BSc (Hons) Cyber Security and Digital Forensics
Programme Specification

1. Programme title	BSc (Hons) Cyber Security and Digital Forensics BSc (Hons) Cyber Security and Digital Forensics with Foundation Year
2. Awarding institution	Middlesex University
3a Teaching institution	Middlesex University: Hendon (HEN), Dubai (DBI) and Mauritius (MRU)
3b Language of study	English
4a Valid intake dates	September (DBI, HEN, MRU); April (MRU)
4b Mode of study	FT/PT/TKSW (PT not available for Foundation Year / TKSW only available in HEN)
4c Delivery method	☒ On-campus/Blended ☐ Distance Education
5. Professional/ Statutory/ Regulatory body	N/A
6. Apprenticeship standard	N/A
7. Final qualification(s) available	BSc (Hons) Cyber Security and Digital Forensics BSc (Hons) Cyber Security and Digital Forensics with Foundation Year BSc Cyber Security and Digital Forensics DipHE Cyber Security and Digital Forensics CertHE Cyber Security and Digital Forensics
8. Academic year effective from	**2024-25**

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.

All candidates should possess at least grade 4 in GCSE Maths and English Language, or equivalent.

Student should have the equivalent of 112 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.

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 (with a minimum of 5.5 in all sections). 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.

10. Aims of the programme

The programme aims to:

Allow students to develop a significant range of cyber security skills as well as digital 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 “MSc Cyber Security and Penetration Testing”. Wherever appropriate, modern laboratories equipped with industry-standard equipment, software and network development tools will support the development of these skills. The programme’s aims are twofold:

i) Students will be able to protect, prevent and identify vulnerabilities of digital assets in organisations, whilst being compliant with regulations governing Cyber Security; and,

ii) Students will be able to detect and investigate a range of digital artefacts 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:

1. The essential fundamentals and underpinning theory of relevant digital devices and the communication networks they rely on.
2. The essential facts, concepts, principles and theories required to analyse, model and develop the protection of relevant digital devices and the networks they rely on, and the detection and preservation of digital artefacts on such devices.
3. The regulations, specifications and limitations to Cyber Security and Digital Forensic problems and plan strategies for their solutions that comply with standards.
4. The consideration and explanation of the relevance and ramifications of a range of professional, legal, regulatory, project management, ethical, compliance, social and sustainability issues in the lifecycles of cyber security, and digital forensic investigations.
5. The reproduction and communication of concepts, fundamental design principles and analytical information to develop secure systems in organisations using a variety of programming languages and appropriate software tools.
6. The comparisons and contrasts between the theory and practise of 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. The significance, role and function of digital devices within society and the regulations, standards, ethics, and procedures that govern the cyber security and digital forensics sectors.
8. The comparisons and contrasts between the theory and practise of a variety of approved tools and techniques that aid investigations in cyber security, including identification, protection, detection, preservation, response, and recovery.
9. The evaluation of the underpinning theory and applications of 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 digital artefacts.
10. The research, rationalisation, warranted and reasoned arguments that address a range of issues relating to cyber security and digital forensics.

Teaching/learning methods
Students gain knowledge and understanding through
The curriculum has been designed to offer the opportunity of an orderly academic 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 workshops, seminars, academic advising 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 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. Concept videos will be made available on VLE to introduce subjects and concepts for the week. 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 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. Importance is emphasised for A3 and A4 and focus on standards, regulations and ethics before students embark on their final year project.

Employability

At all levels there is an emphasis on preparing for employment in the Cyber Security and Digital Forensics sectors. This is different from sectors that do not require security clearance.

The issues of knowledge and confidence is instilled in the syllabus. Students will be gaining a professional understanding of the employability sectors via the successful completion of authentic coursework. This will ensure the importance of planning and completing projects to deadlines and instil the work ethic to be successful in industry.

There will be opportunities to engage with prospective employees throughout the programme. There will be guest lectures organised.

Leadership and Project Management are important issues in any modern organisation and are reflected by the level 5 module on project management.

Opportunities to engage with MDXWorks will be encouraged throughout all levels.

Assessment

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 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
- Key concept videos
- Encouragement to raise questions and be open minded to suggestions from other team members when seeking practical solutions.
- Supervised seminars
- Engaging and interactive workshops
- Open-ended practical sessions
- Formative and Summative feedback on assignments

- Laboratory Experimentation
- Guest Lectures
- Debates/Arguments
- Interviews
- Modelling
- Authentic Coursework
- Essays/Reports
- Guided and independent research
- Directed reading
- Independent study
- Academic Advisor 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 of authentic nature. 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, time constrained practical exercises, experiments and essays are used for assessing knowledge and understanding.

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

All students have the opportunity to consult their Academic Advisor throughout the year and each module will have many opportunities for formative feedback.

B. Skills

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

1. Use dedicated hardware and software safely and effectively in all stages of cyber security, and digital forensic lifecycles.
2. Design and develop experimental frameworks to test hypotheses impartially and summarise 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 and digital forensics lifecycles.
5. Design and develop software to generate solutions to a wide range of problems.
6. Document, design and critically evaluate 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 and/or a digital investigation.

Teaching/learning methods

Students learn 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 individual and as a member of a team is summatively assessed at Level 4 both in seminars and laboratories using a variety of methods, which include: Online quizzes, Modelling, Programming, Essays, Presentations, Practical laboratories, Practical Exercises, 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.

Sustainability
Where possible open access books are recommended and their use is encouraged. This enables students to reach a broad and diverse number of authors, practitioners and policymakers that promote the Sustainability Development Goals throughout the curriculum.
Where possible digital poverty has been keenly avoided in all areas of the programme by encouraging the use of open-source. Proprietary and specialist software is made available remotely for students who are off-campus.
ISO26000 is taught in level 5. This module covers other issues related to Sustainability Development Goals and how organisations can embed and integrate these practices as standard, including diversity, inclusivity and environmental considerations.
Assessment methods
Students’ skills are assessed by a mixture of coursework, practical tests and essays. There are no examinations and skills are assessed by a combination of:

- Authentic Coursework
- Project work and management
- Multiple choice questions
- Student observable behaviour
- Modelling and programming
- Supervised laboratory exercises
- Practical Laboratory tests
- Writing-up experiments into a report and taking contemporaneous notes
- Dissertation

All students have the opportunity to consult their Academic Advisor throughout the year and each module will have opportunities for formative feedback.

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

12.1 Structure of the programme

Please refer to the programme specification for the Foundation Year for the modules to be taken during the foundation year of the BSc (Hons) Cyber Security & Digital Forensics with Foundation Year programme.

All modules are 30 credits.

Optional modules at level 6 will only run if 15 or more students are registered.

BSc (Hons) Cyber Security & Digital Forensics (CS&DF)

Full-Time Mode

Year 1
Semester 1
Level 4
CST1500: Computer Systems Architecture & Operating Systems
CST1510: Programming for Data Communication & Networks
Semester 2
Level 4
CST1530: Computer Networks
CST1340: Information in Organisations
Year 2
Semester 1
Level 5
CST2590: Internet of Things
CST2572: Secure Web Technologies
Semester 2
Level 5
CST2580: Digital Incident Scene Investigation & Analysis
CST2560: Project Management & Professional Practice
Year 3
Semester 1
Level 6
CST3510: Memory Analysis
CST3535: Computer Security & Ethical Hacking
CST3590: Individual Project

Semester 2
Level 6
CST3520: Defensive Security (Choose 1 from the following 3 options)
CST3550: Blockchain Engineering & Analytics
CST3133: Advanced Topics in Data Science & Artificial Intelligence

BSc (Hons) Cyber Security & Digital Forensics (CS&DF) in Thick-Sandwich Mode:

Year 1
Semester 1
Level 4
CST1500: Computer Systems Architecture & Operating Systems
CST1510: Programming for Data Communication & Networks
Semester 2
Level 4
CST1530: Computer Networks
CST1340: Information in Organisations
Year 2
Semester 1
Level 5
CST2590: Internet of Things
CST2572: Secure Web Technologies
Semester 2
Level 5
CST2580: Digital Incident Scene Investigation & Analysis
CST2560: Project Management & Professional Practice
Year 3
Level 6
CST3500: Supervised Industrial Placement
Year 4
Semester 1
Level 6
CST3510: Memory Analysis
CST3535: Computer Security & Ethical Hacking
CST3590: Individual Project

Semester 2
Level 6 (Choose 1 from the following 3 options)
CST3520: Defensive Security
CST3550: Blockchain Engineering & Analytics
CST3133: Advanced Topics in Data Science & Artificial Intelligence

BSc (Hons) Cyber Security & Digital Forensics (CS&DF) - Part-Time Mode:
Level 4/ Year 1
Semester 1:
CST1500: Computer Systems Architecture & Operating Systems
Semester 2:
CST1530: Computer Networks
Year 2

Semester 1:
CST1510: Programming for Data Communication & Networks
Semester 2:
CST1340: Information in Organisations
Level 5/ Year 3
Semester 1:
CST2590: Internet of Things
Semester 2:
CST2580: Digital Incident Scene Investigation & Analysis
Year 4:
Semester 1:
CST2572: Secure Web Technologies
Semester 2:
CST2560: Project Management & Professional Practice
Level 6/ Year 5:
Semester 1:
CST3510: Memory Analysis
Semester 2:
CST3520: Defensive Security
Choose 1 from the following 3 options:
CST3550: Blockchain Engineering & Analytics

CST3133: Advanced Topics in Data Science & Artificial Intelligence
Year 6
Semester 1:
CST3535: Computer Security & Ethical Hacking
Semester 2:
CST3590: Individual Project

This is an indicative programme structure for part-time students.
Students starting in April may experience a different order of the running of modules.

12.2 Levels and modules

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

Compulsory

Students must take all the following:
CST1500 – Computer Systems Architecture and Operating Systems
CST1510 – Programming for Data Communication and Networks
CST1340 – Information in Organisations
CST1530 – Computer Networks

Optional

None

Progression requirements

Students must pass at least 90 credits to progress to Level 5. To achieve Honours, failed credit will need to be repeated.

Level 5
Compulsory

Students must take all the following:
CST2560 – Project Management and Professional Practice
CST2572 – Secure Web Technologies
CST2590 – Internet of Things
CST2580 – Digital Incident Scene Investigation and Analysis

Optional
None

Progression requirements

Students must pass at least 210 credit points (including 90 at level 5) in order to be eligible to enrol on modules at level 6, and at least 240 credits (including 90 at level 5) in order to be eligible to enrol on the level 6 individual project module (**CST3590**).

Level 6
Compulsory
Students must take all the following:
CST3590 – Individual Project
CST3510 -- Memory Analysis
CST3535 – Computer Security and Ethical Hacking
Students registered in thick sandwich mode complete the Industrial Placement module, then return to complete the final year
CST3500 – Supervised Industrial Placement

Optional
Students must also choose ONE from the following:
CST3550 – Blockchain Engineering & Analytics
CST3133 – Adv. Topics in Data Science and Artificial Intelligence
CST3520 – Defensive Security
Optional modules at level 6 will only run if 15 or more students are registered.

Progression requirements
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

Module level: Level 6

Module code: CST3590

13. 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 in-class tests.

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

14. Placement opportunities, requirements and support (if applicable)

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 can embark on an industrial placement.
- Obtaining a placement is co-ordinated through the Campus Careers 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.
- Students who complete the Supervised Industrial Placement module on TKSW mode will receive an additional qualification referred to as a Diploma of Industrial Studies Note: The placement option is not available to direct-entry students into level 6.

15. Future careers / progression

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.

Graduates will find roles in Organisation that require: their digital assets to be protected; confidential access whilst maintain integrity of data; and, non-repudiation of any actions. So, far these have included a broad range of companies and government organisations. The other area of employment is Digital Forensics and has seen students employed with Law Enforcement Agencies and e-Discovery organisations.

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

16. Particular support for learning

Students will be supported throughout their programme of study by academic experts in the appropriate fields. In addition, students will be supported by a Learning Resource Centre that works closely with academics in order to offer the most up-to-date resources. Some of the modules on this programme are supported by a team of Student Learning Assistants, Graduate Teaching Assistants and Technical Tutors who work with academic colleagues to ensure that labs are resourced, materials are available, and feedback is provided.

17. HECos code(s) 100365 (33%) / 100358 (67%)

18. Relevant QAA subject benchmark(s) Computing Benchmark (March 2022)

19. Reference points

The following reference points were used in designing the programme:

- QAA Computing subject benchmark statement, Computing (2022)
- Computing Curricula – The Overview Report - ACM CC2020: Computing Curricula 2020: Paradigms for Global Computing Education
- ISO2700X, ISO17025 & ISO26000
- University Regulations
- Learning and Quality Enhancement Handbook (LQEH)
- Curriculum Design Policy
- Assessment Design Guidance 2022-23

- 2031 Learning Framework Principles

20. 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 http://www.europe.mdx.ac.uk/

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 they take 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.

21. 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.

Programme learning outcomes

Knowledge and understanding

A1 The essential fundamentals and underpinning theory of relevant digital devices and the communication networks they rely on.

A2 The essential facts, concepts, principles and theories required to analyse, model and develop the protection of relevant digital devices and the networks they rely on, and the detection and preservation of digital artefacts on such devices.

A3 The regulations, specifications and limitations to Cyber Security and Digital Forensic problems and plan strategies for their solutions that comply with standards.

A4 The consideration and explanation of the relevance and ramifications of a range of professional, legal, regulatory, project management, ethical, compliance, social and sustainability issues in the lifecycles of cyber security, and digital forensic investigations.

A5 The reproduction and communication of concepts, fundamental design principles and analytical information to develop secure systems in organisations using a variety of programming languages and appropriate software tools.

A6 The comparisons and contrasts between the theory and practise of 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 The significance, role and function of digital devices within society and the regulations, standards, ethics, and procedures that govern the cyber security and digital forensics sectors.

A8 The comparisons and contrasts between the theory and practise of a variety of approved tools and techniques that aid investigations in cyber security, including identification, protection, detection, preservation, response, and recovery.

A9 The evaluation of the underpinning theory and applications of 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 digital artefacts.

A10 The research, rationalisation, warranted and reasoned arguments that address a range of issues relating to cyber security and digital forensics.

Skills

B1 Use 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 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 and digital forensics lifecycles.

B5 Design and develop software to generate solutions to a wide range of problems.

B6 Document, design and critically evaluate 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 and/or a digital investigation.

Programme outcomes: A1 A2 A3 A4 A5 A6 A7 A8 A9 A10 B1 B2 B3 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

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	x	X													X		
Programming for Data Communication & Networks	CST1510	x	x			x										X		
Information in Organisations	CST1340	X	x													X		
Computer Networks	CST1530	x	X									X						
Digital Incident Scene Investigation and Analysis	CST2580		x	x			X		x	x		x		x				X
Project Management & Professional Practice	CST2560			X	x		x	x										x
Internet of Things	CST2590	x	x	x		x			x	x	x	x			X			
Secure Web Technologies	CST2572			X		x			x	x		x			x	X		
Supervised Industrial Placement	CST3500				X					X					X		X	
Individual Project	CST3590			X	x			x			X		x				x	X
Computer Security and Ethical Hacking	CST3535	x		X		X			x	X		X			X	X		
Memory Analysis	CST3510		x	x			X		X	X		X		x	X			
Blockchain Engineering & Analytics*	CST3550					X	x		X	x x		X			X	x		

Defensive Security*	CST3520	x	x	x		X			X	x		x			x			x
Adv. Topics in Data Science and Artificial Intelligence*	CST3133					X							X			X		

*Indicates optional modules