BSc Honours Cyber Security and Digital Forensics

Programme Specification

1. Programme title	BSc Honours Cyber Security and Digital Forensics BSc Honours Cyber Security and Digital Forensics with Foundation Year (Hendon only)
2. Awarding institution	Middlesex University
3. Teaching institution	Middlesex University: Hendon Middlesex University: Mauritius Middlesex University: Dubai
4. Details of accreditation by professional/statutory/regulatory body	
5. Final qualification	BSc Honours, BSc, DipHE, CertHE
6. Year of validation **Year of amendment**	2018/19 2019/20 / 2021/22
7. Language of study	English
8. Mode of study	Full Time & Part Time

9. Criteria for admission to the programme

Please refer to the programme specification for the Foundation Year for criteria for admission to the BSc Cyber Security and Digital Forensics with Foundation Year programme.

Student should have the equivalent of 96 UCAS Tariff points to gain entry to level 4. All candidates should possess at least grade C in GCSE Maths and English language, or equivalent. For direct entry to levels 5 & 6 the student is required to pass the equivalent of 120 credits specified in the programme at levels 4 & 5, respectively. You will be expected to demonstrate the programme learning outcomes have been met at these levels, for example by attainment of industrially based qualifications such as Cisco Certified Security Associate/ Professional.

Mature applicants with relevant work experience are also welcome to apply for Direct entry at levels 3, 4 and 5. These applicants are required to submit a portfolio of work experience to show evidence of achieving relevant learning outcomes, and these will vary depending on both the programme and level the student is applying for. Evidence should

comprise the applicant's own work and may include documents they have written, procedures they have designed, proposals they have drafted, electronic resources, photographs, video etc or information gathered from others about you such as statements from employers, certificates of in-house courses completed.

Further guidance may be obtained from the Programme Leader or Director of Programmes.

International students who have not been taught in the English medium must show evidence of proven ability in English such as IELTS grade 6.0. The University provides pre-sessional English language courses throughout the year for candidates who do not meet the English requirements. University policies supporting students with disabilities apply, as described in the University Regulations

University policies supporting students with disabilities apply, as described in the University Regulations, 'Information for students with disabilities'

10. Aims of the programme

The programme aims to:

Allow students to develop a significant range of pen testing skills as well as investigation skills which are highly valued and sought-after by the international security and digital forensics sector. These skills include the ability to use digital tools to investigate incidents as well as deep understanding of CS & DF compliance. The primary educational aim is to produce graduates fully prepared for a range of careers in Cyber Security and Digital Forensics who are capable of progressing to postgraduate study in either of the following postgraduate titles: "Cyber Security and Penetration Testing", or "e-Security and Digital Forensics". Wherever appropriate, modern laboratories equipped with industry-standard equipment, software and network development tools will support the development of these skills. Essentially the programme's aims are twofold:

i) Students will be able to protect and prevent cybercrimes occurring in organisations and be compliant with regulations governing Cyber Security; and,

ii) Students will be able to detect and advise on cybercrimes that have occurred in organisations and be compliant with regulations governing Digital Forensics

11. Programme outcomes*

A. Knowledge and understanding

On completion of this programme the successful student will have knowledge and understanding of and be able to:

1. Recognise and explain essential fundamentals and underpinning

Teaching/learning methods

Students gain knowledge and understanding through

The curriculum has been designed to offer the opportunity of an orderly academic

theory of relevant digital devices and the communication networks they rely on.

2. Define and recall essential facts, concepts, principles and theories required to analyse and model the protection of relevant digital devices and the networks they rely on.

3. Identify and analyse specifications appropriate to Cyber Security and Digital Forensic problems and plan strategies for their solutions that comply with standards.

4. Consider, contemplate and explain the relevance and ramifications of a range of professional, legal, managerial, business, organisational, ethical, compliance, social and sustainability in the lifecycles of cyber security, and digital forensic investigations.

5. Reproduce concepts and fundamental design principles to produce, secure and/or analyse information in organisations using a variety of programming languages and appropriate software tools.

6. Contrast and compare the theory behind a variety of approved tools and techniques that aid investigations in the digital forensic lifecycle, including seizure, preservation, acquisition, reconstruction, analysis, reporting, and presentation.

7. Explain and describe the significance, role and function of digital devices within society and the regulations, ethics, and

progression between levels of study within identifiable cyber security and digital forensics related themes.

At Level 4, modules address the conceptual, technical and mathematical underpinnings of the study of computer networks using SOBs (Students' Observable Behaviour). A1 and A2 are introduced in contexts relating to networks, information, programming and computer communication by means of lectures, seminars, personal tutor system and laboratories. Students are helped to understand the relevance to the development and analysis of networks systems, programs, database and network applications. Set tasks are used to engender confidence and proficiency within the particular topics addressed.

Elements of A3, A4 ,A6, A8 – A10 are addressed both implicitly to motivate initial understanding and to place technical topics into a wider context Learning materials are designed to relate to computers and networks. Wherever case studies or problems concerning networks at system- (rather than topic-level) are addressed, additional learner support is offered by tutors. Problem solving and design tasks are used in seminars to reinforce and deepen understanding, and students are given the opportunity of practically applying theory in laboratory tasks and seminars.

At Level 5, there is significant horizontal integration of learning materials; for example networking concepts and terminology are introduced in one module, and in another real-life scenarios are used to deepen and refine understanding.

At Level 5, further material addressing A1, and A2 are introduced, whilst A3-A9 topics

procedures that govern the cyber security, digital forensics and e-discovery sectors.

8. Contrast and compare the theory behind a variety of approved tools and techniques that aid investigations in the cyber security lifecycle, including identify, protect, detect, respond, and recover.

9. Recall and evaluate underpinning theory behind a variety of tools and techniques that cover the digital forensic lifecycle, including seizure, preservation, acquisition, reconstruction, analysis, reporting, and presentation of inculpatory and exculpatory artefacts.

10. Research and present rational, warranted and reasoned arguments that address a range of issues relating to cyber security and digital forensics.

are introduced and typically involve an increasingly cyber security and digital forensic focus. As modules progress there is an increasing emphasis on design, problem solving and analysis. Particular importance is emphasised for A3 and A4 and focus on standards, regulations and ethics before students embark on their final year project.

Progressively increasing levels of appreciation of quality (A5-A9) and performance aspects of products and processes is also encouraged and expected in seminar work and coursework at Levels 5 & 6.

At Level 6, students are expected to consolidate their understanding of new material and to take greater responsibility for the selection of concepts, principles and methodology needed to analyse, synthesise and evaluate particular systems, processes and products in a range of contexts (A3-A10).

Students gain knowledge and comprehension through a combination of:

- Closely supervised laboratories and various exercises
- Encouragement to raise questions and be open minded to suggestions from other team members when seeking practical solutions.
- Supervised seminars
- Open-ended practical sessions
- Formative and Summative feedback on assignments
- Laboratory Experimentation

- Lectures
- Debates
- Modelling
- Coursework
- Guided and independent research
- Reading
- Independent study
- Personal Tutor support

Assessment methods
Students' knowledge and understanding is assessed by
Outcomes A1, A2, A5 are assessed using SOBs and coursework assignments involving a range of problem-solving, design, analysis, modelling, and simulation tasks. Individual and group work (including presentations and formal reports of work undertaken) is increasingly framed at investigations in cyber security and digital forensics. Throughout the programme multiple choice questions, presentations of work-in-progress, practical assessment, time constrained exercises, technical reports and experiments (at Levels 5 and 6) are used for assessing knowledge and understanding.

Typically a module will involve a variety of assessment types to target students' differing learning styles.

B. Skills

On completion of this programme the successful student will be able to:

1. Apply dedicated hardware and software safely and effectively in all

Teaching/learning methods
Students learn cognitive skills through

Skills are developed initially at Level 4 where communication skills, basic research skills and skills in applying mathematical principles and concepts are developed. The ability to work effectively both as an

stages of cyber security, and digital forensic lifecycles.

2. Design and develop experimental frameworks to test hypotheses impartially and summarise efficaciously on the results.

3. Competently execute data acquisition from various sources to maximise preservation of data, whilst minimising contamination, and then use that data to inform an investigation.

4. Competently execute an investigation to cover all aspects of the cyber security lifecycle.

5. Design and develop software to generate solutions to a wide range of problems.

6. Document, design and analytically work appropriately; commission, research, and sustain individual project activity and to report on findings in a defensible fashion relying on minimal supervision.

7. Plan, manage and prepare for an incident response.

individual and as a member of a team is summatively assessed at Level 4 both in seminars and laboratories using a variety of teaching methods, which include: Online quizzes, Modelling, Programming, Formative feedback, technical reports, Presentations, Practical laboratories, Practical Exercises, Personal Tutor Support and Time Constrained Exercises.

At Level 4 students become involved in many different activities requiring the exercise of B1, B2 and B5 and are supported by regular and frequent formative feedback in laboratories and seminars

The development of transferable skills B3, B4, B6 and B7 is progressed at Level 5 in the contexts of group project work and, at Level 6, in that of individual project work and other Level 6 modules.

At all levels students are taught how to operate specialist equipment effectively and safely and to respect rules of conduct in laboratories.

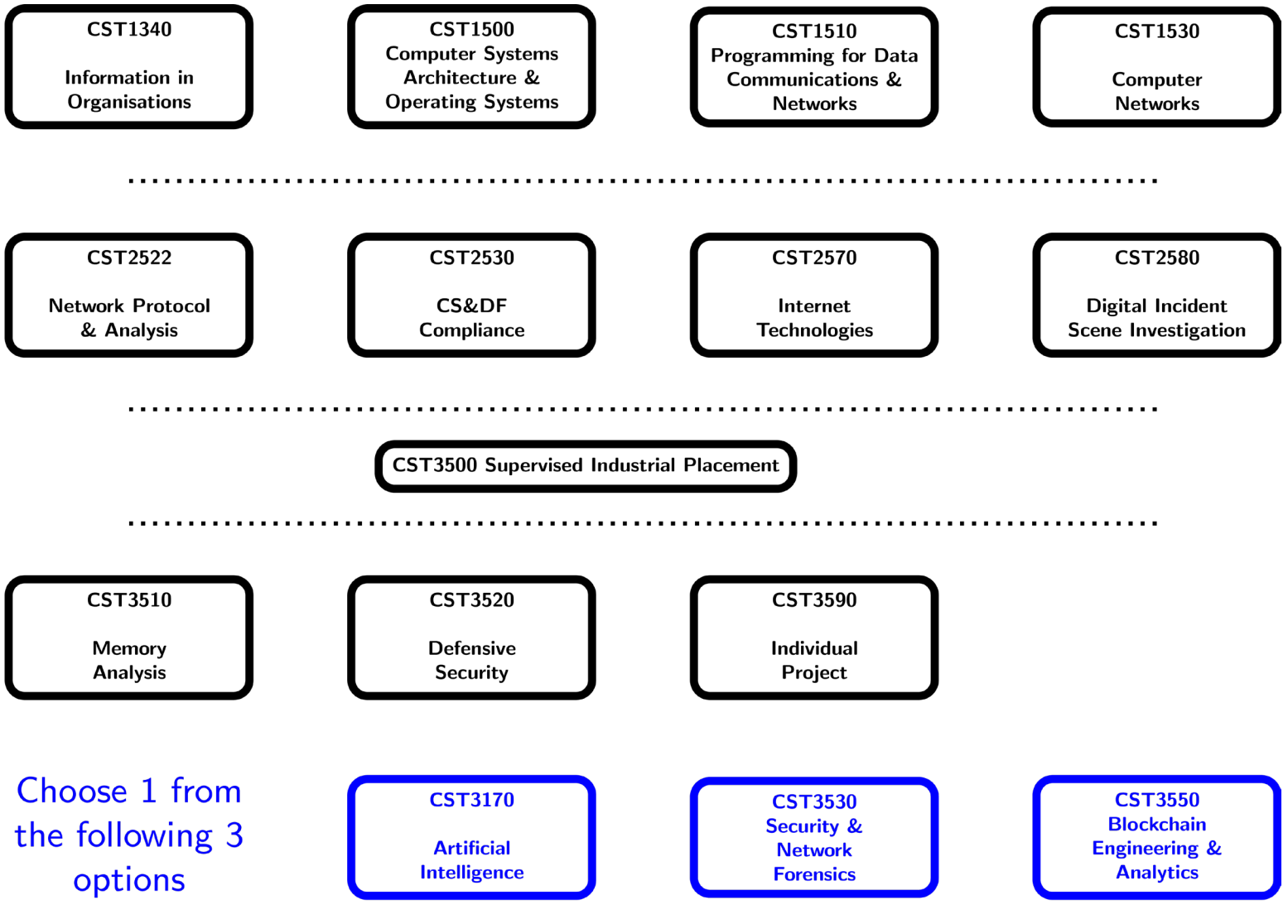
Assessment methods

Students' skills are assessed by a mixture of coursework and exams. There are no exams at level 4 but students' skills are assessed by a combination of:

- Coursework
- Project work
-
- Multiple choice questions
- Student observable behaviour
- Modelling and programming
- Supervised laboratory exercises
- Technical reports
- Writing-up experiments into a report
- Time constrained exercises
- Dissertation

12. Programme structure (levels, modules, credits and progression requirements)

12. 1 Overall structure of the programme – (all modules are 30cps except CST3500, 120cps)



12.2 Levels and modules
Starting in academic year 2010/11 the University is changing the way it references modules to state the level of study in which these are delivered. This is to comply with the national Framework for Higher Education Qualifications. This implementation will be a gradual process whilst records are updated. Therefore the old coding is bracketed below.

Level 3 (FY) - Please refer to the programme specification for the Foundation Year for the modules to be taken during the foundation year of the BSc Cyber Security and Digital Forensics with Foundation Year programme

Level 4 (1)

COMPULSORY	OPTIONAL	PROGRESSION REQUIREMENTS
Students must take all of the following: **CST1500** - Computer Systems Architecture and Operating Systems **CST1510** - Programming for Data Communications and Networks **CST1340 -** Information in Organisations **CST1530 -** Computer Networks	None	Students are normally expected to pass 120 credit points to progress to level 5 full-time study or level 5 part-time study. University regulations apply.

Level 5 (2)

COMPULSORY	OPTIONAL	PROGRESSION REQUIREMENTS

Students must take all of the following: **CST2530** - Cyber Security & Digital Forensics Compliance **CST2570 -** Internet Technologies **CST2522 –** Network and Protocol Analysis **CST2580 –** Digital Incident Scene Investigation and Analysis	Students registered in thick sandwich mode complete the Industrial Placement module, then return to complete the final year **CST3500** – Industrial Placement	Students are normally expected to achieve 240 credits at levels 4 & 5 to progress to level 6. University regulations apply.
Level 6 (3)		
COMPULSORY	OPTIONAL	PROGRESSION REQUIREMENTS
Students must take all of the following: **CST3590 -** Individual Project **CST3510 –** Memory Analysis **CST3520** – Defensive Security	Students must also choose ONE from the following: **CST3550** - Blockchain Engineering & Analytics **CST3530 -** Security and Network Forensics **CST3170** - Artificial Intelligence	In order to graduate with an honours degree i.e. with a BSc Hons Cyber Security and Digital Forensics award, students must have achieved 360 credit points. To graduate with an ordinary degree, 300 credit points with a minimum of 60 credit points at Level 6. University regulations apply.

12.3 Non-compensatable modules (note statement in 12.2 regarding FHEQ levels)	
Module level	**Module code**
Level 6	CST3590
Level 6	CST3520

13. Curriculum map

See attached.

14. Information about assessment regulations

- Information on how the University formal assessment regulations work, including details of how award classifications are determined, can be found in the University Regulations at https://www.mdx.ac.uk/about-us/policies

- Practical aspects of the programme are often assessed via coursework that may be carried out using specialist software and may include lab tests.

- Theoretical material is assessed by coursework and examinations.

- Grades are awarded on the standard University scale of 1–20, with Grade 1 being the highest. To pass a module all components, both coursework and examination, must be passed individually with a minimum grade of 16. Failure in one of the components will result in the failure of the module.

For additional information on assessment and how learning outcomes are assessed please refer to the individual module narratives for this programme.

15. Placement opportunities, requirements and support

All Undergraduate students have the opportunity to go on Industrial Placement. Industrial Placements are encouraged as this valuable experience enhances a student's future career prospects. Additionally students normally achieve better results in their final year. In brief:

- The placement provides a years' experience as an appropriately paid graduate trainee.

- Industrial placement is conditional on the successful completion of all modules at Level 4 and Level 5; therefore students need 240 credits before they are able to embark on an industrial placement.

- Obtaining a placement is co-ordinated through the Campus Placement Office.

- For Undergraduate programmes, students wishing to undertake a placement position must register for CST3500.

- Each placement will be assigned to an industrial tutor who will visit the student on placement.

- On graduation the degree will be qualified with the term "…with approved industrial experience".

Note: The placement option is not available to direct-entry students into level 6.

16. Future careers (if applicable)

All programmes in the Faculty of Science and Technology – their curricula and learning outcomes – have been designed with an emphasis on currency and the relevance to future employment.

- The majority of graduates are employed in IT posts relevant to the subject.
- Over 20% of students pursue further postgraduate study or research.

The employer links with the faculty are encouraged in a number of ways e.g. by inviting practitioners from industry as guest speakers in lectures; through links with companies where students are employed as part of their Industrial placement and through alumni both in the UK and overseas

Campus Careers Offices can be found on each campus for advice, support and guidance.

17. Particular support for learning (if applicable)

- The faculty's Teaching and Learning Strategy is compliant with those of the University, in seeking to develop learner autonomy and resource- based learning In support of the students learning experience:
- All new students go through an induction programme and some have early diagnostic numeric and literacy testing before starting their programme. Learning Resources (LR) provide workshops for those students needing additional support in these areas.
- Students are allocated a personal email account, secure networked computer storage and dial-up facilities
- New students are provided with a CD containing the faculty Subject Handbook at enrolment
- New and existing students are given module handbooks for each module they study. Soft copies of all module handbooks can be found on Oasis. Web-based learning materials are provided to further support learning
- Extensive library facilities are available on all campuses. Visit https://unihub.mdx.ac.uk/study/library for pages on learning resources. Students can access advice and support on a wide range of issues from the UniHelp Student Information Desk.
- Placements are supported by Campus Placement Offices and School academics; please refer to section 15 of this programme specification
- High-quality specialist network, software, digital and wireless laboratories equipped with industry standard software, hardware and tools as appropriate, for formal

teaching as well as self-study. Middlesex University is a Cisco Local Academy and a Xilinx University partner

- Teaching staff are available for each subject offering personal academic advice and help if needed. Staff availability for this purpose is posted outside staff office doors. Formative feedback is given on completion of student coursework
- Past exam papers with solutions and marking schemes for all modules are available for students in module handbooks.
- Research activities of academic staff feed into the teaching programme, which can provide individual students with ad-hoc opportunities to work with academics on some aspect of research. .

18. JACS code (or other relevant coding system)	144I118 BSc CSDF 114I123 BSc CSDF with FY
19. Relevant QAA subject benchmark group(s)	Computing Benchmark & Digital Forensics

20. Reference points

The following reference points were used in designing the programme:

• QAA Computing subject benchmark statements, Computing (2016) and Engineering (2015)

• QAA Framework for Higher Education Qualifications in England, Wales and Northern Ireland

• QAA guidelines for programme specifications

• QAA Code of Practice for the assurance of academic quality and standards in HE

• UK Standard for Professional Engineering Competence; Chartered Engineer and Incorporated Engineer Standard, Engineering Council UK, 2010

• UK Standard for Professional Engineering Competence; The Accreditation of Higher Education Programmes, Engineering Council UK, 2008

• Middlesex University Learning Teaching and Assessment Strategy (2012 – 2014)

• University Regulations

• Module Narratives

• Middlesex University and Faculty of Science and Technology Teaching Learning and Assessment policies and strategies.

21. Other information

Middlesex University has formal links with 250 institutions world-wide, including student exchange agreements with more than 100 institutions. Currently a number of students both from the UK/EU and overseas take part in such exchanges. For further details please visit **https://www.mdx.ac.uk/global-impact/middlesex-and-brexit**

Please note programme specifications provide a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve if s/he takes full advantage of the learning opportunities that are provided. More detailed information about the programme can be found in the rest of your programme handbook and the university regulations.

Curriculum map for *BSc (Hons) Cyber Security and Digital Forensics*

This section shows the highest level at which programme outcomes are to be achieved by all graduates, and maps programme learning outcomes against the modules in which they are assessed.
Please refer to the programme specification, which includes the curriculum map for the Foundation Year.

Programme learning outcomes

Knowledge and understanding	
A1	Recognise and explain essential fundamentals and underpinning theory of relevant digital devices and the communication networks they rely on.
A2	Define and recall essential facts, concepts, principles and theories required to analyse and model the protection of relevant digital devices and the networks they rely on.
A3	Identify and analyse specifications appropriate to Cyber Security and Digital Forensic problems and plan strategies for their solutions that comply with standards.
A4	Consider, contemplate and explain the relevance and ramifications of a range of professional, legal, managerial, business, organisational, ethical, compliance, social and sustainability in the lifecycles of cyber security, and digital forensic investigations.
A5	Reproduce concepts and fundamental design principles to produce, secure and/or analyse information in organisations using a variety of programming languages and appropriate software tools.
A6	Contrast and compare the theory behind a variety of approved tools and techniques that aid investigations in the digital forensic lifecycle, including seizure, preservation, acquisition, reconstruction, analysis, reporting, and presentation.
A7	Explain and describe the significance, role and function of digital devices within society and the regulations, ethics, and procedures that govern the cyber security, digital forensics and e-discovery sectors.
A8	Contrast and compare the theory behind a variety of approved tools and techniques that aid investigations in the cyber security lifecycle, including identify, protect, detect, respond, and recover.
A9	Recall and evaluate underpinning theory behind a variety of tools and techniques that cover the digital forensic lifecycle, including seizure, preservation, acquisition, reconstruction, analysis, reporting, and presentation of inculpatory and exculpatory artefacts.
A10	Research and present rational, warranted and reasoned arguments that address a range of issues relating to cyber security and digital forensics.
Skills	
B1	Apply dedicated hardware and software safely and effectively in all stages of cyber security, and digital forensic lifecycles.
B2	Design and develop experimental frameworks to test hypotheses impartially and summarise efficaciously on the results.
B3	Competently execute data acquisition from various sources to maximise preservation of data, whilst minimising contamination, and then use that data to inform an investigation.

B4	Competently execute an investigation to cover all aspects of the cyber security lifecycle.
B5	Design and develop software to generate solutions to a wide range of problems.
B6	Document, design and analytically work appropriately; commission, research, and sustain individual project activity and to report on findings in a defensible fashion relying on minimal supervision.
B7	Plan, manage and prepare for an incident response.

Programme outcomes																	
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B7	B4	B5	B6	B7
Highest level achieved by all graduates																	
6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

Module Title	Module Code by Level	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B4	B5	B6	B7	
Computer Systems Architecture & Operating Systems	CST1500	✔	✔													✔			
Programming for Data Communications & Networks	CST1510	✔	✔			✔										✔			
Information in Organisations	CST1300	✔	✔													✔			
Computer Networks	CST1530	✔	✔									✔							
Digital Incident Scene Investigation	CST2580	✔	✔	✔			✔					✔		✔				✔	
Cyber Security & Digital Forensics Compliance	CST2530		✔	✔	✔		✔	✔											
Network & Protocol Analysis	CST2522	✔	✔	✔		✔			✔	✔	✔	✔			✔				
Internet Technologies	CST2570			✔		✔			✔	✔	✔				✔	✔			
Supervised Industrial Placement	CST3500																✔		
Individual Project	CST3990			✔	✔						✔		✔			✔	✔		
Memory Analysis	CST3510		✔	✔			✔		✔	✔	✔			✔	✔				
Defensive Security	CST3520	✔	✔	✔		✔			✔	✔	✔	✔			✔			✔	
Blockchain Engineering & Analytics*	CST3550	✔				✔			✔	✔	✔				✔	✔			
Artificial Intelligence*	CST3170					✔			✔				✔			✔			
Network Security & Forensics*	CST3530	✔		✔		✔			✔	✔	✔	✔			✔				