UNIVERSITY CENTRE TRURO & PENWITH

University of Plymouth
Academic Partnerships

Truro & Penwith College

Programme Quality Handbook

FdSc Cyber Security

2024–2025

TRURO COLLEGE PENWITH COLLEGE UNIVERSITY OF PLYMOUTH

Contents

WELCOME AND INTRODUCTION

Welcome and Introduction to FdSc Cyber Security

Welcome to the Foundation Degree (FdSc) in Cyber Security. This programme has been devised to develop a wide range of employable skills and knowledge in the field of computing, and is the result of consultations with employers, experts and University of Plymouth, as well as the specialist skills of staff involved in the programme. In it you will build on some aspects of computing that you already know, but will also come across new and challenging work that will broaden your expertise and make you aware of new possibilities. Apart from learning about computer systems and networks, you will also be developing skills in specialist subject areas, such as Behavioural Analytics, Security Programming and working with real clients and organisations. Particularly in the second year you will be developing skills to prepare you for higher level employment.

This programme has been designed to equip you with the skills and knowledge relevant to your chosen specialism and 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 University Centre Student Handbook (on SharePoint) which contains information on issues such as finance, student support, careers, learning resources and studying at University Centre Truro and Penwith; the University of Plymouth Student Handbook https://www.plymouth.ac.uk/your-university/governance/student-handbook; and your Teaching, Learning and Assessment Handbook available on SharePoint.

Programme Specification

1. Award

Final award title: FdSc Cyber Security

UCAS code: I120

JACS code: I120

HECoS code: 100376 computer and information security

2. Awarding Institution: University of Plymouth

Teaching institution(s): Truro and Penwith College

3. Accrediting body(ies)

N/A

4. Distinctive Features of the Programme and the Student Experience

The FdSc Cyber Security is an exciting opportunity to study a combination of Computing and Cyber Security modules that include the development of higher level specialist skills in areas such as Risk Management, Disaster Recovery Planning, Network Security Design and Digital Forensics. It is suitable for level 3 students progressing from computing related programmes. It should also appeal to industry employees, and system administrators who are working in/or have role descriptions that include a level of responsibility for organisational IT Security provisioning. The world of Cyber Security is fast moving and this programme will provide people with an opportunity to develop their practical and academic skills within a specialist pathway, using professional equipment within a dedicated adult learning environment. This programme will equip students with an understanding of IT Security issues, technical working methodologies and the academic and practical skills required to specialise in their chosen field. The HE Computing team have a network of connections to a range of local employers, and in the past students have created opportunities to work for local, national and international companies. The ability to develop entrepreneurship has led to some learners starting their own businesses. The programme intends to take a “360ºapproach” to studying Cyber Security and its uniqueness within Cornwall.

The FdSc Cyber Security has the following distinctive features:

- Learners will learn a range of specialist Cyber Security skills that are required by Cyber Security companies and organisations which they deem necessary for employment within the Cyber Security industry.
- Students will undertake a security/cyber audit on a business infrastructure.
- Undertake penetration testing/ethical hacking on an isolated physical network.
- Using behavioural analytics identify areas of weakness and effects of social engineering.
- Investigate and analyse the effects and evidence left behind after a range of cyber attacks.
- Undertake a digital forensics investigation.
- Learners will process a digital crime scene and acquisition digital hardware and evidence.
- Undertake digital evidence retrieval and processing.
- The course is vocational, developing practical Cyber Security skills with the aid of employer led briefs and industry placed case studies, at the same time as keeping the academic and intellectual rigor. The course will enable students to develop their own practice from this knowledge base, acquiring the skills that employers see as important to succeed in any area of employment (such as communication, democratic, self-motivation and responsibility).
- The course develops students understanding of practice and makes clear links between theory and practice and the importance of work placements, drawn from the programme team's network of local practitioners and employers.
- A strong emphasis on learning and practice undertaken during year 1 (level 4) provides a solid foundation, through which students are able to progress into year 2 (level 5).
- The opportunity to engage in research allowing students to develop their own interests, whilst acquiring and developing skills of research and investigation.
- The programme has been designed to equip students with the skills and knowledge base required to work in their chosen specialism with opportunities

for support and mentoring from employer's in-order to progress to employment and/or further educational opportunities.

- Students have access to professional equipment, and technicians within a dedicated, modern and comfortable building.
- Students will have the opportunity to undertake additional qualifications recognised by industry such as CISCO, CISCO Cyber Opps, A+, Network+.
- Regular individual tutorial support and guidance is a strong feature of this course.

5. Relevant QAA Subject Benchmark Group(s)

- Framework for Higher Education (FHEQ) programmes at level 4 and 5
- Foundation Degree Characteristics Statement (2015)
- Subject Benchmark Statement: Computing (2016)

6. Programme Structure

6.1. Full-time

YEAR 1 (Level 4)			
Module Title	**No. of Credits**	**Core / Optional**	**Term/ Semester**
TRUR1193 Professional Development & Study Skills	20	Core	1
TRUR1194 Work Practice Case Study	20	Core	1
TRUR1195 Security Programming	20	Core	1 & 2
TRUR1269 Networking & Systems	20	Core	1 & 2
TRUR1197 Server Administration & Systems Compliance	20	Core	2
TRUR1198 Behavioural Analytics & Data Security	20	Core	2

YEAR 2 (Level 5)			
Module Title	**No. of Credits**	**Core / Optional**	**Term/ Semester**
TRUR2188 Risk Management & Disaster Recovery Planning	20	Core	1
TRUR2267 Digital Forensics	20	Core	2
TRUR2190 Work Placement & Current Issues	20	Core	1 & 2
TRUR2268 Network Security & Design	20	Core	1
TRUR2192 Security Technology & Applied Cryptography	20	Core	2
TRUR2193 System Development Project	20	Core	1 & 2

6.2. Part Time Indicative route (Four Years)

YEAR 1 (Level 4)			
Module Title	**No. of Credits**	**Core / Optional**	**Term/ Semester**
TRUR1193 Professional Development & Study Skills	20	Core	1
TRUR1198 Behavioural Analytics & Data Security	20	Core	2
TRUR1195 Security Programming	20	Core	1 & 2

YEAR 2 (Level 4)			
Module Title	**No. of Credits**	**Core / Optional**	**Term/ Semester**
TRUR1269 Networking & Systems	20	Core	1 & 2
TRUR1197 Server Administration & Systems Compliance	20	Core	2
TRUR1194 Work Practice Case Study	20	Core	1

YEAR 3 (Level 5)			
Module Title	**No. of Credits**	**Core / Optional**	**Term/ Semester**
TRUR2188 Risk Management & Disaster Recovery Planning	20	Core	1
TRUR2267 Digital Forensics	20	Core	2
TRUR2190 Work Placement & Current Issues	20	Core	1 & 2

YEAR 4 (Level 5)			
Module Title	**No. of Credits**	**Core / Optional**	**Term/ Semester**
TRUR2268 Network Security & Design	20	Core	1
TRUR2192 Security Technology & Applied Cryptography	20	Core	2
TRUR2193 System Development Project	20	Core	1 & 2

7. Programme Aims

The Programme intends to:

A1. develop a comprehensive understanding of computer systems, computer networks, hardware and applications.

A2 develop an analytical appreciation of current industry focused Cyber Security issues.

A3. develop academic and professional skills which can be appropriately applied to practice.

A4. develop an ability to apply and evaluate an analytical knowledge of computer systems, computer networks and hardware. This should be applied to a range of problems and scenarios to communicate solutions appropriately.

A5. develop student's knowledge of their responsibilities as IT security practitioners. An awareness of the cultural, economic, ethical, legal, political and social dynamics will be developed to inform effective working environments.

8. Programme Intended Learning Outcomes

8.1. Knowledge and understanding

On successful completion learners should have developed:

8.1.1. a broad understanding and knowledge of the role of changing computing technologies and trends, including emergent technologies, environmental issues.

8.1.2. a knowledge and understanding of a range of Cyber Security threats and mitigation.

8.1.3. an understanding of the IT Security Sector enabling identification and evaluation of employment and further education opportunities.

8.2. Cognitive and intellectual skills

On successful completion learners should be able to:

8.2.1. identify principles and concepts applied to industry processes and practices through engagement with employers.

8.2.2. apply analytical and evaluative skills, to solve unfamiliar industry/non-industry related problems.

8.2.3. comprehend and evaluate how sustainability and social divisions play key roles in the computing industry.

8.2.4. consider and evaluate their own work in a reflexive manner, with reference to academic and/or professional conventions, issues and debates.

8.3. Key and transferable skills

On successful completion learners should have developed the ability to:

8.3.1. identify, locate and access information, developing skills and abilities for independent learning.

8.3.2. propose solutions from analytical enquiry to practical problems and scenarios, communicating outcomes effectively to a range of audiences.

8.3.3. carry out detailed research for creative productions, essays, projects, or reports involving sustained independent and critical enquiry.

8.3.4. work productively in a group or a team, showing ability to listen, communicate, and contribute.

8.4. Employment related skills

On successful completion learners should have developed:

8.4.1. planning and organisational skills managing own workflows and schedules.

8.4.2. flexible, creative and independent ways of working, showing self-discipline, self-direction and reflexivity.

8.4.3. the ability to develop, initiate, evaluate and explain solutions from analytical enquiry to practical problems and scenarios, communicating outcomes effectively to a range of audiences.

8.4.4. a range of industry/employer desirable “trade experience/certificates/ qualifications”.

8.5. Practical skills

On successful completion learners should be able to:

8.5.1. demonstrate the ability to design, install and configure networks, systems and applications within specific contexts and produce solutions and/or alternatives.

8.5.2. develop as appropriate, specific proficiencies in using a range of current and emergent Cyber Security and Computer technologies.

8.5.3. use a range of appropriate mediums for effective presentation and communication.

8.5.4. apply theory to industry based Cyber Security scenarios and the production and evaluation of effective solutions to complex problems.

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

All applicants must have GCSE (or equivalent will be considered) Maths and English at Grade 4/C or above plus a relevant level 3 qualification. Applicants will be interviewed to assess the experience/capabilities for successful entry and completion of the course.

Entry Requirements for FdSc Cyber Security	
Level 3: at least one of the following: - AS/A Levels - Advanced Level Diploma - BTEC National Certificate/Diploma - VDA: AGNVQ, AVCE, AVS - Access to HE or Year 0 provision - International Baccalaureate - Irish/Scottish Highers/Advanced Highers	48 UCAS points from relevant Level 3 qualification. Achievement of an Access to HE Diploma
Work Experience	Considered on an individual basis through an interview process.
Other HE qualifications / non-standard awards or experiences	Considered on an individual basis through an interview process.
APEL / APCL possibilities	APEL/APCL will be considered as per University of Plymouth Regulations
Interview / Portfolio requirements	All students will be interviewed
Entry to Level 5	Entry from L4 HNC Cyber Security; other HNCs/Level 4 qualifications will be considered on an individual basis.
Independent Safeguarding Agency (ISA) / Disclosure and Barring Service (DBS) clearance required	Students are expected to purchase a current DBS, if required for placement.

Apply online at www.ucas.com. For further information on the admissions process contact heEnquiry@truro-penwith.ac.uk or 01872 267061.

10. Progression criteria for Final and Intermediate Awards

Students undertaking the FdSc Cyber Security may progress onto the following degrees:

- BSc (Hons) Applied Computing Technologies (Truro and Penwith College).
- BSc (Hons) Computer Science Level 6 at University of Plymouth
- BSc (Hons) Computer Science (Cyber Security) Level 6 at University of Plymouth

Other institutions may also offer appropriate third year choices and students are encouraged to discuss other options with their Personal Tutor. Applications for progression will be subject to availability and must be submitted by the given deadline.

Upon completion of the FdSc Cyber Security, students may be suited to work in a variety of settings and these opportunities include, but are not limited to working in the following sectors:

- Cyber Security
- Digital Forensics
- IT Organisational Security
- Networking
- IT Compliance
- Computing
- Data and systems analytics

11. Non Standard Regulations

N/A

12. Transitional Arrangements

N/A

Appendix A: Programme Specification Mapping (FdSc Cyber Security Yr1)

Core Modules		Programme Intended Learning Outcomes contributed to (for more information see Section 8)																		Compensation Y/N	Assessment Element(s) and weightings [use KIS definition] E1- exam E2 – clinical exam T1- test C1- coursework A1 – generic assessment P1 - practical
		8.1 Knowledge & understanding			8.2 Cognitive & intellectual skills				8.3 Key & transferable skills				8.4 Employment related skills				8.5 Practical skills				
		8.1.1	8.1.2	8.1.3	8.2.1	8.2.2	8.2.3	8.2.4	8.3.1	8.3.2	8.3.3	8.3.4	8.4.1	8.4.2	8.4.3	8.4.4	8.5.1	8.5.2	8.5.3	8.5.4		
Level 4	TRUR1193 Professional Development & Study Skills				✓	✓			✓	✓				✓				✓			Y	C1 – 100%
	TRUR1194 Work Practice Case Study	✓			✓	✓			✓					✓					✓		Y	C1 – 70% P1 – 30%
	TRUR1195 Security Programming		✓		✓				✓				✓				✓				Y	C1 – 100%
	TRUR1269 Networking & Systems		✓			✓				✓			✓				✓	✓			Y	C1 – 50% O1 – 50%
	TRUR1197 Server Administration & Systems Compliance	✓	✓		✓				✓				✓					✓			Y	C1 – 100%
	TRUR1198 Behavioural Analytics & Data Security	✓	✓			✓				✓									✓		Y	C1 – 70% P1 – 30%
Level 4 LOs																						

Core Modules		Programme Intended Learning Outcomes contributed to (for more information see Section 8)																			Compensation Y/N	Assessment Element(s) and weightings [use KIS definition] E1- exam E2 – clinical exam T1- test C1- coursework A1 – generic assessment P1 - practical
		8.1 Knowledge & understanding			8.2 Cognitive & intellectual skills				8.3 Key & transferable skills				8.4 Employment related skills				8.5 Practical skills					
		8.1.1	8.1.2	8.1.3	8.2.1	8.2.2	8.2.3	8.2.4	8.3.1	8.3.2	8.3.3	8.3.4	8.4.1	8.4.2	8.4.3	8.4.4	8.5.1	8.5.2	8.5.3	8.5.4		
Level 5	TRUR2188 Risk Management & Disaster Recovery Planning						✓				✓			✓	✓					✓	Y	C1 – 100%
	TRUR2267 Digital Forensics						✓	✓							✓				✓		Y	C1 – 50% O1 – 50%
	TRUR2190 Work Placement & Current Issues			✓				✓				✓		✓		✓			✓		Y	C1 – 70% P1 – 30%
	TRUR2268 Network Security & Design										✓			✓	✓	✓					Y	C1 – 50% O1 – 50%
	TRUR2192 Security Technology & Applied Cryptography			✓			✓	✓				✓			✓						Y	C1 – 100%
	TRUR2193 System Development Project			✓				✓			✓	✓		✓	✓				✓	✓	Y	C1 – 70% P1 – 30%
Level 5 LOs																						
Confirmed Award LOs																						

Appendix B: WBL / ERL Mapping

Embedded employability skills assessed on higher education modules

Course: FdSc Cyber Security

Report completed by: Clint Washington

Date February 2019

Code: include date and activity as mapped on scheme of work; and A(F or S): if linked to assessment (formative or summative);

year	Module code	Module title	***Professional Skills***				
			Verbal communication	**Written communication**	**ICT & Mathematics**	**Time management and organisation**	**Independent learning ability**
Year 1	1193	Professional Development & Study Skills	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.	In all modules students are expected to produce written assignments, in the form of reports, essays, responses to problem questions, and/or mock examinations. As IT/Computing students a high level of English and Maths is expected and encouraged. Feedback will include reference to this (AS (Exam))	ICT- throughout Maths: Lectures cover a range of relevant numerical information and manipulation thereof in order for HE study.	Nov & Mar AS Throughout There is opportunity for developing key time management and organisational skills throughout all modules. The HNC is primarily a vocational based course, students are actively encouraged to maximise time, and develop key organisational skills, not only linking to assignments and exam deadlines, but to complete tasks and formative work	Throughout All students are encouraged throughout all modules to consider work experience. (many students only experience is education) with this in mind CPD and Work Experience Folders have been created and supplied for learners to log experience and practice.

Year 1	1194	Work Practice Case Study	Presentation completed websites Students undertake classroom discussions and group presentation of research findings regularly throughout the module		ICT- throughout Maths: logic & Equality Lectures cover a range of work related case topics. covering relevant numerical information and manipulation thereof.	AS – Oct, Jan	Throughout
Year 1	1195	Security Programming	Students undertake classroom discussions and group presentation of research findings regularly throughout the module	Throughout – and AS Jan	Number Systems Performance Data Algorithms. Logic, operators Lectures cover a range of programming based topics, including Algorithms, number systems, arrays, matrices etc. Covering relevant numerical information and manipulation of data	Throughout – AS	Throughout
Year 1	1269	Networks & Systems	Students undertake classroom discussions and group presentation of research findings throughout the module	Throughout	ICT: throughout Maths: logic operators number systems Binary, Octal, Hex. Lectures cover a range of networking and computer systems information based topics, including: Computer Architecture, Network Architecture, number systems, addressing.	Throughout	Throughout

Year 1	1197	Server Administration & Systems Compliance	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.	Throughout	ICT- throughout Oct Analog / Digital Dec Compression, bandwidth, usage etc.	Feb AS May E	Throughout
Year 1	1198	Behavioural Analytics & Data Security	Students undertake classroom discussions and group presentation of research findings throughout the module. The module leans heavily upon the development of individuals reasoning and democratic processes skills		ICT: throughout Maths: Heuristics & Problem solving, statistics, analysing data sets, matrices etc, Maths is an inherent discipline within Heuristics and analytical processes.	Mar AS May AS	Throughout
Year 2	2188	Risk Management & Disaster Recovery Planning	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.		Throughout	AS – OCT - Dec	Throughout
Year 2	2267	Digital Forensics	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.		Hex, Binary maths throughout	AS –Apr E - Jun	Throughout
Year 2	2190	Work Placement & Current Issues	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.		Workplace dependant/throughout	AS – Nov - Apr	Throughout

Year 2	2268	Network Security & Design	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.		Throughout	AS – Mar E- Jun	Throughout
Year 2	2192	Security Technology & Applied Cryptography	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.		Throughout	AS – Feb-May	Throughout
	2193	System Development Project	Students undertake classroom discussions and group presentation of research findings regularly throughout the module.		Throughout	AS Jan - May	Throughout

Opportunities for WBL in modules on Higher Education programme

Course: FdSc Cyber Security

Report completed by: Clint Washington

Date: February 2019

Code: include date of activity that is mapped on scheme of work; and A(F or S): if linked to assessment (formative or summative);

year	Module code	Module title	Employer engagement in regular review of module content	One or more examples of this practice required by Foundation Degree.			Module includes employer designed assessment brief	Module assessment is a work-related scenario	Employers visit college as part of module or deliver substantive module content	Trips to employer as part of timetable	Co-curricular employer based or derived projects
				Work-placement or existing place of work	work practice relating to ‘ self-employment’	Work placement simulation in college					
1	1193	Professional Development & Study Skills			Yes			F&S . (F&S, A)	Yes		External employer to engage with the learners to help with interview skills, CVs, communicatio n etc.

											1st year progress is monitored through a range of formative worked embedded within current curricular. (F)
1	1194	Work Practice Case study				Yes		Assessment will include a work based scenario suitable for developing Computing and Cyber Security employees consideration of Ecommerce, DPA, legal and ethical issues (F&S, A)	Yes		
1	1195	Security Programming	Review content upon current trends in delivering Security Programming in industry (F)			Yes	Yes	Assessment will include a work based scenario, (F&S, A)	Yes		

1	1269	Networking & Systems	Review content upon current trends in delivering information including “Internet of Things” “Big Data” various models of storing data. Computer and networked systems			Yes		Assessment Includes a work based scenario. (F&S, A)			
1	1197	Server Administration & Systems compliance				Yes		Assessment will include a work based scenario, which also investigates the use of Servers, security policies, and governance and compliance (F&S, A)			
1	1198	Behavioural Analytics & Data Security	Providing data sets simulation and linking theory to practice		Yes	Yes		Assessment will include a work based scenario			
2	2188	Risk Management & Disaster					Yes	Assessment will include a			

		Recovery Planning						work based scenario			
2	2267	Digital Forensics					Yes				
2	2190	Work Placement & Current Issues	Work Placement	Yes	Yes				Yes	Yes	
2	2268	Network Security & Design					Yes	Assessment will include a work based scenario			
2	2192	Security Technology & Applied Cryptography									
2	2193	System Development Project	Possible Project/live project brief		Yes	Yes	Yes		Yes		Yes

Level 4 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: TRUR1193	**MODULE TITLE: Professional Development & Study Skills**	
CREDITS: 20	**FHEQ LEVEL:** 4	**HECoS CODE:** 101090 study skills
PRE-REQUISITES: None	**CO-REQUISITES:** None	**COMPENSATABLE:** Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module introduces and develops the necessary academic, research and study skills needed at HE mode of study, lifelong learning and personal development. The students will also develop an appreciation, understanding through evaluation of the IT security industry, identifying opportunities and developing professional skills in answer to employers, technologies and industries changing needs.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical**)**	
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop an understanding of the concepts of professional, and continual professional development.
- To develop research, communication & presentation skills and techniques relevant to academic study and working practice.
- To investigate and evaluate the developing Cyber Security Industry, identifying emergent trends and shortages of skills.
- To develop knowledge and skills relevant to the Cyber Security Industry

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Research and present an understanding of professional development and its relevance to industry.	8.2.1, 8.2.2, 8.3.1, 8.4.2
2. Plan, document and implement career development pathways.	8.3.1
3. Develop, explain and demonstrate the key skills required within academic study.	8.3.1
4. Plan, deliver and communicate effectively within a range of appropriate formats.	8.2.2, 8.3.1, 8.3.2, 8.5.2

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-19	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 1

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 used in the KIS return and published on the extranet 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: Dave Cook

OTHER MODULE STAFF: Naomi Johns-Dyer, Dave Cook, John Glazebrook, Richard Morris, Paul Smith

Summary of Module Content

Professional development along with relevant study skills are a vital part of modern computing industry and academic study. This module introduces both the concepts, reasoning and practice of these essential skills. The module introduces the student to research, reading, academic and professional writing and communication skills, as well as the opportunity to investigate, plan and develop those employability skills necessary for their desired career pathway.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecture	15	Lectures, investigations. (FA)
Practical classes and workshops	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided Study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Report – upon cyber security industry trends and emergent technologies and key skill shortages Assignment 2 Essay – upon professional development, personal reflection upon developing CS skills sets	50% 50% 100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns-Dyer Date: 04 September 2024	**Approved by**:

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: TRUR1194	**MODULE TITLE: Work Practice Case Study**	
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)*
Students studying this module will undertake an investigation/research and will include work practice case studies relating to the Cyber Security Industry. By using these case studies, emphasis is placed upon the learner in developing a "working knowledge" of practice .

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	70%	**P1** (Practical**)**	30%
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop an understanding of the basics of industry working practices.
- To develop skills in the use of research, reasoning and application of knowledge.
- To devise solutions to work practice problems through case studies addressing both employer and employee issues

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Evaluate a range of case study scenarios and advise upon solutions and responses appropriate for the stated problems.	8.1.1, 8.2.1, 8.3.1, 8.4.2
2. Demonstrate and describe the understanding of industry practice and working practice.	8.2.1, 8.2.2, 8.3.1
3. Describe an appropriate response to a set brief using an imaginative and creative approach.	8.2.2, 8.3.1, 8.5.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-19	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 1

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 used in the KIS return and published on the extranet 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: Dave Cook

OTHER MODULE STAFF: Naomi Johns-Dyer, Dave Cook, John Glazebrook, Richard Morris, Paul Smith

Summary of Module Content

Students studying this module will investigate and research work and industry practice, through case studies and producing reports communicating solutions to industry and working practices, learning about problems faced in industry, including ethics, personal experiences, legal implications and producing standalone solutions and responses appropriate to the problems posed in the case studies.

SUMMARY OF TEACHING AND LEARNING ***[Use HESA KIS definitions]***		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecture	15	Lectures, investigations. (FA)
Practical Classes	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided Independent Study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Assignment 1 Academic Poster – based upon research of current working practices.	100%
Practical	Presentation Based upon case study – covering legalities, ethics proposing standalone solutions appropriate to case study.	100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Like for like	100%
Practical	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns-Dyer Date: 04 September 2024	**Approved by**:

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: TRUR1195	**MODULE TITLE: Security Programming**	
CREDITS: 20	**FHEQ LEVEL:** 4	**HECoS CODE:**100956 programming
PRE-REQUISITES: None	**CO-REQUISITES:** None	**COMPENSATABLE:** Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
Students studying this module will learn both the fundamentals of programming and the deeper and more complex issues of programming in relation to Cyber Security, concepts including web programming & scripting, application programming, socket programming, developing skills in its use, and evaluating the importance of programming from a cyber-security perspective.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical**)**	
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop basic understanding of program design.
- To develop programming skills through the use of a range of programs in both Command Line and GUI interfaces.
- To design and implement programs/scripts as solutions to address a range of security concepts.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Develop simple programs for a range of scenarios / tasks.	8.1.2, 8.3.1, 8.4.1, 8.5.1
2. Evaluate different programs solutions to computer security problems.	8.2.1, 8.4.1, 8.5.1
3. Design, implement programs/scripts to interrogate a range of IT system environments.	8.3.1, 8.4.1
4. Report upon system security for a designated network/system using programs/scripts.	

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-19	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 1 & 2

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 used in the KIS return and published on the extranet 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: John Glazebrook

OTHER MODULE STAFF: Naomi Johns-Dyer, Richard Morris

Summary of Module Content

Students studying this module will learn the fundamentals of programming and the deeper and more complex issues of programming in relation to Cyber Security, concepts include web programming & scripting, application programming, socket programming, BASH as well as a range of structured OOP elements. Developing practical skills in its use, and evaluating the importance of programming within a cyber-security perspective.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecturer	15	Lectures, investigations. (FA)
Practical classes and workshops	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided Study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Report – upon practical programming problems based upon work related scenarios Assignment 2 Report – based upon web application security programming practical	50% 50% 100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns-Dyer Date: 04 September 2024	**Approved by**:

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: TRUR1269	**MODULE TITLE: Networking & Systems**	
CREDITS: 20	**FHEQ LEVEL:** 4	**HECoS CODE:** 100365 computer networks
PRE-REQUISITES: None	**CO-REQUISITES:** None	**COMPENSATABLE:** Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module introduces students to the foundation topic underlying the design, implementation operation and structure of both networks, systems and their components. Issues such as installation configuration, maintenance and security will be addressed.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical)	
T1 (In-Class Test)		**O1** (online open book assessment)	50%		

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop an understanding of the basic concepts underlying computer networks and computer systems.
- To describe communication principles, protocols, transmission techniques, system components and structure.
- Develop knowledge of skills relevant to design, implementation, configuration of systems and networks.
- Investigate computer and networked systems problems and suitable solutions

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Describe the relevance of the OSI/TCP/IP models and its relevance to networks.	8.1.2
2. Produce, plan, and evaluate implementation of systems and networks for a given purpose.	8.2.2, 8.4.1, 8.5.1
3. Report on problems encountered with networks and systems, advise on appropriate solutions.	8.1.2, 8.3.2, 8.4.1, 8.5.1, 8.5.2
4. Explain the function and operation of systems and protocols.	8.2.2, 8.3.2, 8.5.2

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-19	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: Feb-22	**SEMESTER:** Semester 1 & 2

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 used in the KIS return and published on the extranet 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: Naomi Johns-Dyer

OTHER MODULE STAFF: Naomi Johns-Dyer, Dave Cook, John Glazebrook, Richard Morris, Paul Smith

Summary of Module Content

An understanding of the operation, structure of computer systems are necessary for their effective use. Today's ubiquitous computing world everything is connected and networks are vital part of modern computer systems. This module introduces the theory, practice of networked systems through a range of activities from design, configuration, implementation and trouble-shooting. Both performance and network security methods are studied using a mixture of virtual and physical technologies.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecture	15	Lectures, investigations. (FA)
Practical Classes and workshops	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided Independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Report – based upon practical activity of work based scenarios of networking and systems	100%
Online Assessment	Online Open Book Assessment	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%
Online Assessment	Online Open Book Assessment	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns-Dyer Date: 04 September 2024	**Approved by**:

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: TRUR1197	**MODULE TITLE: Server Administration & Systems Compliance**	
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)*
Students undertaking this module will develop an understanding of a range of networked services that support modern business platforms. Students will learn how to install, configure, maintain, monitor and evaluate these platforms, systems and services within a LAN environment. Students will investigate and document various security protocols and policies for effective, secure and compliant usage.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical**)**	
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To investigate both theoretical and practical aspects of networked services.
- Develop skills in network management including the implementation and monitoring of servers, networks, and communications.
- Develop practical skills and understanding of monitoring, fault-tracing and managing network usage, archiving and back-up strategies.
- Demonstrate an understanding of process relating to governance of user and corporate activities and compliance.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Demonstrate and assess processes for installing & configuring a range of networked services.	8.1.1, 8.1.2
2. Identify and evaluate, the processes of routine network management activities.	8.3.1
3. Demonstrate and compare the use of a range of monitoring and network analysis techniques.	8.1.1, 8.1.2, 8.2.1, 8.4.1
4. Evaluate tools used for networked services and systems compliance.	8.2.1, 8.5.2

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-19	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 2

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 used in the KIS return and published on the extranet 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: Dave Cook

OTHER MODULE STAFF: Naomi Johns-Dyer, Dave Cook, John Glazebrook, Richard Morris, Paul Smith

Summary of Module Content

This module gives the student opportunity to investigate the range and use, both theoretically and practically, of a range of networked service platforms relevant to modern business. The module explores the choice, installation configuration, monitoring and evaluation of services, platforms, systems and users whilst maintaining the CIA triad. Students will have the opportunity to investigate and use a variety of service platforms, and tools which includes:- Windows Server, Linux Server, IAS, Active Directory, Solar Winds, Nagios and IDS. Students will also investigate the role that policies, laws, ethics and legislation play in the governance and compliance of computing and data networks.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecturer	15	Lectures, investigations. (FA)
Practical classes and workshops	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Assignment 1 Report – upon practical activities based upon work related scenario including server deployment, configuration, administration and policies	50%
	Assignment 2 Essay – evaluating tools & processes of routine network management and systems compliance	50% 100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns-Dyer Date: 04 September 2024	**Approved by**:

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: TRUR1198	**MODULE TITLE: Behavioural Analytics & Data Security**	
CREDITS: 20	**FHEQ LEVEL:** 4	**HECoS CODE:** 100963 knowledge and information systems
PRE-REQUISITES: None	**CO-REQUISITES:** None	**COMPENSATABLE:** Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module introduces students to the concept of behavioural analytics. The students investigate both through theory and practical activity the actions of people and how (BA) is used to identify opportunities for both positive and negative areas of computing, the investigation will see students profiling users and network activity and identify areas for security optimisation in relation to the CIA triad.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	70%	**P1** (Practical**)**	30%
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop an understanding of the basic principles of Human Behavioural Analytics
- To develop analytical skills in relation to identifying trends and synthesising of data.
- Apply Behavioural Analytic Data to establish patterns and identify risks in Data Security.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Evaluate the use of Behavioural Analytics within the cyber security industry.	8.1.1, 8.1.2, 8.2.2
2. Analyse and compare data to identify trends in computer and network operations.	8.1.1
3. Demonstrate and apply understanding of Data Analysis and comment upon findings to identify risks to Data and Information Security.	8.1.1, 8.1.2, 8.3.2, 8.5.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-19	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 2

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 used in the KIS return and published on the extranet 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: Naomi Johns-Dyer

OTHER MODULE STAFF: Naomi Johns-Dyer, Dave Cook, John Glazebrook, Richard Morris, Paul Smith

Summary of Module Content

This module introduces students to the concepts of behavioural analytics. The students investigate both through theory and practical activity the actions of people and how (BA) is used to identify opportunities for both positive and negative areas of computing. The investigation will see students profiling users and attacks, and understanding how "traffic pattern analysis" affects data security analysing data from current trends and network activity and identify areas for security optimisation in relation to the CIA triad.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecturer	15	Lectures, investigations. (FA)
Practical classes and workshops	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Poster – evaluation upon the use of data analytics within the Cyber Security industry	100%
Practical	Presentation – based upon the practical WRL scenario and datasets identifying risks to CIA triad	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%
Practical	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns-Dyer Date: 04 September 2024	**Approved by**:

Level 5 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: TRUR2188	**MODULE TITLE: Risk Management & Disaster Recovery Planning**	
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 investigates the CIA triad, its importance to Cyber Security in business and industry. Students will, through means of case studies, practical's and exploring theory, understand and develop IT risk management strategies and disaster recovery planning.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical**)**	
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop knowledge of various risk management tools and strategies for a range of scenarios to provide solutions to manage and mitigate risks to Organisational IT.
- To develop an understanding of the CIA triad and its relevance to industry.
- To develop and apply knowledge of disaster recovery strategies.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Investigate and evaluate the appropriate tools for organisational risk management.	8.3.3
2. Apply knowledge of potential IT threats and report upon management and mitigation strategies.	8.2.3, 8.3.3
3. Apply understanding and critically evaluate methods of IT disaster recovery planning	8.4.2, 8.4.3, 8.5.4

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-20	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 1

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 used in the KIS return and published on the extranet 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: Clint Washington

OTHER MODULE STAFF: John Glazebrook, Naomi Johns, Dave Cook

Summary of Module Content

This module introduces the students to the process of identifying, quantifying and mitigating risks within an Organisational IT Security context. Students will investigate the relevance of the CIA triad, carry out detailed examinations of a range of threats to medium sized enterprises IT systems and networks. Opportunities to develop practical skills in using various tools to plan, document, mitigate and recover from a range of potential threats.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecture	20	Lectures, investigations. (FA)
Practical sessions and workshops	25	Training, practical tasks, guest speakers, planning careers. (FA)
Guided Independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Report – upon WBL scenario based upon risk identification, management and tools Assignment 2 Essay – evaluation of disaster recovery planning	50% 50% 100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns Date: September 2022	**Approved by**: K McCoag Date: September 2022

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: TRUR2267	**MODULE TITLE: Digital Forensics**	
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 introduces students to the detection, diagnosis, prevention and reporting of attacks on computer systems and networks. Students will have the opportunity to undertake Digital Forensics Investigation.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical**)**	
T1 (Test)		**O1** (online open book assessment)	50%		

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop a knowledge of how to use diagnostic tools in a range of situations to assess the potential threats to computer systems.
- To develop an understanding of how to counter attacks from both a theoretical and practical aspect.
- To develop an understanding of the concepts and principles of a Cyber Crime Investigation.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Investigate and evaluate the appropriate tool(s) for diagnosing problems in a range of different computer systems;	8.5.3
2. Apply understanding of potential threats to track, log and report user activity on a computer system;	8.2.3, 8.2.4
3. Apply and evaluate the principles of a cybercrime investigation.	8.4.3, 8.5.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-20	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: Feb-22	**SEMESTER:** Semester 2

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 used in the KIS return and published on the extranet 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: Clint Washington

OTHER MODULE STAFF: Naomi Johns, John Glazebrook, Dave Cook

Summary of Module Content

This module introduces students to the detection, diagnosis, prevention and reporting of attacks on computer systems and networks. Students will have the opportunity to undertake Digital Forensics Investigation.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecturer	15	Lectures, investigations. (FA)
Practical classes and workshops	30	Training, practical tasks, guest speakers, planning careers. (FA)
Guided independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Assignment 1 Report – on the work based simulation practical - forensic investigation which covers the choice of tools, principles and cybercrime report.	100%
Online Assessment	Online Open Book Assessment	100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Like for like	100%
Online Assessment	Online Open Book Assessment	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns Date: September 2022	**Approved by**: K McCoag Date: September 2022

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: TRUR2190	**MODULE TITLE: Work Placement & Current Issues**	
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 provides students with experience, knowledge and understanding of the working environment and current issues facing todays IT professional. It will provide practical knowledge of working practices, ethical, social responsibilities, processes and legal aspects associated with an IT professional.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	70%	**P1** (Practical**)**	30%
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop knowledge and understanding of the working environment of an IT professional.
- To develop analytical skills and evaluate IT professionals working practices, responsibilities and socio-ethical aspects of working IT professional.
- To gain practical skills by undertaking a meaningful (computing) work placement.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Demonstrate analytical knowledge of working practices of IT professional through work placement.	8.1.3, 8.2.4, 8.3.4
2. Analyse and evaluate the role and function of legislation, codes of conduct, and codes of ethics within the IT profession.	8.1.3, 8.4.2
3. Report upon the working of, legal and social responsibilities of an IT professional in practice.	8.4.4, 8.5.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-20	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 1 & 2

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 used in the KIS return and published on the extranet 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: John Glazebrook

OTHER MODULE STAFF: Clint Washington, Naomi Johns, Dave Cook

Summary of Module Content

This module provides students with IT working experience, gaining practical knowledge and understanding of the modern IT working environment, including current issues facing today's IT professional. The module also explores through both working practice and theory social, ethical and legal responsibilities of the IT practitioner the practical element through the form of work placements.

SUMMARY OF TEACHING AND LEARNING ***[Use HESA KIS definitions]***		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecturers	15	Lectures, investigations. (FA)
Seminars	15	Training, practical tasks, guest speakers, planning careers. (FA)
Work Placement	100	Work experience (evidence of experience portfolio)
Guided independent study	70	Guided Study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Assignment Essay - based upon current issues including socio ethical, legal responsibilities and working practice coupled with submission of a log of hours (Work Experience Portfolio)	100%
Practical	Presentation Presentation upon work experience, which includes evaluation of IT in the workplace, this presentation should include a self-reflection of their work placement performance (Work Experience Portfolio).	100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Like for like	100%
Practical	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns Date: September 2022	**Approved by**: K McCoag Date: September 2022

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: TRUR2268	**MODULE TITLE: Network Security & Design**	
CREDITS: 20	**FHEQ LEVEL:** 5	**HECoS CODE:100365**
PRE-REQUISITES: None	**CO-REQUISITES:** None	**COMPENSATABLE:** Yes

SHORT MODULE DESCRIPTOR: *(max 425 characters)*
This module introduces students to the planning, design and implementation of modern secure computer networks including investigation into the detection, prevention and reporting of various security threats faced by modern industry.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	50%	**P1** (Practical**)**	
T1 (Test)		**O1** (online open book assessment)	50%		

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To develop the knowledge and practical skills required for the planning, design, configuration and implementation of secure data networks.
- To develop an understanding of the common methods of securing networked systems, the understanding of log files and analysis of corresponding data.
- Develop a knowledge of how to mitigate various data network threats from a theoretical and practical understanding.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Demonstrate knowledge and report upon the planning, design, configuration and implementation of secure networks.	8.3.3, ,8.4.2, 8.4.3 8.4.4
2. Critically evaluate the appropriate tools and methodology for securing networked systems.	
3. Evaluate the potential threats to networks, track, log and report upon networked activity.	8.3.3, 8.4.2, 8.4.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-20	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: Feb-22	**SEMESTER:** Semester 1

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 used in the KIS return and published on the extranet 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: Clint Washington

OTHER MODULE STAFF: Naomi Johns, John Glazebrook, Dave Cook

Summary of Module Content

This module introduces students to the planning, design, and implementation of secure modern computer networks. Including; investigation into the detection, prevention and reporting of various security threats faced by modern business and industry. Opportunities to develop practical skills in using detection tools, auditing and penetration tools and analysing findings and providing counter measures are to be used to support the theoretical parts of the module.

SUMMARY OF TEACHING AND LEARNING ***[Use HESA KIS definitions]***		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecture	20	Lectures, investigations. (FA)
Practical sessions and workshops	25	Training, practical tasks, guest speakers, planning careers. (FA)
Guided independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Report – evaluation based upon the practical scenario of designing, implementing and configuring a secure network against a range of threats.	100%
Online Assessment	Online Open Book Assessment	100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%
Online Assessment	Online Open Book Assessment	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns Date: September 2022	**Approved by**: K McCoag Date: September 2022

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: TRUR2192	**MODULE TITLE: Security Technology & Applied Cryptography**	
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)*
Students will be introduced to various security technologies available to both maintain and keep secure systems and networks. Students will investigate and explore basic cryptographic methods used in data and data communications. Students will have the opportunity of applying both theoretical and practical aspects during this module.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	100%	**P1** (Practical**)**	
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- Investigate and develop a deep knowledge of current security technologies.
- Apply knowledge and understanding to provide solutions to IT security problems posed.
- To be able to determine cryptographic concepts, their importance and application within industry.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Compare and contrast current security technology trends.	8.1.3, 8.2.4, 8.3.4, 8.4.3
2. Apply knowledge to a range of IT Security problems posed and report upon IT security solutions.	8.2.3
3. Analyse and evaluate cryptographic concepts to a range of security issues.	8.4.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-20	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 2

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 used in the KIS return and published on the extranet 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: Naomi Johns

OTHER MODULE STAFF: Clint Washington, John Glazebrook, Dave Cook

Summary of Module Content

Students will be introduced to various security technologies available to both maintain and keep secure systems and networks. Students will investigate and explore basic cryptographic methods used in data and data communications including PKI, Web of Trust, Digital Signatures and hashes. Students will have the opportunity of applying both theoretical and practical aspects during this module.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lectures	20	Lectures, investigations. (FA)
Practical sessions and workshops	25	Training, practical tasks, guest speakers, planning careers. (FA)
Guided independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Assignment 1 Poster – based upon case study, evaluation of current security technology trends and cryptographic concepts in use. Assignment 2 Report – based upon the practical, range of IT Security problems posed and producing IT security solutions.	50% 50% 100%

REFERRAL ASSESSMENT

Element Category	**Component Name**	**Component Weighting**
Coursework	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns Date: September 2022	**Approved by**: K McCoag Date: September 2022

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: TRUR2193	**MODULE TITLE: System Development 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 module aims to teach methods of planning, implementation and managing a project as it progresses through its life cycle. This is a group based project, allowing student groups to follow their own Cyber Security interests after being approved for suitability of project by the course team.

ELEMENTS OF ASSESSMENT *[Use HESA KIS definitions] – see Definitions of Elements and Components of Assessment*					
E1 (Examination)		**C1** (Coursework)	70%	**P1** (Practical**)**	30%
T1 (Test)					

SUBJECT ASSESSMENT PANEL to which module should be linked: Computing

Professional body minimum pass mark requirement: N/A

MODULE AIMS:

- To introduce the tools and techniques for the design, implementation and management of a medium sized project through viable methodology.
- Develop understanding of various project management strategies and tools.

ASSESSED LEARNING OUTCOMES: (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	**Award/ Programme Learning Outcomes contributed to**
1. Demonstrate analytical understanding of the principles and practices of project management.	8.1.3, 8.2.4
2. Apply knowledge and understanding of project management.	8.4.2
3. Evaluate project management practices, analyse design, plan and implement solutions to specific problems involving Cyber Security.	8.3.3, 8.4.3, 8.5.4
4. Evaluate the issues of working in a multi-discipline project group.	8.3.3, 8.3.4, 8.5.3

DATE OF APPROVAL: Apr-19	**FACULTY/OFFICE:** Academic Partnerships
DATE OF IMPLEMENTATION: Sep-20	**SCHOOL/PARTNER:** Truro and Penwith College
DATE(S) OF APPROVED CHANGE: N/A	**SEMESTER:** Semester 1 & 2

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 used in the KIS return and published on the extranet 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: Naomi Johns

OTHER MODULE STAFF: Clint Washington, John Glazebrook, Dave Cook

Summary of Module Content

The module provides students the opportunity to explore techniques used in the management of computer security related projects. Traditional and agile methodologies are introduced giving students the opportunities to compare and evaluate them. The group project will provide both context in-which students can develop technical and democratic processes, analytical and reasoning skills alongside experiencing their chosen project strategy.

SUMMARY OF TEACHING AND LEARNING *[Use HESA KIS definitions]*		
Scheduled Activities	**Hours**	**Comments/Additional Information (briefly explain activities, including formative assessment opportunities)**
Lecture	20	Lectures, investigations. (FA)
Project supervision	25	Training, practical tasks, guest speakers, planning careers. (FA)
Guided and independent study	155	Guided study
Total	**200**	**(NB: 1 credit = 10 hours of learning; 10 credits = 100 hours, etc.)**

SUMMATIVE ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	1 - Report – based upon the students group project – including evaluation of design, implementation, research, development, performance and management of the project. (3 parts to the report – 1, group project documentation, 2, peer review assessment, 3, individual evaluation)	100%
Practical	Project Presentation Individual project presentation (viva)	100%

REFERRAL ASSESSMENT

Element Category	Component Name	Component Weighting
Coursework	Like for like	100%
Practical	Like for like	100%

To be completed when presented for Minor Change approval and/or annually updated	
Updated by: Naomi Johns Date: September 2022	**Approved by**: K McCoag Date: September 2022