Programme specification

(Notes on how to complete this template are provide in Annexe 3)

1. Overview/ factual information

Programme/award title(s)	a. BSc (Honours) in Cybersecurity and Networks b. BSc in Cybersecurity and Networks c. Diploma of Higher Education in Cybersecurity and Networks d. Certificate of Higher Education in Cybersecurity and Networks
Teaching Institution	Deree – The American College of Greece
Awarding Institution	The Open University (OU)
Date of first OU validation	July 2020
Date of latest OU (re)validation	
Next revalidation	
Credit points for the award	360
UCAS Code	
HECoS Code	
LDCS Code (FE Colleges)	
Programme start date and cycle of starts if appropriate.	September 2020
Underpinning QAA subject benchmark(s)	Computing
Other external and internal reference points used to inform programme outcomes.	None
Professional/statutory recognition	
For apprenticeships fully or partially integrated Assessment.	
Mode(s) of Study (PT, FT, DL, Mix of DL & Face-to-Face) Apprenticeship	
Duration of the programme for each mode of study	FT - 3 year
Dual accreditation (if applicable)	NECHE Accredited
Date of production/revision of this specification	June 2020

Please note: This specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if s/he takes full advantage of the learning opportunities that are provided.

More detailed information on the learning outcomes, content, and teaching, learning and assessment methods of each module can be found in student module guide(s) and the students handbook.

The accuracy of the information contained in this document is reviewed by the University and may be verified by the Quality Assurance Agency for Higher Education.

2.1 Educational aims and objectives

In congruence with the mission statements of the College and the School of Liberal Arts and Sciences, the B.Sc. in Cybersecurity and Networks aims to provide students with the theoretical background and the practical skills in fixed and mobile telecommunication protocols and infrastructure, cryptography, network security requirements and standards, secure software design, policy making and implementation in multiple contexts.

Programme goals

Goal 1: Integrate state-of-the-art research into classroom teaching.

Goal 2: Prepare graduates for further studies in Cybersecurity and Networks disciplines.

Goal 3: Prepare graduates for professional certifications in Cybersecurity and Networks.

Goal 4: Prepare graduates for careers in Cybersecurity and Networks, such as, network & security administrator, architect, engineer, security software developer, information security officer, forensics analyst, data protection officer, information systems auditor, vulnerability assessor, penetration tester.

Programme Competencies

Cyber Security and Networks program graduates should be able to:
1. Critically evaluate cybersecurity threats, associated risks and implications, and devise appropriate counter measures for ICT and cyber-physical systems
2. Assess and design cybersecurity operational and risk management policies according to current ethical and legal standards
3. Design and apply cryptographic and cryptanalytic techniques for data protection purposes
4. Critically evaluate best practices to design and develop secure software
5. Apply forensic engineering principles when conducting a security incident investigation
6. Implement end-to-end security in fixed/wireline and mobile/wireless networks.

Program Learning Outcomes (PLOs)

A. *Knowledge and Understanding*
   A1. Demonstrate knowledge and understanding of current cybersecurity and networking technologies.
   A2. Demonstrate understanding of the ethical, legal, and policy issues related to

cybersecurity approaches and professional practice.

A3. Demonstrate knowledge of networking and cybersecurity industry standards.

A4. Demonstrate knowledge of theory and tools relevant to ethical hacking, penetration testing, and digital forensics methodologies.

A5. Demonstrate knowledge of emergent networking and cybersecurity technologies.

B. *Cognitive Skills*

B1. Discuss social, ethical, and legal issues related to the impact of information technology in the context of cybersecurity.

B2. Apply appropriate design and problem-solving techniques within the cybersecurity domain.

B3. Critically assess the cybersecurity resilience of an organization and design cybersecurity policy based on current standards.

B4. Conduct field research and in-depth investigation related to the development of a networking and cybersecurity solution.

C. *Practical and Professional Skills*

C1. Communicate using appropriate and relevant language and terminology to reach a wide range of different audiences on networking and cybersecurity subjects.

C2. Use design, production, and programming tools relevant to cybersecurity in associated areas.

C3. Structure and write reports on various aspects of networking and cybersecurity domains

C4. Structure and write in-depth technical reports detailing the concept, design and development of a product or policy relevant to cybersecurity and networking.

C5. Model security solutions for wireline and wireless networks.

D. *Key/Transferable Skills*

D1. Demonstrate personal and time management skills appropriate to professional conduct.

D2. Possess the oral and written communication skills to work successfully in a professional environment.

D3. Demonstrate ability to work effectively as part of a group.

D4. Demonstrate ability to learn independently and reflect on one's own learning needs and achievements.

D5. Demonstrate problem-solving skills and reflect on the process of development of a product in the networking and cybersecurity industry.

2.2 Relationship to other programmes and awards

(Where the award is part of a hierarchy of awards/programmes, this section describes the articulation between them, opportunities for progression upon completion of the programme, and arrangements for bridging modules or induction)

This programme is part of a US bachelor's degree programme, awarded with a total of 121 US credits and consisting of 40 modules:

- 11 modules in Liberal Education
- 26 modules of Concentration

- 3 modules of Electives

LIBERAL EDUCATION-MISSION

A vital component of the undergraduate experience, the Liberal Education program prepares students to become globally engaged twenty-first century citizens with the knowledge, intellectual habits, practical skills, and socio-cultural sensibilities needed in a rapidly changing world. Liberal Education helps students develop essential competencies for success across disciplines and in life beyond college by cultivating open mindedness, tolerance, problem-solving ability, intellectual curiosity and creativity. It also promotes thoughtful self-expression, an ethical compass, and responsibility to the local and global communities.

Deree-Liberal Education Program

Total	43
Core Modules	
Academic Writing (WP designated course)	3
Integrated Academic Writing & Ethics	3
Academic Writing, Research (WP 1212)	3
Mathematics (basic statistics, college algebra, OR higher)	3
Public speaking or professional communication or equivalent	3
Introduction to information systems or equivalent computer literacy course*	3
Any Natural Science with lab	4
Liberal Education electives (must meet at least 4 LE competencies)	3
LE designated course in STEM/Natural Sciences	3
LE designated course in Social Sciences	9
LE designated course in Humanities	6
LE designated course in Fine and Performing Arts	3
* May be fulfilled through appropriate academic evaluation	
LE designated course in Social Sciences and Humanities must come from at least two different principles	

Cybersecurity and Networks programme Liberal Education Program

Core Courses:	
WP 1010 Introduction to Academic Writing	3
WP 1111 Integrated Academic Writing and Ethics	3
WP 1212 Academic Writing and Research	3
MA 2010 Statistics I *or*	
MA 2021 Applied Statistics for Business *or*	3
MA 2025 Applied Statistics for Science	
SP 2300 Presentation Skills *or*	3
EN 3742 Professional Communication	
ITC 1070 Information Technology Fundamentals *	3
Any Natural Science with a lab	4

Liberal Education Electives:

LE designated course in STEM/Natural Sciences	3
LE designated courses in the Social and Behavioural Sciences (from more than one discipline)	9
PS 1001 LE Psychology as a Social Science (L4)	3
MG 3034 LE Managing People and Organizations	3
One additional course in Social and Behavioural Sciences	3
LE designated courses in Humanities (from more than one discipline)	6
PH 3005 LE Business Ethics (L5) *-or-* PH 3010 LE Ethics (L5)	3
One additional course in Humanities (except Philosophy courses)	3
LE designated course in Fine and Performing Arts	3

*May be fulfilled through appropriate academic evaluation

The programme also shares modules with the following programmes:

Module	Shared with
ITC 2088 Introduction to Programming (L4)	BSc in Information Technology
ITC 2193 Operating Systems Concepts (L4)	BSc in Information Technology
ITC 2186 Computer System Architecture (L4)	BSc in Information Technology
CS 2179 Business Information Systems (L4)	BSc in Management Information Systems
ITC 3006 Mathematics for Computing (L5)	BSc in Information Technology
ITC 3160 Fundamentals of RDBMS (L5)	BSc in Information Technology
ITC 4214 Internet Programming (L6)	BSc in Information Technology
ITC 3121 Computer Networks Modelling and Analysis (L5)	BSc in Information Technology (Network Technologies pathway - *on teach out*)
L5 ITC 3319 Network Administration (L5)	BSc in Information Technology (Network Technologies pathway - *on teach out*)
ITC 4426 Distributed Systems (L6)	BSc in Information Technology (Network Technologies pathway - *on teach out*)

2.3 For Foundation Degrees, please list where the 60-credit work-related learning takes place. For apprenticeships an articulation of how the work based learning and academic content are organised with the award.

N/A

2.4 List of all exit awards

Certificate of Higher Education in Cybersecurity and Networks

Diploma of Higher Education in Cybersecurity and Networks

BSc (Honours) in Cybersecurity and Networks

BSc in Cybersecurity and Networks

3. Programme structure and learning outcomes
(The structure for any part-time delivery should be presented separately in this section.)

Programme Structure - LEVEL 4					
Compulsory modules	**Credit points**	**Optional modules**	**Credit points**	**Is module compensable?**	**Semester runs in**
	120				
PS 1001 LE Psychology as a Social Science	15				
CS 2179 Business Information Systems	15				
ITC 20xx Computer Networks & Cybersecurity Fundamentals	15				
ITC 2088 Introduction to Programming	15				
ITC 2186 Computer System Architecture	15				
ITC 2193 Operating Systems Concepts	15				
ITC 2101 Principles of Wireless, IoT, and Mobile Networks	15				
ITC 2197 Object Oriented Programming Techniques	15				

Intended learning outcomes at Level 4 are listed below:

Learning Outcomes – LEVEL 4
3A. Knowledge and understanding

Learning outcomes:	Learning and teaching strategy/ assessment methods
	Learning and Teaching Strategy: In congruence with the Learning and Teaching strategy of the College, the following methods are used at **Level 4**: • Class lectures, interactive learning (class discussions, group work), exercises and practical problems solved in class. Active learning methods and a student-centred teaching approach are particularly encouraged. • Formative coursework is regularly assigned and discussed in class with students actively participating in the discussion. • Collaborative in-class assignments and discussions are assigned. • Laboratory practical sessions using various simulations tools as well as training and practice on data analysis tools. • Video Tutorials • Formative group-work assignments aiming at exposing students to team-work and cooperation are regularly assigned. • Blackboard online learning platform tools including discussion boards, blogs, Wikis and Journals are employed to facilitate learning and collaboration. At **Level 4**, student learning is guided by the teaching staff and provides the ground for students to blend theories in psychology and information systems with programming and networking practices to come up with a practical solution to a problem. Almost all modules will take part in the laboratory to facilitate real-time practice and application. At this level, students are exposed to group work projects through formative assessments and in class assignment. Assessment methods give students the opportunity to display knowledge and understanding and staff the opportunity to identify issues in either. Students get timely feedback (within 21 days) on their formative and summative assessments by their lecturer.

Learning Outcomes – LEVEL 4

3A. Knowledge and understanding

A1. Demonstrate knowledge and understanding of current cybersecurity and networking technologies.	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals** Computer communications systems components, models, operation, and applications. Networking standards, protocols and connectivity aspects. Local area networks design, implementation. Wide area networks, emerging technologies. Cybersecurity threats, measures and protocols. Cryptography basics. **ITC 2101 Principles of Wireless, IoT, and Mobile Networks** Signals in the time and frequency domains. Propagation of radio frequencies. Noise, large-scale path loss, small scale fading and multipath. Modulation techniques for mobile radio. Capacity of wireless channels. Error correction principles and techniques. Multiple access techniques (TDMA, CDMA, OFDM) and interference in wireless networks. Main subsystems of mobile telephony networks. Examples of existing wireless standards including IEEE 802.11 (WiFi), 3G, 4G. **Assessment Methods:** Student performance is assessed as follows:

		ITC 2024 *	ITC 21xx *
Coursework "diagnostic" - **formative**	0	Take-home short problems, quizzes	Take-home short problems, quizzes, independent readings
Coursework - **summative**	30	Short problems on protocols, network equipment and design.	Simulations of wireless signals and their properties
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)	Portfolio of student work and oral assessment (not eligible for 2nd marking)
In-class final examination (2-hours) comprehensive - **summative**	60	Short essay questions and problem-solving cases.	Short essay questions and problem-solving cases

* The final assessment tests all learning outcomes of this modules, therefore students pass the module if the average module grade is 40% or higher.

Learning Outcomes – LEVEL 4

3A. Knowledge and understanding

A2. *Demonstrate understanding of the ethical, legal, and policy issues related to cybersecurity approaches and professional practice.*	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above **CS 2179 Business Information Systems** Business information systems concepts, categories and trends. The strategic impact of information systems and technologies on business functions and decision-making process. Ethical and security issues. Global information systems concepts.

CS2179 Assessment Methods:

Coursework "diagnostic" - **formative**	0	Online assignments through Blackboard, case studies, computer lab assignments
Coursework - **summative**	30	Implementation of data analysis in business cases
Portfolio - **summative**	10	Portfolio of student work (not eligible for 2nd marking)
In-class final examination (2-hours) - **summative**	60	Answers to essay questions

A3. *Demonstrate knowledge of networking and cybersecurity industry standards.*	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above
A4. *Demonstrate knowledge of theory and tools relevant to ethical hacking, penetration testing, and digital forensics*	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2088 Introduction to Programming** Problem solving; problem analysis; top-down design of algorithms; implementation; testing and debugging techniques; documentation. Structured programming language constructs: data types, variables, constants, parameters, input and output, selection, iteration, file handling, arrays, elementary sorting and searching

Learning Outcomes – LEVEL 4

3A. Knowledge and understanding

methodologies.	algorithms. Modular programming.

ITC 2197 Object Oriented Programming Techniques
Object-oriented concepts and problem solving techniques. GUI components; event handling, collections framework and data structures, data persistence, performance and efficiency issues.

ITC 2186 Computer System Architecture
Computer architecture. Digital circuits and components. Types of data representation. Computer organizations and design. Logic design.

ITC 2193 Operating Systems Concepts
Operating system structures; functions and techniques; Performance; avoidance of deadlock and security issues. Management of Operating System resources and processes.

Assessment Methods:
Assessment methods give students the opportunity to display knowledge and understanding and staff the opportunity to identify issues in either. Students get timely feedback (within 21 days) on their formative test and midterm exam by their lecturer.

In **ITC2197 *,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Short programming exercises, online quizzes
In-class midterm examination (1 hour) - **summative**	30	Short programming problems and short essay questions
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Coursework (test all Loss) - **summative**	60	Progressive small-scale application

In **ITC2088, ITC2186** and **ITC2193**, student performance is assessed as follows:

		ITC 2088 *	ITC 2186*	ITC2193
Coursework "diagnostic" - **formative**	0	In-class and take-home short problems	In-class and take-home short problems, questions and math. problems	In-class and take-home short problems.
Coursework - **summative**	30	Programming problems	Design and implementation of a digital	Case problems

Learning Outcomes – LEVEL 4

3A. Knowledge and understanding

				circuit.
	Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)	Portfolio of student work and oral assessment (not eligible for 2nd marking)	Portfolio of student work and oral assessment (not eligible for 2nd marking)
	In-class final examination (2-hours) comprehensive - **summative**	60	Short programming problems.	Short essay questions and mathematical problems	combination of short essay questions and case problems

* The final assessment tests all learning outcomes of this modules, therefore students pass the module if the average module grade is 40% or higher.

A5. Demonstrate knowledge of emergent networking and cybersecurity technologies.

Where it is taught:

ITC 2024 Computer Networks & Cybersecurity Fundamentals - As described above

ITC 2101 Principles of Wireless, IoT, and Mobile Networks - As described above

3B. Cognitive skills

Learning outcomes:	Learning and teaching strategy/ assessment methods
B1. Discuss social, ethical, and legal issues related to the impact of information technology in the context of cybersecurity.	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above

3B. Cognitive skills	
	CS 2179 Business Information Systems - As described above
B2. Apply appropriate design and problem-solving techniques within the cybersecurity domain.	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1. Communicate using appropriate and relevant language and terminology to reach a wide range of different audiences on networking and cybersecurity subjects.	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above
C2. Use design, production, and programming tools relevant to cybersecurity in associated areas.	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above **ITC 2088 Introduction to Programming -** As described above **ITC 2197 Object Oriented Programming Techniques -** As described above **ITC 2186 Computer System Architecture -** As described above **ITC 2193 Operating Systems Concepts -** As described above

3C. Practical and professional skills	
C3. Structure and write reports on various aspects of networking and cybersecurity domains	**Where it is taught:** **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
D1. Demonstrate personal and time management skills appropriate to professional conduct.	**Where it is taught:** **CS 2179 Business Information Systems -** As described above **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above **ITC 2088 Introduction to Programming -** As described above **ITC 2197 Object Oriented Programming Techniques -** As described above **ITC 2186 Computer System Architecture -** As described above **ITC 2193 Operating Systems Concepts -** As described above
D2. Possess the oral and written communication skills to work successfully in a professional environment.	**Where it is taught:** **CS 2179 Business Information Systems -** As described above **ITC 2024 Computer Networks & Cybersecurity Fundamentals -** As described above **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above **ITC 2088 Introduction to Programming -** As described above **ITC 2197 Object Oriented Programming Techniques -** As described above

3D. Key/transferable skills	
	ITC 2186 Computer System Architecture - As described above
	ITC 2193 Operating Systems Concepts - As described above
	PS 1001 LE Psychology as a Social Science
	Overview of the field of psychology as a social science with emphasis on theoretical perspectives and research methods, life-span development, mental abilities, personality theory and assessment, stress and coping, psychological disorders and treatment, social behaviour.
	Assessment Methods:
	In **PS 1001,** student performance is assessed as follows:

In **PS 1001,** student performance is assessed as follows:

In-class, 1-hour, "diagnostic" test - **formative**	0	Multiple choices & short answer questions
In-class 1-hour midterm examination - **summative**	40	Multiple choices & short answer questions
In-class final examination (2-hours) - **summative**	60	Multiple choices & short answer questions

D3. Demonstrate ability to work effectively as part of a group.	**Where it is taught:** **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above **ITC 2197 Object Oriented Programming Techniques -** As described above
D4. Demonstrate ability to learn independently and reflect on one's own learning needs and achievements.	**Where it is taught:** **ITC 2101 Principles of Wireless, IoT, and Mobile Networks -** As described above **ITC 2197 Object Oriented Programming Techniques -** As described above

[Certificate of Higher Education in Cybersecurity and Networks]

Programme Structure - LEVEL 5					
Compulsory modules	**Credit points**	**Optional modules**	**Credit points**	**Is module compensatable?**	**Semester runs in**
	120				
PH 3005 LE Business Ethics *or* PH 3010 LE Ethics	15 15				
ITC/PH 3036 Privacy, Policy, Law and Technology	15 15				
ITC 3006 Mathematics for Computing	15				
ITC 3121 Computer Networks Modelling and Analysis	15 15				
ITC 3319 Network Administration	15				
ITC 3160 Fundamentals of RDBMS					
ITC 3431 Cryptography & Network Security					
ITC 3632 Security of Wireless, IoT, and Mobile Networks					

Intended learning outcomes at Level 5 are listed below:

Learning Outcomes – LEVEL 5
3A. Knowledge and understanding

Learning outcomes:	Learning and teaching strategy/ assessment methods
	Learning and Teaching Strategy: In congruence with the Learning and Teaching strategy of the College, the following methods are used at **Level 5**: • Class lectures, interactive learning (class discussions, group work), exercises and practical problems solved in class. Active learning methods and a student-centred teaching approach are particularly encouraged. • Formative coursework is regularly assigned and discussed in class with students actively participating in the discussion. • Collaborative in-class assignments and discussions are assigned. • Laboratory practical sessions using various simulations tools as well as training and practice on data analysis tools. • Video Tutorials • Formative and summative group-work assignments aiming at exposing students to team-work and cooperation are regularly assigned. • Blackboard online learning platform tools including discussion boards, blogs, Wikis and Journals are employed to facilitate learning and collaboration. At Level 5, student learning gradually becomes more independent through projects aiming at developing students' analytical and computational thinking. Students are exposed to all types of assessments including exams as well as individual and group projects. Assessment methods give students the opportunity to display knowledge and understanding and staff the opportunity to identify issues in either. Students get timely feedback (within 21 days) on their formative and summative assessments by their lecturer.

Learning Outcomes – LEVEL 5

3A. Knowledge and understanding

A1. Demonstrate knowledge and understanding of current cybersecurity and networking technologies.	**Where it is taught:** **ITC 3121 Computer Networks Modelling and Analysis** Data communications technologies. Computer network systems. Network convergence architectures. Connectivity and internetworking of LANs. **ITC 3319 Network Administration** Installation and administration concepts. Management, monitoring, and optimization of system performance, reliability, and availability. Design issues and support in a corporate environment. Troubleshooting and end user support. **ITC 3431 Cryptography & Network Security** Basic symmetric encryption algorithms; DES, AES; Public key encryption; hash functions; digital signatures; confidentiality issues; authentication and identity management; SSL/TLS; IP security. **ITC 3632 Security of Wireless, IoT, and Mobile Networks** Security challenges in wireless, mobile and IoT networks; Interference and jamming in wireless systems; 802.11 Authentication and Key Management; WEP, WAP functions, protocols and configurations for realizing authentication, key distribution, integrity, confidentiality and anonymity in wireless access networks for mobile users. Authentication and confidentiality in 4G mobile telephony systems. Identity and Access Management (IAM) for the Internet of Things. **Assessment Methods:** In **ITC3121 *,** student performance is assessed as follows:

In-class "diagnostic" test and coursework - **formative**	0	Short essay questions, case problems
In-class 1-hour midterm examination - **summative**	30	Short essay questions and case problems
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive -	60	Design and implementation of a small-scale network

summative		system

In **ITC3319 *,** student performance is assessed as follows:

In-class "diagnostic" test and coursework - **formative**	0	Short essay questions, case problems
In-class 1-hour midterm examination - **summative**	30	Short essay questions and case problems
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive - **summative**	60	Design a network solution for a given set of requirements

In **ITC 34xx** *student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home short problems, quizzes, project progress
Project *(group)* - **summative**	30	literature review, design, implementation (code, script or simulation)
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
In-class final examination (2-hours) comprehensive - **summative**	60	Short essay questions and case problems.

In **ITC36xx *,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home short problems
In-class 1-hour midterm examination - **summative**	30	Short essay questions and case problems.
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive - **summative**	60	literature review, design, implementation (code, script or simulation)

Learning Outcomes – LEVEL 5

3A. Knowledge and understanding

A2. Demonstrate understanding of the ethical, legal, and policy issues related to cybersecurity approaches and professional practice.	** The final assessment tests all learning outcomes of this modules, therefore students pass the module if the average module grade is 40% or higher.*

Where it is taught:

PH 3005 LE Business Ethics
Introduction to major theories and basic moral problems in the domain of business. The use of reasoning in moral
assessment of business practices. Application of moral theories to specific cases of corporate conduct ranging from the individual to society in general, in the local and the international context.
- or -
PH 3010 LE Ethics
Introduction to the basic problems and theories of moral philosophy. The use of reasoning in moral assessment of actions and persons. Emphasis on the connection between theory and practice by application of theories to issues that matter.

ITC/PH 3036 Privacy, Policy, Law and Technology
An examination of policy issues and theoretical frameworks to privacy and security. Privacy threat models and privacy protective technologies. Philosophical approaches and legal functions on information privacy. GDPR.

ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above

Assessment Methods:
In **PH3005** and **PH3010,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home assignments. Essay-type questions
In-class midterm examination (1 hour) - **summative**	30	Essay-type questions (choice: 1 out of 2)
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)

Learning Outcomes – LEVEL 5

3A. Knowledge and understanding

In-class final examination (2-hours) - **summative**	60	Essay-type questions (choice: 2 out of 4)

In **ITC 30xx,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	In-class or take-home diagnostic assignments
In-class midterm examination (1 hour) - **summative**	30	
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Research paper - **summative**	60	

A3. Demonstrate knowledge of networking and cybersecurity industry standards.

Where it is taught:

ITC 3121 Computer Networks Modelling and Analysis - As described above

ITC 3319 Network Administration - As described above

ITC 3431 Cryptography & Network Security - As described above

ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above

A4. Demonstrate knowledge of theory and tools relevant to ethical hacking, penetration testing, and digital forensics methodologies.

Where it is taught:

ITC 3431 Cryptography & Network Security - As described above

ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above

ITC 3160 Fundamentals of RDBMS
Relational Database Management Systems concepts. Data modelling, systems development and data administration in a database environment. The relational model, normalization, transaction management, concurrency, control, database security and the Structured Query Language (SQL).

Learning Outcomes – LEVEL 5

3A. Knowledge and understanding

ITC 3006 Mathematics for Computing
The course aims to expose students to a synthesis of algebra, logic, combinatorics, probabilities, graph theory, and machine learning topics. It provides students with the necessary mathematical background to address issues in ICT related areas

Assessment Methods:

In **ITC3160,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Programming problems, take-home "diagnostic" test
In-class 1-hour midterm examination - **summative**	30	SQL problems
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive - **summative**	60	Database application development

In **ITC 3006,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	In-class and take-home short problems.
In-class midterm examination (1 hour) - **summative**	30	Short answers to problems
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
In-class final examination (2-hours) comprehensive - **summative**	60	Short answers to problems

A5. Demonstrate knowledge of emergent networking

Where it is taught:

ITC 3121 Computer Networks Modelling and Analysis - As described above

Learning Outcomes – LEVEL 5

3A. Knowledge and understanding	
and cybersecurity technologies.	**ITC 3319 Network Administration -** As described above
	ITC 3431 Cryptography & Network Security - As described above
	ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
B1. Discuss social, ethical, and legal issues related to the impact of information technology in the context of cybersecurity.	**Where it is taught:** **PH 3005 LE Business Ethics - or - PH 3010 LE Ethics -** As described above **ITC/PH 3036 Privacy, Policy, Law and Technology -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above
B2. Apply appropriate design and problem-solving techniques within the cybersecurity domain.	**Where it is taught:** **ITC/PH 3036 Privacy, Policy, Law and Technology -** As described above **ITC 3121 Computer Networks Modelling and Analysis -** As described above **ITC 3319 Network Administration -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above
B3. Critically assess the cybersecurity resilience of an	**Where it is taught:** **ITC 3121 Computer Networks Modelling and Analysis -** As described above

3B. Cognitive skills	
organization and design cybersecurity policy based on current standards.	**ITC 3319 Network Administration -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1. Communicate using appropriate and relevant language and terminology to reach a wide range of different audiences on networking and cybersecurity subjects.	**Where it is taught:** **ITC/PH 3036 Privacy, Policy, Law and Technology -** As described above **ITC 3121 Computer Networks Modelling and Analysis -** As described above **ITC 3319 Network Administration -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above
C2. Use design, production, and programming tools relevant to cybersecurity in associated areas.	**Where it is taught:** **ITC 3121 Computer Networks Modelling and Analysis -** As described above **ITC 3319 Network Administration -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above **ITC 3006 Mathematics for Computing -** As described above **ITC 3160 Fundamentals of RDBMS -** As described above **Where it is taught:**

3C. Practical and professional skills	
C3. Structure and write reports on various aspects of networking and cybersecurity domains	**ITC 3121 Computer Networks Modelling and Analysis -** As described above **ITC 3319 Network Administration -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above
C4. Structure and write in-depth technical reports detailing the concept, design and development of a product or policy relevant to cybersecurity and networking.	**Where it is taught:** **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above
C5. Model security solutions for wireline and wireless networks.	**Where it is taught:** **ITC 3121 Computer Networks Modelling and Analysis -** As described above **ITC 3319 Network Administration -** As described above **ITC 3431 Cryptography & Network Security -** As described above **ITC 3632 Security of Wireless, IoT, and Mobile Networks -** As described above

3D. Key/transferable skills	
Learning outcomes:	Learning and teaching strategy/ assessment methods
D1. Demonstrate personal and time management skills appropriate to professional conduct.	**Where it is taught:** **ITC/PH 3036 Privacy, Policy, Law and Technology -** As described above **ITC 3006 Mathematics for Computing -** As described above **ITC 3160 Fundamentals of RDBMS -** As described above

3D. Key/transferable skills	
	ITC 3121 Computer Networks Modelling and Analysis - As described above
	ITC 3319 Network Administration - As described above
	ITC 3431 Cryptography & Network Security - As described above
	ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above
D2. Possess the oral and written communication skills to work successfully in a professional environment.	**Where it is taught:**
	PH 3005 LE Business Ethics *- or -* PH 3010 LE Ethics - As described above
	ITC/PH 3036 Privacy, Policy, Law and Technology - As described above
	ITC 3121 Computer Networks Modelling and Analysis - As described above
	ITC 3160 Fundamentals of RDBMS - As described above
	ITC 3319 Network Administration - As described above
	ITC 3431 Cryptography & Network Security - As described above
	ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above
D3. Demonstrate ability to work effectively as part of a group.	**Where it is taught:**
	ITC 3121 Computer Networks Modelling and Analysis - As described above
	ITC 3160 Fundamentals of RDBMS - As described above
	ITC 3319 Network Administration - As described above
	ITC 3431 Cryptography & Network Security - As described above
	ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above
D4. Demonstrate ability to learn independently	**Where it is taught:**
	PH 3005 LE Business Ethics *- or -* PH 3010 LE Ethics - As described above

3D. Key/transferable skills	
and reflect on one's own learning needs and achievements.	**ITC/PH 3036 Privacy, Policy, Law and Technology -** As described above
	ITC 3006 Mathematics for Computing - As described above
	ITC 3160 Fundamentals of RDBMS - As described above
	ITC 3121 Computer Networks Modelling and Analysis - As described above
	ITC 3319 Network Administration - As described above
	ITC 3431 Cryptography & Network Security - As described above
	ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above
D5. Demonstrate problem-solving skills and reflect on the process of development of a product in the networking and cybersecurity industry.	**Where it is taught:**
	PH 3005 LE Business Ethics *- or -* **PH 3010 LE Ethics -** As described above
	ITC/PH 3036 Privacy, Policy, Law and Technology - As described above
	ITC 3006 Mathematics for Computing - As described above
	ITC 3160 Fundamentals of RDBMS - As described above
	ITC 3121 Computer Networks Modelling and Analysis - As described above
	ITC 3319 Network Administration - As described above
	ITC 3431 Cryptography & Network Security - As described above
	ITC 3632 Security of Wireless, IoT, and Mobile Networks - As described above

[Diploma of Higher Education in Cybersecurity and Networks]

Programme Structure - LEVEL 6					
Compulsory modules	**Credit points**	**Optional modules**	**Credit points**	**Is module compensatable ?**	**Semester runs in**
	120				
ITC 4214 Internet Programming	15				
ITC 4344 Digital Forensics	15				
ITC 4446 Intrusion Detection and Incident Response	15				
	15				
ITC 4426 Distributed Systems	15				
ITC 4447 Secure Software Development	15				
ITC 4648 Ethical Hacking & Penetration Testing	15				
ITC 4140 Methods in ICT Project Research & Management	15				
ITC 4949 Cybersecurity and Networks Capstone					

Intended learning outcomes at Level 6 are listed below:

Learning Outcomes – LEVEL 6	
3A. Knowledge and understanding	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
	Learning and Teaching Strategy: In congruence with the Learning and Teaching strategy of the College, the following methods are used at **Level 6**: • Class lectures, interactive learning (class discussions, group work), exercises and practical problems solved in class. Active learning methods and a student-centred teaching approach are particularly encouraged. • Formative coursework is regularly assigned and discussed in class with students actively participating in the discussion. • Collaborative in-class assignments and discussions are assigned. • Laboratory practical sessions using various simulations tools as well as training and practice on data analysis tools. • Video Tutorials • Formative and summative group-work assignments aiming at exposing students to team-work and cooperation are regularly assigned. • Milestone submissions set to assist the students with their summative work in a progressive manner, cultivating their project and time management skills, while they receive formative feedback on selected components. • Progress meetings complement the milestone submissions; individual or group, they are held in order to monitor the progress of research/project assessments, provide formative feedback through discussion. • Blackboard online learning platform tools including discussion boards, blogs, Wikis and Journals are employed to facilitate learning and collaboration. **At level 6**, the programme focuses on modules with learning outcomes and teaching methods aiming to develop student's skills in managing cybersecurity related projects, so that they can deploy appropriate theory and tools for the specification, modelling, design, implementation and evaluation of systems. At this level, students will apply critical thinking and computational skills in an independent learning environment. Through the capstone project module students will integrate knowledge and apply cybersecurity-related

3A. Knowledge and understanding

<table>
<tr>
<td rowspan="2">A1. Demonstrate knowledge and understanding of current cybersecurity and networking technologies.</td>
<td>skills in order to manage the whole process involved in the effective deployment of computers to solve practical problems. The final deliverable of the capstone project modules is a small-scale computer-based system that aims to support the goals of a business firm or organisation.</td>
</tr>
<tr>
<td>

Where it is taught:

ITC 4344 Digital Forensics
Computer crime and the forensic investigation process; principles and practices; digital evidence on computer systems, hardware storage, the Internet, mobile devices. Computer forensics on data analysis; operating systems forensics; assisting cryptographic techniques; event timing; forensic disk imaging; data recovery; file reconstruction. Rules of evidence and standards; principles of evidential management; the expert witness; standards and ethics.

ITC 4446 Intrusion Detection and Incident Response
Intrusion prevention, detection, and response; defensive and offensive techniques and tools; network traffic analysis.

ITC 4426 Distributed Systems
Distributed systems principles; communication; processes; naming; synchronization; fault tolerance; security; consistency and replication; object-based systems; document-based systems; distributed file systems; coordination-based systems; payment systems; Internet and web protocols; scalability.

ITC 4447 Secure Software Development
Best practices for developing secure software; coding techniques for data validation, session management, exception handling, data encryption; configuration techniques. Mitigating security risk from external and internal sources.

ITC 4648 Ethical Hacking & Penetration Testing
Principles of ethical hacking and penetration testing using Kali Linux, Nessus, Metasploit Framework, and Tor. Reconnaissance/Footprinting, weaponization, privilege escalation, exfiltration. Scanning networks; enumeration; sniffing; vulnerability analysis. Denial-of-Service attacks; web apps hacking and patching; SQL injection & parameter binding. Buffer overflow attacks and defenses. Introduction to hacking wireless networks and IoT. Structured security testing aimed at finding focused security vulnerabilities, flaws, risks and unreliable environments.

</td>
</tr>
</table>

Learning Outcomes – LEVEL 6

3A. Knowledge and understanding

Assessment Methods:

In **ITC43xx *,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home short problems
In-class 1-hour midterm examination - **summative**	30	Short essay questions and case problems.
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive - **summative**	60	Investigation, collection and analysis of digital evidence, ethical and legal considerations of a real-world scenario

In **ITC44xx *** (Intrusion Detection & Incident Response), student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home short problems
In-class 1-hour midterm examination - **summative**	30	Short essay questions and case problems.
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive - **summative**	60	Situational incident response plan including attack tracing, evidence collection and evidence tracing

In **ITC 4426** *student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Individual and group case problems
In-class 1-hour midterm examination - **summative**	30	Short essay questions and case problems.
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Research project (individual) comprehensive - **summative**	60	Literature review/methodology/interpretation

Learning Outcomes – LEVEL 6

3A. Knowledge and understanding

In **ITC 44xx** (Secure SW Development), student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Individual and group case problems
In-class 1-hour midterm examination - **summative**	30	Short answers and case problems.
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (group) - **summative**	60	Design and assessment of secure SW policy for a given set of SW application requirements, including a programming implementation

In **ITC 46xx ,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home short problems, in-lab practice
In-class 1-hour midterm examination - **summative**	20	Short essay questions and case problems
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (group) - **summative**	70	Development of an ethical hacking procedure and recommendation of defence measures for a given set of conditions

* The final assessment tests all learning outcomes of this modules, therefore students pass the module if the average module grade is 40% or higher.

A2. Demonstrate understanding of the ethical, legal, and policy issues related to cybersecurity approaches and professional practice.

Where it is taught:

ITC 4344 Digital Forensics - As described above

ITC 4446 Intrusion Detection and Incident Response - As described above

ITC 4447 Secure Software Development - As described above

ITC 4648 Ethical Hacking & Penetration Testing - As described above

Learning Outcomes – LEVEL 6
3A. Knowledge and understanding

<table>
<tr><td rowspan="2"></td><td>

ITC 4140 Methods in ICT Project Research & Management

Integrated methods for ICT projects investigation and planning; problem identification; field review; selected investigative

techniques; modelling and evaluation techniques; testing strategies; quality considerations. A comprehensive coverage of the procedure required for the development of a thorough ICT capstone project proposal. Components of this procedure include: (a) identification of the problem; (b) background research (c) objectives and impact of the project; (d) project feasibility and risk assessment; (e) analysis; (f) testing and testing strategies, (g) quality considerations; (h) progress planning & management.

Assessment method:

In **ITC 41xx* ,** student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Take-home case problems
Project (group)- **summative**	20	Small-scale research project on selected topics including perspective, focused domain research, high-level analysis, cost estimation, risk analysis, testing
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive-**summative**	70	Preparation for the capstone project, including literature review and justification, analysis, preliminary design, methodology, risk assessment, testing strategy and quality considerations

* The final assessment tests all learning outcomes of this modules, therefore students pass the module if the average module grade is 40% or higher.

Where it is taught:

ITC 4344 Digital Forensics - As described above

ITC 4446 Intrusion Detection and Incident Response - As described above

ITC 4447 Secure Software Development - As described above
</td></tr>
<tr><td>

A3. Demonstrate knowledge of networking and cybersecurity industry standards.
</td></tr>
</table>

Learning Outcomes – LEVEL 6

3A. Knowledge and understanding

A4. Demonstrate knowledge of theory and tools relevant to ethical hacking, penetration testing, and digital forensics methodologies.	**ITC 4648 Ethical Hacking & Penetration Testing** - As described above **ITC 4140 Methods in ICT Project Research & Management** - As described above **Where it is taught:** **ITC 4344 Digital Forensics** - As described above **ITC 4446 Intrusion Detection and Incident Response** - As described above **ITC 4447 Secure Software Development** - As described above **ITC 4648 Ethical Hacking & Penetration Testing** - As described above **ITC 4214 Internet Programming** Internet standards and infrastructure. Client and server technologies. Rich Internet applications. Scripting Languages. Server-side programming. Frameworks. Security and privacy. **Assessment Method:** In **ITC 4214*** , student performance is assessed as follows:

In **ITC 4214*** , student performance is assessed as follows:

Coursework "diagnostic" - **formative**	0	Short programming exercises, online quizzes
In-class 1-hour midterm examination - **summative**	30	combination of short essay questions and case problems
Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Project (individual) comprehensive - **summative**	60	Rich internet application development

* The final assessment tests all learning outcomes of this modules, therefore students pass the module if the average module grade is 40% or higher.

Where it is taught:

ITC 4344 Digital Forensics - As described above

A5. Demonstrate knowledge of	

Learning Outcomes – LEVEL 6

3A. Knowledge and understanding

emergent networking and cybersecurity technologies.	**ITC 4446 Intrusion Detection and Incident Response -** As described above
	ITC 4447 Secure Software Development - As described above
	ITC 4648 Ethical Hacking & Penetration Testing - As described above
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4426 Distributed Systems - As described above
	ITC 4949 Cybersecurity and Networks Capstone Project Design, simulation/emulation, evaluation and testing of a cybersecurity solution or component applicable in a network device or part of a wireline or wireless network. Use of research results, networking and cybersecurity standards and solutions in order to produce publishable outcomes.
	Assessment Method: In **ITC 4949 ,** student performance is assessed as follows:

Portfolio - **summative**	10	Portfolio of student work and oral assessment (not eligible for 2nd marking)
Research project (individual) comprehensive- **summative**	90	Independent or part of an R&D program

3B. Cognitive skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
B1. Discuss social, ethical, and legal issues related to the impact of information technology in the context of cybersecurity.	**Where it is taught:** **ITC 4344 Digital Forensics -** As described above **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above

3B. Cognitive skills	
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4949 Cybersecurity and Networks Capstone Project - As described above
B2. Apply appropriate design and problem-solving techniques within the cybersecurity domain.	**Where it is taught:**
	ITC 4344 Digital Forensics - As described above
	ITC 4446 Intrusion Detection and Incident Response - As described above
	ITC 4447 Secure Software Development - As described above
	ITC 4426 Distributed Systems - As described above
	ITC 4648 Ethical Hacking & Penetration Testing - As described above
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4949 Cybersecurity and Networks Capstone - As described above
B3. Critically assess the cybersecurity resilience of an organization and design cybersecurity policy based on current standards.	**Where it is taught:**
	ITC 4344 Digital Forensics - As described above
	ITC 4447 Secure Software Development - As described above
	ITC 4446 Intrusion Detection and Incident Response - As described above
	ITC 4648 Ethical Hacking & Penetration Testing - As described above
	ITC 4949 Cybersecurity and Networks Capstone - As described above
B4. Conduct field research and in-depth investigation related to the development of a networking and cybersecurity solution.	**Where it is taught:**
	ITC 4344 Digital Forensics - As described above
	ITC 4426 Distributed Systems - As described above
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4949 Cybersecurity and Networks Capstone Project - As described above

3C. Practical and professional skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
C1. Communicate using appropriate and relevant language and terminology to reach a wide range of different audiences on networking and cybersecurity subjects.	**Where it is taught:** **ITC 4344 Digital Forensics -** As described above **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4426 Distributed Systems -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone Project -** As described above
C2. Use design, production, and programming tools relevant to cybersecurity in associated areas.	**Where it is taught:** **ITC 4214 Internet Programming -** As described above **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4426 Distributed Systems -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone -** As described above
C3. Structure and write reports on various aspects of networking and cybersecurity	**Where it is taught:** **ITC 4214 Internet Programming -** As described above **ITC 4344 Digital Forensics -** As described above

3C. Practical and professional skills	
domains	**ITC 4446 Intrusion Detection and Incident Response -** As described above
	ITC 4447 Secure Software Development - As described above
	ITC 4426 Distributed Systems - As described above
	ITC 4648 Ethical Hacking & Penetration Testing - As described above
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4949 Cybersecurity and Networks Capstone - As described above
C4. Structure and write in-depth technical reports detailing the concept, design and development of a product or policy relevant to cybersecurity and networking.	**Where it is taught:**
	ITC 4426 Distributed Systems - As described above
	ITC 4648 Ethical Hacking & Penetration Testing - As described above
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4949 Cybersecurity and Networks Capstone - As described above
C5. Model security solutions for wireline and wireless networks.	**Where it is taught:**
	ITC 4214 Internet Programming - As described above
	ITC 4446 Intrusion Detection and Incident Response - As described above
	ITC 4447 Secure Software Development - As described above
	ITC 4426 Distributed Systems - As described above
	ITC 4648 Ethical Hacking & Penetration Testing - As described above
	ITC 4140 Methods in ICT Project Research & Management - As described above
	ITC 4949 Cybersecurity and Networks Capstone - As described above

3C. Practical and professional skills		

3D. Key/transferable skills	
Learning outcomes:	**Learning and teaching strategy/ assessment methods**
D1. Demonstrate personal and time management skills appropriate to professional conduct.	**Where it is taught:** **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4426 Distributed Systems -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone -** As described above
D2. Possess the oral and written communication skills to work successfully in a professional environment.	**Where it is taught:** **ITC 4214 Internet Programming -** As described above **ITC 4344 Digital Forensics -** As described above **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4426 Distributed Systems -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone -** As described above

	3D. Key/transferable skills
D3. Demonstrate ability to work effectively as part of a group.	**Where it is taught:** **ITC 4214 Internet Programming -** As described above **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone -** As described above
D4. Demonstrate ability to learn independently and reflect on one's own learning needs and achievements.	**Where it is taught:** **ITC 4214 Internet Programming -** As described above **ITC 4344 Digital Forensics -** As described above **ITC 4446 Intrusion Detection and Incident Response -** As described above **ITC 4447 Secure Software Development -** As described above **ITC 4426 Distributed Systems -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone -** As described above
D5. Demonstrate problem-solving skills and reflect on the process of development of a product in the networking and cybersecurity	**Where it is taught:** **ITC 4447 Secure Software Development -** As described above **ITC 4648 Ethical Hacking & Penetration Testing -** As described above **ITC 4140 Methods in ICT Project Research & Management -** As described above **ITC 4949 Cybersecurity and Networks Capstone -** As described above

3D. Key/transferable skills	
industry.	

[BSc (Honours) in Cybersecurity and Networks]

[BSc in Cybersecurity and Networks]

4. Distinctive features of the programme structure

- **Where applicable, this section provides details on distinctive featurs such as:**
  - ➢ where in the structure above a professional/placement year fits in and how it may affect progression
  - ➢ any restrictions regarding the availability of elective modules
  - ➢ where in the programme structure students must make a choice of pathway/route
- **Additional considerations for apprenticeships:**
  - ➢ how the delivery of the academic award fits in with the wider apprenticeship
  - ➢ the integration of the 'on the job' and 'off the job' training
  - ➢ how the academic award fits within the assessment of the apprenticeship

The Cybersecurity and Networks programme has the following distinctive features:
1. It leads to the awarding of two degrees:
   a. A US BSc degree accredited by the US NECHE (New England Commission of Higher Education), and
   b. A UK BSc (Honors) validated by the UK Open University (OU).
2. It prepares students to sit for relevant certifications
3. It offers opportunities for practical and professional experience through research and internships (US degree).
4. It provides a student-centered learning environment that promotes the academic and personal development, broadens horizons, and builds confidence to become independent learners.
5. It exposes students to state-of-the art facilities and a unique campus environment.

5. Support for students and their learning.
(For apprenticeships this should include details of how student learning is supported in the workplace)

All new students participate in an orientation programme as they begin their first semester at the College. The orientation program is designed to introduce them to the campus, the academic system, College regulations and policies, and student life.

Student Success Center (SSC)

The Student Success Centre supports students by offering comprehensive, integrated services in the areas of academic advising, Open University validation issues, student records, registration, and payments in a one-stop area. The Centre is committed to providing students with consistent, high-quality service, both in person and through technology. The Student Success Centre aims to create the optimum conditions so that students can follow the path to academic success.

Students may visit the Student Success Centre to pay a bill, request a certificate, obtain a form, arrange to bring a visitor on campus, obtain their transcript, see an academic advisor, ask about OU validation, change a course, and obtain or replace their student ID.

The SSC web page has been set up to reflect the one-stop concept of the Centre and includes information from different departments. It may be accessed from the "Quick Links" on the ACG homepage (www.acg.edu) and it allows students to print forms or view the academic calendar, academic policies, final exams schedule, course schedule, graduation instructions, major requirements, frequently asked questions (FAQs), the e-mail directory, and financial aid and international student information. From the SSC web page students may choose to log on to the myACG portal, where they can print their personal course schedule and their unofficial transcript. To log on, students need to go to the SSC and get their PIN, which is private, should not be shared with anyone, and will be given to the students only if they have no obligations (business office, library, or academic advising).

Academic Advising

All students are assigned an academic advisor responsible for assisting them in gaining the greatest benefit from their educational experience at the College. Good academic advising is a vital part of the learning process and an integral part of the basic teaching function of the College. Effective academic advising provides specific aid to students in considering and completing academic programs, but it goes beyond mere course scheduling; it includes planning, decision-making, implementation, and evaluation of academic, personal, and career-related matters, and exploration. The College assigns all entering freshmen a First-Year advisor from the Office of Academic Advising. Thereafter, the advising programme is faculty-based and fosters personal contact between students and faculty. Department Heads and Programme Coordinators act as educational consultants.

New incoming students and continuing Deree-ACG students are required to consult every semester and during the announced advising period with an advisor at the Office of Academic Advising.

Advisors never make decisions for students. Their overriding objective is to assist students in developing the maturity required to make their own choices and to be responsible for the consequences of those choices.

Student Academic Support Services (SASS)

Student Academic Support Services (SASS) provides support to the learning of Deree students at the undergraduate and graduate level through a variety of approaches encouraging participatory learning. SASS learning facilitators recognize that individual qualities and efforts vary; therefore, facilitators adopt a learner-centred approach without undue interference in order to promote individual development and to respond to the needs of each student. The goal of SASS is to help students become insightful readers, effective critical thinkers, and independent learners.

Student Academic Support Services offers two major types of academic support:

1. One-on-one Sessions conducted on a one-on-one basis between a facilitator and a student. They are provided on a first-come-first-served basis and cover a wide range of college skills.
2. Group Sessions are of two kinds, both designed to emphasize direct interaction

between participants:

a. Academic-skills workshops are offered on demand. They may focus on sharpening a quantitative or qualitative skill for a course or help participants sharpen conversational skills in a foreign languages.

b. Study-skills workshops are offered regularly. They are designed to help participants improve a particular study skill, such as note-taking or exam preparation.

Disability and Learning Differences

The College Committee on Disability and Learning Differences monitors and recommends policies and procedures to benefit individuals with disabilities and learning differences. In addition, it makes recommendations in consultation with relevant academic departments/ areas regarding special assessments to be given by tutors to specific students with disability and/or learning differences.

The Committee proposes alternative assessment methods for specific students with disability and/or learning differences in consultation with relevant academic departments/ areas to ensure appropriateness of assessment method. The Committee is obliged to follow the advice of the department with regard to appropriateness and communicate with the Registrar about this. The Committee on Disability and Learning Differences submits the list of OU students with disabilities and learning difficulties and their approved alternative assessment methods to the OU Validation Office and Registrar.

6. Criteria for admission
(For apprenticeships this should include details of how the criteria will be used with employers who will be recruiting apprentices.)

The Admissions Process

To qualify for admission to the academic programs of the College, applicants must demonstrate that they possess the appropriate qualifications to enable them to be successful in the program of their choice. To this end, applicants must meet the following requirements:

The standard minimum entry requirement for the major's programme is the following: 14/20 in the Greek system, an overall average grade of C in the US system, or 24 and above in the International Baccalaureate or the equivalent of any other educational grading system. Applicants whose grades are between 11/20-13.99/20 or its equivalent, may be admitted to the College on a provisional basis.

Students admitted on a provisional basis will be required to fulfil the following conditions in order to be allowed to continue on their selected major after the completion of one academic year after their acceptance to Deree:

• Meet with an assigned advisor at the Academic Advising Office at least twice every month or whenever the advisor thinks it is necessary. The assigned advisor will monitor

the student progress very closely and may require that they seek academic help through the Student Academic Support Services.

• The number of modules students will be allowed to register for will be determined by their English language placement (see section "English Language Requirements"). However, in no case will they be allowed to register for a total of more than 2 modules if placed in EAP 1002 or for more than 4 modules if placed in WP 1010. Students with provisional status who are placed in

EAP 999, EAP 1000, EAP 1001 must first complete their English for Academic Purpose modules before they begin taking College level modules along with EAP 1002.

• Students who have successfully completed only the EAP sequence during their first academic year will be able to continue.

• Achieve a minimum cumulative average (CI) of at least 2.0 after one academic year.

• After the completion of one academic year on provisional status, students' performance will be reviewed by the Committee on Academic Standards and Policies (CASP), which will decide on student progression and/or new conditions.

• Students on provisional status are subject to the College probation policy (see section "Academic Probation").

The following is required for all freshmen applicants:

1. A completed application form.
2. A letter of recommendation from an academic teacher or professor.
3. An official secondary school transcript and an official copy of a secondary diploma, both legally certified.
4. A certified copy of their identity card for Greek citizens or a valid passport for non-Greek citizens.
5. An interview with an admissions counsellor.
6. Evidence of proficiency in English.

Evidence of Proficiency in English

All applicants must demonstrate proficiency in the English language either by taking the College's English Placement Test (EPT) or by submitting any evidence derived from one of the following tests:
Pearson test of Academic English (PTE Academic): 58 or greater
Michigan State University Certificate of Language Proficiency (MSU-CELP)
Michigan Proficiency Certificate
Cambridge Proficiency Certificate
Cambridge Advanced English (CAE) with Grade A only
International Baccalaureate Certificate*
International Baccalaureate Diploma
IELTS: (academic) 6.5 or above
SAT: 450 or above
ACT: 18 or above
TOEFL

(paper based): 567 or above
TOEFL (computer based): 227 or above
TOEFL (internet based): 87 or above
GCE higher level English: Grade C or greater
Oxford Online Placement Test: 99 or above

* With grade 4 and above in the English higher-level subject or at least an average of 12 in the higher level subjects.

Applicants presenting a TOEFL score should arrange to have the test results sent directly to the Office of Admissions by the Educational Testing Service (ETS). The College's Institution Code Number is 0925. TOEFL scores are valid for 2 years.

Students may also qualify to take WP 1010 by submitting evidence of fluency based on graduation from an English-speaking secondary school or programme.

The above listed grades qualify the student for placement directly into WP 1010. Applicants who do not qualify for WP 1010 but who otherwise show academic promise may be admitted

conditionally and placed in the English for Academic Purposes Program (see section "English Language Requirements").

---

7. Language of study
English

---

8. Information about non-OU standard assessment regulations (including PSRB requirements)
N/A

---

9. For apprenticeships in England End Point Assessment (EPA). *(Summary of the approved assessment plan and how the academic award fits within this and the EPA)*
N/A

10. Methods for evaluating and improving the quality and standards of teaching and learning.

Deree faculty comprises of experienced professionals active in their respective fields through their research, publications, think-tank work and other forms of professional engagement. Significant body of research has been garnered by Deree faculty in the fields of learning innovation and pedagogy. Recognizing the need of a structured holistic approach to teaching and learning, over the past years, Deree has been implementing a variety of initiatives aimed at boosting the faculty's teaching excellence geared toward maintaining high standards and their comparability across sections, modules, and schools. An important component of this strategy was driven by the recognition that new members of the faculty have to be socialized with the sophisticated, induced with best standard emulated by the OU, Deree teaching culture.

Each academic year a wide range of activities take place aiming to raising staff awareness with regards to the College's emphasis on pedagogy and research. Lectures, workshops, and seminars are organized by the College and are well-attended by the staff of all departments/areas.

Recognizing the importance of pedagogy and research, the College has established the Deree Teaching and Learning Center, which organizes workshops on current pedagogy, informs faculty about relevant opportunities abroad and seeks external funding for such purposes among other things. It also assists departments with planning and monitoring implementation of a series of events (e.g. lectures, workshops, symposia, round-table discussions, colloquia, retreats) every semester.

A variety of teaching, learning and assessment resources will be used that include:

- web-based materials
- hands-on practical work
- virtual and augmented reality solutions
- computer-aided learning packages
- online forums
- directed reading
- formative assessments
- summative assessments
- self-assessment questions

10. Changes made to the programme since last (re)validation

N/A

Annexe 1: Curriculum map

Annexe 2: Notes on completing the OU programme specification template

Annexe 1 - Curriculum map

This table indicates which study units assume responsibility for delivering (shaded) and assessing (**X**) particular programme learning outcomes.

Level	Study module/unit	A1	A2	A3	A4	A5	B1	B2	B3	B4	C1	C2	C3	C4	C5	D1	D2	D3	D4	D5
																Programme outcomes				
4	PS 1001 LE Psychology as a Social Science																X			
	CS 2179 Business Information Systems		X				X									X	X			
	ITC 2024 Computer Networks & Cybersecurity Fundamentals	X	X	X	X	X	X	X			X	X	X			X	X			
	ITC 2088 Introduction to Programming				X							X				X	X			
	ITC 2186 Computer System Architecture				X							X				X	X			
	ITC 2193 Operating Systems Concepts				X							X				X	X			
	ITC 2101 Principles of Wireless, IoT, and Mobile Networks	X	X	X		X		X			X	X	X			X	X	X	X	
	ITC 2197 Object Oriented Programming Techniques				X							X				X	X	X	X	

Level	Study module/unit	A1	A2	A3	A4	A5	B1	B2	B3	B4	C1	C2	C3	C4	C5	D1	D2	D3	D4	D5
																Programme outcomes				
5	PH 3010 LE Ethics *or* PH 3005 LE Business Ethics		X				X										X		X	X
	ITC/PH 3036 Privacy, Policy, Law and Technology		X				X	X			X	X				X	X		X	X
	ITC 3121 Computer Networks Modeling & Analysis	X		X		X		X	X		X	X	X		X	X	X	X	X	X
	ITC 3006 Mathematics for Computing				X							X				X			X	X
	ITC 3319 Network Administration	X		X		X		X	X		X	X	X		X	X	X	X	X	X
	ITC 3160 Fundamentals of RDBMS				X							X				X	X	X	X	X
	ITC 3431 Cryptography & Network Security	X		X	X	X	X	X	X		X	X	X		X	X	X	X	X	X
	ITC 3632 Security of Wireless, IoT, and Mobile Networks	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X

Level	Study module/unit	A1	A2	A3	A4	A5	B1	B2	B3	B4	C1	C2	C3	C4	C5	D1	D2	D3	D4	D5
												Programme outcomes								
6	ITC 4214 Internet Programming				X							X	X		X		X	X	X	
	ITC 4344 Digital Forensics	X	X	X	X	X	X	X	X	X	X		X				X		X	
	ITC 4446 Intrusion Detection and Incident Response-	X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X
	ITC 4426 Distributed Systems	X				X	X			X	X	X	X			X	X	X		X
	ITC 4447 Secure Software Development	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X
	ITC 4648 Ethical Hacking & Penetration Testing	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X
	ITC 4140 Methods in ICT Project Research & Management		X	X		X	X	X		X	X	X	X	X	X	X	X	X	X	X
	ITC 4949 Cybersecurity and Networks Capstone					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Annexe 2: Notes on completing programme specification templates

1 **-** This programme specification should be mapped against the learning outcomes detailed in module specifications.

2 – The expectations regarding student achievement and attributes described by the learning outcome in <u>section 3</u> must be appropriate to the level of the award within the **QAA frameworks for HE qualifications**:
http://www.qaa.ac.uk/AssuringStandardsAndQuality/Pages/default.aspx

3 – Learning outcomes must also reflect the detailed statements of graduate attributes set out in **QAA subject benchmark statements** that are relevant to the programme/award: http://www.qaa.ac.uk/AssuringStandardsAndQuality/subject-guidance/Pages/Subject-benchmark-statements.aspx

4 – In section 3, the learning and teaching methods deployed should enable the achievement of the full range of intended learning outcomes. Similarly, the choice of assessment methods in section 3 should enable students to demonstrate the achievement of related learning outcomes. Overall, assessment should cover the full range of learning outcomes.

5 - Where the programme contains validated **exit awards** (e.g. CertHE, DipHE, PGDip), learning outcomes must be clearly specified for each award.

6 - For programmes with distinctive study **routes or pathways** the specific rationale and learning outcomes for each route must be provided.

7 – Validated programmes delivered in **languages other than English** must have programme specifications both in English and the language of delivery.