city college plymouth

UNIVERSITY OF PLYMOUTH

PROGRAMME QUALITY HANDBOOK 2024/25

HNC Applied Cyber Security

1. Welcome and Introduction to HNC Applied Cyber Security

Welcome to HNC 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: HNC Applied Cyber Security**

   Intermediate Award: N/A

   UCAS code: HCYB

   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 HNC 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 HNC Applied Cyber Security are likely to go on to study on the FdSc Applied Cyber Security Level 5 at the City College 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 HNC 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 HNC 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 HNC 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 **Higher National Certificate 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 HNC 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 HNC 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 5 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 HNC Applied Cyber Security (full-time) 2024/25

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

7. Programme Structure for the HNC Applied Cyber Security (part-time) 2024/25

Year 1 80 Level 4 Credits			
Semester 1			
Module Code	**Module Title**	**Credits**	**C/O**
CITY1142	Applied Cryptography	20	C

Year 2 40 Level 4 Credits			
Semester 1			
Module Code	**Module Title**	**Credits**	**C/O**
CITY1144	Introduction to Software Engineering	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

Semester 2			
Module Code	**Module Title**	**Credits**	**C/O**
CITY1145	Security Fundamentals with Computer Networks	20	C

8. Programme Aims

The HNC in Applied Cyber Security aims to:

The HNC Applied Cyber Security programme is intended to:

- Equip learners with a comprehensive understanding of cyber security principles, particularly those related to artificial intelligence (AI). By providing learners with this knowledge, they will be able to seek careers in the cyber security field and become professionals with the necessary skills and expertise.
- Support learners in continuing education and to develop new competencies in cyber security or other related disciplines. Collaborative work is an integral part of the computing field, and learners will be encouraged to work together on computing projects to enhance their skills in this area.
- Equip learners with the skills to be able to make significant contributions to the digital community, locally and beyond. The program is designed to offer high-quality higher education within a further education setting, allowing for greater access and widening participation to ensure that all learners can achieve their full potential.
-

9. Programme Intended Learning Outcomes

9.1 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 knowledge and understanding of the role of modelling and systems analysis in cyber security design and development.

9.2 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 problems, evaluate and recommend solutions using professional judgement with regard to risks, costs, benefits and codes of practice.

9.3. 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.

9.4. 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.

9.5 Practical skills

On successful completion graduates should have developed:

1. Their 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.

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

9. 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.

NB The following table is an exemplar for an undergraduate programme

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

Entry Requirements for HNC 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.

10. Progression criteria for Final and Intermediate Awards

Students, who successfully complete the HNC may progress to:

- Level 5 of the FdSc Applied Cyber Security based at CCP

11. Non Standard Regulations

Overview

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.

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 Module Code	College Module Title	Credit Value	Level	Mandatory/Optional	Location of delivery
CITY1142	Applied Cryptography	**20**	**4**	**M**	**City College Plymouth**
CITY1143	Computer Systems and Operating Systems	**20**	**4**	**M**	**City College Plymouth**
CITY1144	Introduction to Software Engineering	**20**	**4**	**M**	**City College Plymouth**
CITY1145	Security Fundamentals with Computer Networks	**20**	**4**	**M**	**City College Plymouth**
CITY1146	Systems Analysis	**20**	**4**	**M**	**City College Plymouth**
CITY1147	Threat Modelling and Intelligence	**20**	**4**	**M**	**City College Plymouth**

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
	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	1	2	1	2	3	1	2	3	1	2	3	4		

																	assessment) , P1 (practical)
PILOs met at Level 4																	
CITY1142 Applied Cryptography		x			x		x			x		x				Y	C1 (50%) P1 (50%)
CITY1143 Computer Systems and Operating Systems	x			x			x				x				x	Y	C1 (50%) P1 (50%)
CITY1144 Introduction to Software Engineering			x	x		x						x		x	x	Y	C1 (40%) P1 (60%)
CITY1145 Security Fundamentals with Computer Networks		x	x		x	x					x		x	x		Y	C1 (50%) P1 (50%)
CITY1146 Systems Analysis	x				x		x				x	x				Y	C1 (100%)
CITY1147 Threat Modelling and Intelligence			x	x	x	x				x		x				Y	C1 (40%) P1 (60%)

Appendix 2:

Module Mapping to Pearson BTEC Higher National in Digital Technologies (Cyber Security Technologist)

Date completed: 25/01/2023

Pearson **BTEC Higher National Units**	**City College Plymouth** **HNC in Applied Cyber Security**
Unit 1: Professional Practice in the Digital Economy LO1 Explore the evolution and impact of digital technologies on work environments LO2 Examine the importance of professional development for career success LO3 Demonstrate a range of transferable and communication skills used for effective problem solving LO4 Review ways in which feedback can be used to support professional development planning and role in the workplace.	**CITY1142: Applied Cryptography** LO3. Design and implement cryptographic solution(s) for client needs. **CITY1143: Computer Systems and Operating Systems** LO2. Demonstrate an understanding of computer systems that are used for different needs. LO4. Demonstrate the analysis of diverse computer system infrastructures used as a result of modern world needs, which includes cybersecurity issues and solutions. **CITY1144: Introduction to Software Engineering** LO4 Test, verify and document the resulting object oriented software. **CITY1145: Security Fundamentals with Computer Networks** LO2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks.

Unit 2: Innovation & Digital Transformation LO1 Investigate the underlying context for digital innovation and market disruption that leads to business transformation LO2 Explore the different types of digital transformation LO3 Explain the requirements for a successful digital transformation LO4 Review the range of methods for protecting ideas as part of digital transformation strategies and their advantages and disadvantages.	**CITY1146: Systems Analysis** LO1. Understanding the process of analysing of business requirements for cyber security. LO2. Analyse and accurately apply cyber security models to the analysis of a business requirement. LO3. Evaluate modelling notations and their cyber security application to business problems.
Unit 3: Cyber Security LO1 Explore the nature of cybercrime and cyber threat actors LO2 Investigate cyber security threats and hazards LO3 Examine the effectiveness of information assurance concepts applied to ICT infrastructure LO4 Investigate incident response methods to cyber security threats.	**CITY1147: Threat Modelling and Intelligence** LO1. Understand the organisational structures and models; and security threats. LO2. Understand threat modelling and threat intelligence processes. LO3. Identify and analyse vulnerable systems, resources; and identify risks.
Unit 4: Programming LO1 Define basic algorithms to carry out an operation and outline the process of programming an application LO2 Explain the characteristics of procedural, object-orientated and event-driven programming LO3 Implement basic algorithms in code using an IDE LO4 Determine the debugging process and explain the importance of a coding standard.	**CITY1142: Applied Cryptography** LO2. Discuss and analyse a variety of algorithms, procedures and protocols. **CITY1144: Introduction to Software Engineering** LO1 Demonstrate an understanding of the principles of procedural and object oriented programming. LO3 Implement an object oriented programming solution of moderate size and complexity. LO4 Test, verify and document the resulting object oriented software.
Unit 5: Big Data & Visualisation LO1 Examine big data and visualisation for decision making LO2 Investigate statistical and graphical techniques, tools and industry software solutions for big data and visualisation LO3 Demonstrate the use of industry software to manipulate data and prepare visual presentations for a given data set LO4 Assess the role, responsibilities and challenges for data specialists.	**CITY1145: Security Fundamentals with Computer Networks** LO2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks. **CITY1147: Threat Modelling and Intelligence** LO1. Understand the organisational structures and models; and security threats. LO2. Understand threat modelling and threat intelligence processes. LO3. Identify and analyse vulnerable systems, resources; and identify risks. LO4. Design, plan and implement mitigation measures.
Unit 6: Networking in the Cloud LO1 Examine commonplace networking principles used in a cloud infrastructure to support communication LO2 Explain the operation of networking technologies within a cloud infrastructure LO3 Design a networking solution for a cloud-based system for a business use case LO4 Enhance network performance for a cloud-based system developed for a given business use case.	**CITY1145: Security Fundamentals with Computer Networks** LO1. Understand computer network components, types of network systems and protocols, and their security implications. LO2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks. LO3. Design and implement computer and network security systems. LO4. Manage and troubleshoot networks and cybersecurity systems.
Unit 8: Security LO1 Assess risks to IT security LO2 Describe IT security solutions	**CITY1145: Security Fundamentals with Computer Networks**

LO3 Review mechanisms to control organisational IT security LO4 Manage organisational security.	LO1. Understand computer network components, types of network systems and protocols, and their security implications. LO2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks. LO3. Design and implement computer and network security systems. LO4. Manage and troubleshoot networks and cybersecurity systems.
Unit 9: Networking LO1 Examine networking principles and their protocols LO2 Explain networking devices and operations LO3 Design efficient networked systems LO4 Implement and diagnose networked systems.	**CITY1145: Security Fundamentals with Computer Networks** LO1. Understand computer network components, types of network systems and protocols, and their security implications. LO2. Understand organisational aspects of network security, the types and sources and of computer systems and networking attacks. LO3. Design and implement computer and network security systems. LO4. Manage and troubleshoot networks and cybersecurity systems.

2. Module Records

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.	8.1.2 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. 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 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

<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: 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 C2 Design and implement cyber security applications for business/organisation needs. LO3	50% 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: 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. 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

- 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%

<table>
<tr><td colspan="2"><b>To be completed when presented for Minor Change approval and/or annually updated</b></td></tr>
<tr><td><b>Updated by</b>: Tomasz Bergier
Date: 26/01/2023</td><td><b>Approved by</b>: Joe Stephenson
Date: 26/01/2023</td></tr>
</table>