomes with the **FHEQ** descriptors. The Programme also considers the needs of our local **industry partners**, in order to ensure that it supports the growth of the digital sector, and, thus, contributes to sustained economic growth in the region.

Like other types of Computing degree programmes, the FdSc in Applied Cyber Security is "designed to equip graduates with knowledge, understanding and skills which will enable them to begin a professional career in some aspect of Computing" (QAA, 2016). However, the College does not anticipate the particular area of Computing in which students may wish to specialise, nor does it expect all of its graduates to seek employment in the Computing sector. In its UK Digital Strategy policy paper (DCMS, 2017) the Department for Digital, Culture, Media and Sport demonstrates that there are a significant number of computing related careers in non-digital Industries. In addition to developing students' "understanding of the established principles in their field of study" (QAA, 2015), the FdSc in Applied Cyber Security embeds employability, minimum core, communication and critical thinking skills, to ensure that our Graduates have the best opportunity to gain employment in their chosen sector on graduation.

The College understands the desire of its graduates to progress to further study at level 6 and beyond. Therefore, as well as aligning its Learning Outcomes with the FHEQ descriptors at the appropriate level (QAA 2008), the Programme is cognisant of the higher level descriptors, ensuring graduates are adequately equipped to succeed should they continue with their education.

Whilst the College does not have a specific Industrial Advisory Board for Computing, it does work with a number of industry groups and partners in order to ensure that the curriculum is relevant and that its graduates are employable. Partners include Digital Plymouth, Software Cornwall, the Digital Policy Alliance and a variety of local and national organisations, who have either directly or indirectly contributed to the Programme.
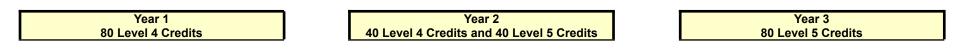
6. Programme Structure for the FdSc Applied Cyber Security (full-time) 2023/24

Year 1 (Level 4) 120 credits				
Module Code	Module Title	Credits	Semester	C / O
CITY1142	Applied Cryptography	20	1	Core
CITY1143	Computer Systems and Operating Systems	20	1	Core
CITY1144	Introduction to Software Engineering	20	1	Core
CITY1145	Security Fundamentals with Computer Networks	20	2	Core
CITY1146	Systems Analysis	20	2	Core
CITY1147	Threat Modelling and Intelligence	20	2	Core

Year 2 (Level 5) 120 credits				
Module Code	Module Title	Credits	Semester	C / O
CITY2160	Advanced Software Engineering	20	1	Core
CITY2161	Data Modelling and Machine Learning for Cyber Security	20	1	Core
CITY2162	Ethics, Legal and Management	20	1	Core
CITY2163	Offensive and Defensive Security	20	2	Core
CITY2164	Penetration Testing	20	2	Core
CITY2165	Team Project	20	2	Core

7. Programme Structure for the FdSc Applied Cyber Security (part-time) 2023/24

Year 1 80 Level 4 Credits	Year 2 40 Level 4 Credits and 40 Level 5 Credits	Year 3 80 Level 5 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

Semester 1			
Module Code	**Module Title**	**Credits**	**C/O**
CITY1144 (L4)	Introduction to Software Engineering	20	C
CITY1145 (L4)	Security Fundamentals with Computer Networks	20	C
Semester 2			
Module Code	**Module Title**	**Credits**	**C/O**
CITY2161 (L5)	Data Modelling and Machine Learning for Cyber Security	20	C

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

8. Programme Aims

The FdSc in Applied Cyber Security aims 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.
- 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 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.

9. Programme Intended Learning Outcomes

8.1. Knowledge and understanding

On successful completion graduates should have developed:

1) A knowledge and understanding of the computing discipline as a whole and its application.
2) A knowledge and understanding of cyber security principles and cyber security development in a range of paradigms.
3) A strong knowledge and understanding of the role of modelling and systems analysis in cyber security design and development.
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.

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.
2) Their ability to analyse cyber security problems, evaluate and recommend solutions using professional judgement with regard to risks, costs, benefits and codes of practice.

8.3. Key and transferable skills

On successful completion graduates should have developed the ability to:

1) Communicate effectively in speaking, interview and interact productively with a client, present and defend a substantial piece of work, engage with others and respond effectively to questions.
2) To communicate effectively in writing, present a two-sided argument, expose technical information clearly, and comprehend and summarise resource material with proper citation of sources.
3) To work both autonomously and as part of a team as appropriate.

8.4. Employment related skills

On successful completion graduates should have developed:

1) To demonstrate personal initiative, self-motivation, self-learning and problem-solving skills.
2) Their ability to research, develop and complete a practical problem-solving challenge with reference to appropriate industry standards.

3) Their understanding of the role of cyber security, computer systems, software and algorithms in a variety of industry and public contexts.

8.5.   Practical skills

On successful completion graduates should have developed:

1) Their strong ability to analyse requirements and implement solutions to cyber security problems.
2) Their ability to troubleshoot computer systems for operational faults and to ensure systems security.
3) Their ability to select and apply a variety of cyber security solutions to business problems, including commercial, off-the-shelf and bespoke solutions, which are aligned with organisational goals.
4) Their ability to design, build, and test cyber security (software) systems in a variety of contexts using different paradigms.

9. Admissions Criteria, including APCL, APEL and DAS arrangements

10. All applicants must have, or be working towards, a qualification equivalent to GCSE in Maths and in English at Grade a grade equivalent to C 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 6.0 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.

11. Progression criteria for Final and Intermediate 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
-

12. Non Standard Regulations

The part-time structure for many Foundation Degrees is a three year route, where 80 credits are delivered in the first year/stage at level-4, a mix of 40 level-4 and 40 level-5 credits are delivered in the second year/stage and the remaining 80 credits are delivered in the third year/stage.

An HNC is often approved using the same modules from level 4 of a foundation degree, these HNCs are delivered part-time over two years with students also studying 80 credits in year 1 and 40 credits in year 2 in a similar way to the foundation degree structure. Upon completion of the HNC, there is potential for students to continue their studies and complete level 5 of the foundation degree.

However, from this concept it would take students another 2 years to complete the foundation degree part-time, following the part-time structure and undertaking 40 credits at level 5 in their 3rd year of study and 80 credits at level-5 in their 4th year of study. This is disadvantageous to the students, in terms of the years committed to their study as well as causing their part-time experience to be inequitable in comparison to students who enrolled initially on the full 3 year part-time foundation degree. This currently puts pressure on students' original choice and thus impacts on demand for this area of study for the college.

To enable students to complete the foundation degree in three years, including the HNC and fd level-5 top-up, it has previously been agreed that during the second year of the HNC, students would study 40 credits of the level 5 foundation degree modules as a short course alongside the final 40 credits of level 4 of their HNC. This would mean that at the end of two years of study the students will have completed the HNC comprising of 120 level 4 credits and 40 credits of level 5, a total of 160 credits. These would be the same credits that a student enrolled on the foundation degree, at level-4 from the outset, would have completed.

The HNC students could then proceed to complete the final 80 credits of level 5 of the foundation degree and complete in the same timeframe they would have had they enrolled on the foundation degree.

This would mean that a student would APCL 160 credits onto the foundation degree. A non-standard regulation had previously been approved in 2017 to allow this; however, that non-standard regulation was associated with the change in structure of HNC programmes when their credit value was reduced from 160 to 120.

Proposal
To vary regulation ADM1.2 which states that the maximum amount of credit for prior learning which a student may claim towards a University of Plymouth foundation degree is 120 credits at level 4 or above and the credit which must be studied on a University of Plymouth foundation degree is 120 credits, including at least 60 at level 5 or above.

The non-standard regulation would apply to all City College Plymouth foundation degree programmes only where there is an HNC approved using the same modules from level 4 of that foundation degree. All other foundation degrees at City College Plymouth will follow the standard regulations and students bringing in an HNC awarded by another institution will follow standard regulations.

Proposed wording for the foundation degree programme specifications:

The maximum amount of credit for prior learning which a student may claim towards this University of Plymouth foundation degree is 160 credits - 120 credits at level 4 and 40 credits at level 5. The credit that must be studied on this University of Plymouth foundation degree is 80 credits at level 5. This applies only where the credit previously studied was awarded for:

- *A University of Plymouth HNC which has the same level 4 modules as this foundation degree and*
- *a University of Plymouth short course which has 40 credits of the same level 5 modules as this foundation degree.*

For any other credit previously awarded, standard regulations for recognition of prior learning apply.

13. Transitional Arrangements

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

2. Module Records

<u>**SECTION A: DEFINITIVE MODULE RECORD**</u>. ***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 <u>*Definitions of Elements and Components of Assessment*</u>					
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.	8.1.2 8.3.2
2. Discuss and analyse a variety of algorithms, procedures and protocols.	8.2.2 8.3.2
3. Design and implement the cryptographic solution(s) for client needs.	8.4.2
4. Analyse Case Studies and Systematic Reviews of Cryptographic solutions	8.5.1

DATE OF APPROVAL: 09/05/2023	FACULTY/OFFICE: Partnership
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: 2023/24   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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 8.2.1
2. Demonstrate an understanding of computer systems that are used for business and individual needs.	8.1.1 8.2.1
3. Demonstrate knowledge of computer systems and operating systems used today for cyber security.	8.3.2
4. Demonstrate the analysis of diverse computer system infrastructures used as a result of modern world needs, which includes cyber security issues and solutions.	**8.4.3 8.5.4**

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Partnership**
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: 2023/24　　　　　　　**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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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: 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.	8.1.3 8.3.1
2. Design computer programs in an object-oriented and aspect-oriented structure.	8.2.1 8.5.1
3. Implement an object-oriented programming solution.	8.5.3
4. Test, verify and document the resulting object-oriented software.	8.5.4

DATE OF APPROVAL: 09/05/2023	FACULTY/OFFICE: Partnership
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. <u>Some parts of this page may be published on the website as a guide for prospective students.</u> Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2023/24   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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.	8.1.2 8.4.3
2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks.	8.1.3 8.4.3
3. Design and implement computer and network security systems.	8.2.2 8.3.1 8.5.3
4. Manage and troubleshoot networks and cybersecurity systems.	8.5.2

DATE OF APPROVAL: 09/05/2023	FACULTY/OFFICE: Partnership
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: 2023/24   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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 8.4.3
2. Analyse and accurately apply cyber security models to the analysis of a business requirement	8.2.2 8.3.2
3. Evaluate modelling notations and their cyber security application to business problems	8.5.1

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Partnership**
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: 2023/24   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	100%

	business/organisation needs (new/different). LO1 LO2 LO3	

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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.	8.2.1 8.3.1
2. Understand threat modelling and threat intelligence processes.	8.1.3
3. Identify and analyse vulnerable systems, resources; and identify risks.	8.2.2 8.5.1
4. Design, plan and implement mitigation measures.	8.4.2

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Partnership**
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. <u>Some parts of this page may be published on the website as a guide for prospective students.</u> Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2023/24   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

UNIVERSITY OF PLYMOUTH MODULE RECORD

<u>SECTION A: DEFINITIVE MODULE RECORD</u>. *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).	8.1.3 8.3.2
2. Demonstrate the ability to capture and validate software requirements.	8.2.2 8.4.3
3. Optimise code(s) to perform on IT and OT environments.	8.4.2
4. Implement and test architecture and designs in software.	8.5.4

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE:** Partnership
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: 2024/25 **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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: Data Modelling and Machine Learning for Cyber 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 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.	8.1.3
2. Understanding of the AI and ML principles.	8.2.1
3. Critically evaluate AI and ML paradigms for cyber security applications.	8.5.1
4. Design and implement supervised and unsupervised cyber security applications.	8.4.2 8.5.4

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Partnership**
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. <u>Some parts of this page may be published on the website as a guide for prospective students.</u> Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2024/25   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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

DATE OF APPROVAL: 09/05/2023	FACULTY/OFFICE: Partnership
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. <u>Some parts of this page may be published on the website as a guide for prospective students.</u> Further details for current students should be provided in module guidance notes.

ACADEMIC YEAR: 2024/25   **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	50%
	C2 Report on the ethical impact and repercussions. Design and implement cyber risk assessment. LO3 LO4	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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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.	8.1.2 8.3.1 8.4.3
2. Understand and analyse cyber security policies and rules that are applied in various systems.	8.1.3 8.2.2 8.4.3
3. Design and implement from basic to advanced security systems based on needs.	8.5.3
4. Manage, test and troubleshoot various cyber security applications, systems and rules.	8.5.2

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Partnership**
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)

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

ACADEMIC YEAR: 2024/25   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

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.	8.1.2 8.1.4
2. Demonstrate hacking phases in a computing LAB environment.	8.1.2
3. Use your knowledge and skills and apply them to penetration and testing of vulnerabilities in computing systems.	8.3.3 8.4.3 8.5.4
4. Analyse and log the results from the various penetration testing methods and techniques.	8.2.2 8.3.3 8.5.1

DATE OF APPROVAL: 09/05/2023	**FACULTY/OFFICE: Partnership**
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: 2024/25   **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: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023

UNIVERSITY OF PLYMOUTH MODULE RECORD

<u>**SECTION A: DEFINITIVE MODULE RECORD**</u>*. 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)	70%	**P1** (Practical)	30%
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.	8.2.1 8.3.1
2. Demonstrate the application of CyberDevOps project management to a group project.	8.1.1 8.3.1
3. Demonstrate the ability to work in a team project.	8.3.3 8.4.1
4. Evaluate and present the findings of a project to the client/sponsor.	8.4.1 8.5.3 8.5.4

DATE OF APPROVAL: 09/05/2023	FACULTY/OFFICE: Partnership
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 prototype 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: 2024/25   **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	70%
Practical	P1 Presentation of findings and evaluation to peers and assessor(s). LO3	30% 100%

REFERRAL ASSESSMENT (Same)

Element Category	Component Name	Component Weighting
Coursework	C1 Project proposal and documentation, slideshow with notes and supporting material to present findings and evaluation. LO1 LO2	70%
Practical	P1 Presentation of findings and evaluation to peers and assessor(s). LO3	30%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Tomasz Bergier Date: 26/01/2023	**Approved by**: Joe Stephenson Date: 26/01/2023