Middlesex University London

Programme Specification

1.	**Programme title**	MSc Cyber Security and Pen Testing MSc Cyber Security and Pen Testing with 3 months placement (London only) MSc Cyber Security and Pen Testing with 12 months placement (London only)
2.	**Awarding institution**	Middlesex University
3a	**Teaching institution**	Middlesex University: London / Dubai / Mauritius
3b	**Language of study**	English
4a	**Valid intake dates**	Sept
4b	**Mode of study**	FT/PT – London; FT- Dubai, Mauritius
4c	**Delivery method**	☒ On-campus/Blended ☐ Distance Education
5.	**Professional/Statutory/Regulatory body**	
6.	**Apprenticeship Standard**	
7.	**Final qualification(s) available**	MSc Cyber Security and Pen Testing MSc Cyber Security and Pen Testing with 3 months placement, MSc Cyber Security and Pen Testing with 12 months placement
8.	**Academic year effective from**	**2024/2025**

9. Criteria for admission to the programme

Applicants should normally have one of the following:

A minimum of a second-class Honours degree (UK), or an equivalent overseas qualification – in computer science or in a science or engineering related subjects. Candidates with other degrees but with relevant work experience may also be considered and are encouraged to apply.

Whilst consideration of Recognition of Prior Learning (RPL) has been given, the programme team decided that it will not be accepted for candidates admitted onto this programme. International students whose first language is not English or who have not been taught in the English medium throughout, and whose first degree is not from a British university, must achieve an IELTS score of 6.5 with a minimum score of 6 in each band.

10. Aims of the programme

The programme aims to equip students with:

- An understanding of the fundamental importance of computer, network, and communication system security for an organisation.
- The ability to involve both the management and the user in the process of awareness, decision and implementation with regard to computer and network security.
- The skills to analyse the security risks a communication system may have and to propose/devise solutions.
- The knowledge necessary to evaluate new threats to authentication, confidentiality and privacy with a view of implementing solutions to combat such threats.
- The ability to make a functional security design for a communication system and implement it successfully.
- A balance of theory, advanced practical skills and experience to enable students to develop a sound knowledge and analytical ability to facilitate their intellectual and professional development.

11. Programme outcomes*

A. Knowledge and understanding	**Teaching/learning methods**
On completion of this programme the successful student will have knowledge and understanding of: 1. Algorithms used in computer and network security and be able to perform implementations of selected algorithms in this area together with their potential for increased organisational efficiency.	Students gain knowledge and understanding through Self-directed study, resource-based learning, small group discussions, small group and individual exercises, online laboratory sessions, live demonstration software, on-line examples and research project. Weekly seminar sessions that provide students with the opportunity to address questions, queries and problems.

2. Threats faced by computer operating systems, applications and networks and various countermeasures that can be used 3. Analysis, design and implementation of security systems, with an understanding of how cryptography can be used for providing security within applications. 4. Analysing a problem specification and to design and implement a solution. 5. Relevant professional, ethical and legal issues in computer and network security 6. A range of problems of computer and network security, and the available solutions and trade-offs 7. Applying secure methods for transmission and storage of data 8. To become familiar with different research methods to develop policies and select suitable mechanisms to enforce such policies 9. Full knowledge and understating of rules and regulations pertaining to cyber security 10. Ability to apply technical strategies, tools and techniques to secure data and information for customers/clients	• Traditional lecture delivery (outcomes 1-10), • Group and individual research, presentations and written reports (outcomes 1-9), • Laboratory sessions (outcome 2, 5 & 6). • Individual and group design work (outcomes 3, 4, 5, 8 -10), • Individual project. Throughout the students are encouraged to undertake independent reading both to supplement and consolidate what is being taught/learned and to broaden their individual knowledge and understanding of the subject (outcomes 1-10). **Assessment methods** Students' knowledge and understanding is assessed by: Group and individual coursework, presentations, group and individual reports, and the in-Class activities and the project thesis assess students' knowledge and understanding. • Outcomes 1-7 assessed by in-Class activities • Outcomes 3 and 6 are assessed by laboratory sessions and practical assignments Outcome 1-10 are assessed by individual essay and final project thesis.
B. Skills On completion of this programme the successful student will be able to: 1. Critically evaluate the needs for security provision for communication networks and apply security policies and regulations for existing security systems.	**Teaching/learning methods** Students learn cognitive skills through • traditional lecture delivery (outcomes 1 and 3), • Group and individual research, presentations and written reports (outcomes 1-5),

2. Have a critical and clear understanding of current theories and techniques for apprising user interfaces and practical designs skills for effective user interactions 3. Critically analyse and evaluate security applications and techniques and recommend and propose new measures to improve security 4. Make informed choices of the appropriate security measures to put into place for a given network and/or an operating system 5. Demonstrate fundamental security management skills and techniques relating to the leadership of projects. 6. Draw up security measures for computer networks and communication systems 7. Acquire and apply relevant mathematical techniques to carry out security algorithms 8. Analyse a problem systematically and implement an effective solution both individually and within a group 9. Communicate effectively with peers and senior managers in writing, verbally and through graphical notations. 10. Apply learnt knowledge in computer and network security to better protect a networking environment.	• Small group and individual exercises (outcomes 1-6), • Live virtual online Laboratory sessions (outcome 4 and 5), • Individual project (outcomes 1-6 and 8-13: depending on project title). Analysis, design and problem solving skills are further developed through various design activities as well as case studies, and extensive computer laboratory sessions. Feedback is given to students on all assessed coursework as well as written in-Class activities (In the form of reports produced each term). **Assessment methods** Students' cognitive skills are assessed by: • Group and individual coursework (outcomes 1-6) • Laboratory tests (outcome 1, 4-5), • The in-Class activities (outcomes 1-6 and 7), and • The project thesis (outcomes 1-6 and 8-10 depending on project title) • Skills 7-10 are assessed through coursework and in-Class activities (seminars) • Skills 8-10 are assessed by laboratory sessions.

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

12.1 Structure of the programme

The programme is structured to accommodate both full-time study, which may include an industrial placement for 3 months and 12 months, and part-time enrolment. The standard University academic year consists of 24 weeks, divided into two semesters of approximately 12 weeks each.

The programme comprises 120 credits of compulsory taught modules and a 60-credit postgraduate project module. For an MSc award a total of 180 credits must be attained. For a PGDip (exit) award, 120 credits must be attained, i.e., all taught modules. For a PGCert (exit) award, a minimum of 60 credits must be attained and there is no restriction on which taught modules must be completed to make up those 60 credits. All taught modules are compulsory. Full-time students study the taught modules over a period of 24 weeks. Following the completion of the taught modules, students undertake the project module (60 credits) over the next term to complete the programme in approximately one calendar year. The programme structure is illustrated below.

12. Programme structure (levels, modules, credit points (CPS) and progression requirements)

12. 1 Overall structure of the programme

Your Modules
Full-Time (with placement - UK students) / **Part-Time**

<table>
<tr><th colspan="5">MSc Cyber Security and Pen Testing</th></tr>
<tr><td rowspan="2">Level 7
Terms
1 & 2</td><td>CST4530
Security Solutions and Applications (30credits)</td><td>CST4550
Penetration Testing and Digital Forensics (30 credits)</td><td>CST4500
Computer Networks and Internetworking (15 credits)</td><td>CST4522
Operating Systems for Networked Environments (15 credits)</td></tr>
<tr><td></td><td></td><td>CST4590 Cyber Security and Legal Regulations (15 credits)</td><td>CST4560
Network Security and Mechanisms (15 credits)</td></tr>
<tr><td>Optional Term(s)</td><td colspan="2">CST4840
PG Work Experience (3 months)
(0 credits)</td><td colspan="2">CST4850
PG Work Experience (12 months)
(0 credits)</td></tr>
<tr><td>Note for Part-time</td><td colspan="4">Part-time students can select any one 30 credits modules and two 15 credits in one academic year followed by one more module (30 credits) and two 15 credits in the next academic year.</td></tr>
<tr><td>Level 7
Term 3</td><td colspan="4">CST4599
Individual PG Project
(60 credits)</td></tr>
</table>

Students may advance to the project stage with a 30-credit deficit but must successfully complete all taught modules before registering for the placement. The duration of the postgraduate project is one semester for full-time and two semesters for part-time students. Assessments for taught modules occur at the end of Winter and Spring semesters, with reassessment before the Autumn semester begins**.**

12.2 Levels and modules

Level 7

Compulsory	Optional	Progression requirements
Students must take all of the following: **CST4500:** Computer Networks and Internetworking **CST4522:** Operating Systems for Networked Environments	**Full-time UK** students may additionally take one of the following option modules: Either CST4840 – Postgraduate Work Placement (3 months) Or CST4850 – Postgraduate Work Placement (12 months)	Before progressing to the optional placement module, students are required to successfully pass all taught modules. However, students may advance to the project stage with a maximum of a 30-credit deficit.)

CST4530: Security Solutions and Applications **CST4550:** Penetration Testing and Digital Forensics **CST4560:** Network Security and Mechanisms **CST4590:** Cyber Security and Legal Regulations **CST4599:** Individual PG Project		

*Please refer to your programme page on the website re availability of option modules

12.3 Non-compensatable modules	
Module level	**Module code**
7	CST4550
7	CST4599

13. Information about assessment regulations

This programme will run in line with general University 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/university-regulations

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.

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

Industrial placement is offered as an optional opportunity for **full-time students in the UK.** Students can choose between a 3-month or 12-month placement duration.

Students are responsible for securing their placement through independent applications, with support available from our employability service, MDXWorks. If a suitable placement opportunity has not been identified before the start of the optional placement module due to unsuccessful applications or unsuitability, students will proceed directly to the Project module.

15. Future careers / progression

Successful students will be well placed for a range of roles in the professional computing sector, and the strong research underpinning of the programme provides a platform for further research activity.

16. Particular support for learning

For more information please check this link:

http://unihub.mdx.ac.uk/study

The Department of Computer Science 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. The Learning Enhancement Team (LET) provides one-to-one tutorials and 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.
- A programme handbook is made available to students at enrolment (electronic copies for all students are available via virtual learning environment).
- New and existing students are provided with electronic module handbooks for each module they study Web-based learning materials are provided to further support learning.
- Extensive library facilities are available at the base campus.
- Students can access advice and support on a wide range of issues from the Student Services Counter and the Student Information Desk. Student Advisers aligned to subject areas offer confidential one to one advice and guidance on programme planning (if applicable) and regulations.
- High quality specialist laboratories equipped with industry standard software and hardware where appropriate, for formal teaching as well as self-study.

- Tutorial sessions for each module organised for groups of up to 20 students are provided for additional teaching support.
- Feedback is given on completion of all formative assessments.
- Where applicable, past exam papers for all modules (which are assessed by examination) are available for students via Unihub.
- Research activities of academic staff feed into the teaching programme, which can, on some occasions, provide an opportunity for students to work with academics on some aspect of research.

Middlesex University encourages and supports students with disabilities. Some practical aspects of Computer Science programmes may present challenges to students with particular disabilities. You are encouraged to visit our campuses at any time to evaluate facilities and talk in confidence about your needs. If we know your individual needs we'll be able to provide for them more easily. For further information contact the Disability Support Service (email: disability@mdx.ac.uk).

17. HECos code(s)	

18. Relevant QAA subject benchmark(s)	Computing

19. Reference points

The following reference points were used in designing the programme:

- QAA computing subject benchmark statement (master's degrees in computing 2011)
- QAA framework for higher education qualifications in England, Wales and Northern Ireland
- QAA Quality code
- CLTE Learning and Quality Enhancement Handbook
- University's regulations for postgraduate taught programmes
- University equality and diversity policy document

20. Other information

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.

21. Curriculum map for MSc Cyber Security and Pen Testing

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	Algorithms used in computer and network security and be able to perform implementations of selected algorithms in this area together with their potential for increased organisational efficiency.
A2	Threats faced by computer operating systems, applications and networks and various countermeasures that can be used
A3	Analysis, design and implementation of security systems, with an understanding of how cryptography can be used for providing security within applications.
A4	Analysing a problem specification and to design and implement a solution.
A5	Relevant professional, ethical and legal issues in computer and network security
A6	A range of problems of computer and network security, and the available solutions and trade-offs
A7	Applying secure methods for transmission and storage of data
A8	To become familiar with different research methods to develop policies and select suitable mechanisms to enforce such policies
A9	Full knowledge and understating of rules and regulations pertaining to cyber security
A10	Ability to apply technical strategies, tools and techniques to secure data and information for customers/clients
Skills	
B1	Critically evaluate the needs for security provision for communication networks and apply security policies and regulations for existing security systems.
B2	Have a critical and clear understanding of current theories and techniques for apprising user interfaces and practical designs skills for effective user interactions
B3	Critically analyse and evaluate security applications and techniques and recommend and propose new measures to improve security
B4	Make informed choices of the appropriate security measures to put into place for a given network and/or an operating system
B5	Demonstrate fundamental security management skills and techniques relating to the leadership of projects.
B6	Daw up security measures for computer networks and communication systems
B7	Acquire and apply relevant mathematical techniques to carry our security algorithms
B8	Analyse a problem systematically and implement an effective solution both individually and within a group

B9	Communicate effectively with peers and senior managers in writing, verbally and through graphical notations.
B10	Apply learnt knowledge in computer and network security to better protect a networking environment

Programme outcomes																			
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Highest level achieved by all graduates																			
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7

Module Title	**Module Code by Level**	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Computer Networks and Internetworking	CST4500	✓	✓	✓		✓	✓	✓		✓			✓			✓	✓	✓	✓	✓	
Operating Systems for Networked Environments	CST4522		✓		✓	✓	✓	✓	✓		✓						✓	✓	✓	✓	
Security Solutions and Applications	CST4530	✓		✓		✓				✓	✓	✓		✓	✓	✓		✓			✓
Penetration Testing and Digital Forensics	CST4550	✓		✓	✓		✓		✓				✓				✓	✓			
Network Security and Mechanisms	CST4560		✓			✓		✓		✓				✓			✓	✓		✓	✓
Cyber Security and Legal Regulations	CST4590				✓	✓						✓	✓	✓	✓		✓		✓		
Individual PG Project	CST4990	✓	✓			✓		✓	✓	✓	✓				✓	✓			✓	✓	✓