PROGRAMME SPECIFICATION 2024-25		Newcastle University

1	**Awarding Institution**	Newcastle University
2	**Teaching Institution**	Newcastle University
3	**Final Award**	MSc
4	**Programme Title**	Cyber Security
5	**UCAS/Programme Code**	5144F/P
6	**Programme Accreditation**	British Computer Society
7	**QAA Subject Benchmark(s)**	Computing
8	**FHEQ Level**	7
9	**Date written/revised**	February 2024
10	**Programme Aims**	

1. To equip students with the skills and knowledge required to develop, assess, and maintain the security of computer-based systems.
2. To provide a qualification enhancing employment prospects in cyber security
3. To develop research skills
4. To develop and improve key skills in written and oral communication and in teamwork.
5. To develop and improve skills in using the literature and information technology resources relevant to dependable computing.
6. To encourage the development of creativity skills
7. To develop skills in critical assessment, analysis, and storage of information
8. To provide a programme which meets the accreditation requirements of the appropriate professional bodies, thus providing a basis for further professional development and lifelong learning.
9. To address the relevant professional, legal, and ethical issues relevant to the development, assessment, and maintenance of secure systems
10. To provide an international perspective on developments in cyber security
11. To provide a programme which meets the FHEQ at Masters level and takes appropriate account of the draft subject benchmark statements in Computing.

11	**Learning Outcomes**

The programme provides opportunities for students to develop and demonstrate knowledge and understanding, qualities, skills, and other attributes in the following areas. The programme outcomes have references to the benchmark statements for Computing.

Knowledge and Understanding

On completing the programme students should be able to demonstrate:

A1 Understanding of the theory underpinning dependability and security.
A2 Understanding of the fundamental principles for information and system security.
A3 Knowledge of the major methods for assessing system security.
A4 Knowledge of machine learning and artificial intelligence techniques, and their impact on society.
A5 Understanding of the technologies for the design of trustworthy interactive systems, including human and cyber-physical aspects.
A6 Understanding of the computer aided verification techniques relevant to security.
A7 Knowledge of real-world case studies involving security and data science.
A8 Understanding of major professional, legal, and ethical issues associated with work in secure and resilient computing systems.
A9 Understanding of the international character of contemporary developments in security and resilience.

Teaching and Learning Methods

The primary method of imparting knowledge and understanding is lectures supported by practical work in classes and laboratories (A1-A9). Fundamental motivation (A1), is further reinforced through the exploration of fundamental aspects, methods and technologies (A2-A6). Knowledge of applied technologies (A2-A6), is assisted through the practical laboratory work in addition to the lectures. Professional, legal and ethical issues (A8) are addressed explicitly in the dependability context and reinforced in the core technical modules and again in the group project. The international character of developments in the subject (A9) is emphasised in the research methods module and individual project. Through the many case studies underpinning studies in secure systems (A7), students will be encouraged to deepen understanding by independent reading in the relevant technical and scientific literature, supported by guidance in information literacy skills (in induction and prior to the group and individual projects) and subject-specific guidance given in lectures.

Assessment Strategy

Technical knowledge and understanding are primarily assessed through coursework (A1-9), aiming at providing an authentic and constructive assessment, engaging practical skills and critical thinking.

Intellectual Skills

On completing the programme students should:
B1   Be able to propose, conduct and write up a research project involving, where appropriate, a literature review, problem specification, design, verification, implementation, and analysis.
B2   Have expertise in the use and applicability of up-to-date security tools.
B3   Be able to apply the leading design techniques for security in network and internet environments, including cryptography and public key infrastructures.
B4   Be able to apply up-to-date machine learning methods.
B5   Be able to assess the main social and technical factors relevant to secure system operation.
B6   Be able to organise and take part in systematic security analyses of existing systems.
B7   Be able to discuss the security implications of real-world case studies.
B8   Be able to assess the impact of AI systems in situated use.

Teaching and Learning Methods

Intellectual skills are imparted through lectures on research project planning (B1) and through one-to-one and small group supervisions during the individual project. Specific tools and methods skills (B2-B4) are introduced in practical classes. Assessment skills (B5-B8) are introduced through practical case studies in taught modules. Throughout the programme, the emphasis is on skills development through practical experience. Students are encouraged to acquire relevant skills through the group and individual projects, which have a research element (B1); individual modules' laboratory classes in design (B2-B4), and assessment methods (B5-B8). The group project aims to encourage students to learn how skills specific to sub-disciplines (B2-B8) interact in design and assessment.

Assessment Strategy

Intellectual skills are primarily assessed by means of reports, designs and software developed by students in coursework activities and private study (B2-B7). The individual project deliverables (proposal, presentation, and dissertation) are the main vehicles for assessment of B1. Reports from individual and group projects are used for assessment of B2-B4. For B5-B7, assessment is based on project reports from coursework supplemented by focussed problems on unseen written examinations.

Practical Skills

On completing the programme students should be able to:

C1 Critically evaluate research and literature relating to security and resilience of computer-based systems.
C2 Evaluate and use appropriate tools and techniques.
C3 Undertake critical evaluation (theoretical and empirical) of alternative solutions
C4 Solve design problems.

Teaching and Learning Methods

Practical skills are developed through practical study skills sessions in information research and literacy (C1) and practical design classes as part of the practical component of each module (C2,3,4). Students are encouraged to acquire these skills through preparing seminars and presentations on current topics in computer security (C1), through the preparation and presentation of design and tooling alternatives in practical classes and the group project (C2,3,4)

Assessment Strategy

Practical skills are primarily assessed through practical work. C1 is assessed through specific coursework exercises, a seminar and dissertation at the end of the individual project. C2-C4 are primarily assessed in individual and group-based coursework and the final project.

Transferable/Key Skills

On completing the programme students should have:

D1 The ability to communicate orally in a professional context.
D2 Written communication skills, including an appreciation of the role of peer review of papers, software, proposals and other research and development products.
D3 Information literacy skills, including the ability to use computer-based resources for research in the professional literature and the capacity to undertake critical review.
D4 The ability to work as part of a team, including group-based learning, research, and development activity.
D5 Creativity skills: recognising and responding to opportunities for innovation
D6 Planning and organisation skills.

Teaching and Learning Methods

Communication skills (D1,D2) are imparted through seminars on oral presentation and technical writing within the module on research skills, the group and individual projects. Skills in computer-based information resources (D3) are promoted through specialist classes provided in conjunction with the University Library's Information Literacy programme. Team working skills (D4) are developed in the group project module through introductory lectures on team working issues and guidance during the project. Creativity skills are introduced in practical classes, as well as the group and individual projects. Planning and organisation skills (D6) are stressed throughout the practical aspects of the programme, notably in the preparation for the group and individual projects. Students are encouraged to practise communication skills (D1) through group working, informal and formal presentations, and through written reports associated with practical exercises, the group and individual project (D2). Skills in using computer-based information resources (D3) are encouraged by research-related exercises. Team working skills (D4) are practised through students collaborating in a major team-based project. Creativity skills (D5) are encouraged by tackling design problems which grow in the level of challenge, from specialised technical modules to group and individual projects.

Assessment Strategy
Key skills are primarily assessed through practical work (D1-D6). D1 is assessed by means of student presentations following practical work involving research and literature review, in the group and individual projects. D2 and D3 are assessed via reports submitted as parts of coursework and project work, including a specific research skill module, as well as the final dissertation. D4-D6 is assessed primarily via observation of teams during the group project. D5 and D6 are additionally assessed by observation during the individual project.

12   Programme Curriculum, Structure and Features

Basic structure of the programme

The programme is studied over one-year full time, or two years part time. There is a single stage to the programme, requiring the study of 180 credits. A 10-credit module consists of 100 hours of student effort, covering lectures, practical classes, small group teaching and private study, completion of coursework and revision. Taught modules are either 10 or 20 credits. There is one 60-credit module containing the individual project. The programme is divided into three phases, with an overlap between Phase 2 and Phase 3.

Phase 1 lays foundations in the principles of computer security (A1-A2) and follows this with material on specialist sub-disciplines which develop core technical knowledge (A1-A6) and introduce professional (A7) and subject-specific skills through their practical and coursework components (B2-B8). This phase is composed of six 10-credit modules in Semester 1.

Phase 2 puts a stronger focus on critical analysis and reflection by exploring and assessing the security of complex systems, including social and technical elements (B6), as well as utilising and critically evaluating the impact of Human-AI concepts and technologies within their ecosystems (B8). The emphasis is also on developing professional and cognitive skills. Essential research and communication skills (C1, D1-D3) are explicitly developed in the research method module on topics of current research interest with a strong international emphasis (A9) as well as in a module exploring strategic case studies (A7,B7). A group project module is a major way of developing professional skills in development and evaluation (B3-B5, B7, B8) and cognitive skills relating to design and tools selection (C2-C4). Team working skills (D4) are explicitly developed. Other key skills in communication are developed through oral and written reporting (D1, D2) on planning and design activities in the project (D5, D6). This phase is composed of 40 credits in three modules in Semester 2 and 20 credits in Semester 3.

Phase 3 of the programme emphasises research skills, creativity, and management of independent work through a substantive research-related project selected by the student in consultation with an academic supervisor. It consists of an initial phase in which students are given further training in cognitive and key skills (C1, D2, D3, D6) essential to the management of an individual research-related project, culminating the production of an assessed research proposal. The execution of the project concentrates on the development of specific subject skills in the chosen project area (B1, B4, B7, B8), higher cognitive and key skills (C2, C3, C4, D2, D5, D6). This phase commences in Semester 2 and carries on to the end of the programme.

Duration: 1 year
Stages: 1
Credits: 180
Module credits:
Compulsory with the option to select between CSC8110 and CSC8635 in semester 1.
Semester 1: 6 taught modules, 5 of 10 credits and 1 of 20 credits.
Semester 2: 4 taught modules: 2 of 10 credits, and 2 of 20 credits
Semester 3: project (60 credits). |

Key features of the programme (including what makes the programme distinctive)
Modules in the first semester are taught in intensive mode.

Programme regulations (link to on-line version)
5144F/P Cyber Security MSc:

13	**Support for Student Learning**

Generic information regarding University provision is available at the following link.
Generic Information

Support for students with disabilities
The University's Disability Support team provides help and advice for disabled students at the University - and those thinking of coming to Newcastle. It provides individuals with advice about the University's facilities, services and the accessibility of campus; details about the technical support available; guidance in study skills and advice on financial support arrangements; a resources room with equipment and software to assist students in their studies.

Learning resources

The University's main learning resources are provided by the Robinson and Walton Libraries (for books, journals, online resources), and the University's IT Service (NUIT), which supports campus-wide computing facilities.

All new students whose first language is not English are required to take an English Language Proficiency Test. This is administered by INTO Newcastle University Centre on behalf of Newcastle University. Where appropriate, in-sessional language training can be provided. The INTO Newcastle University Centre houses a range of resources which may be particularly appropriate for those interested in an Erasmus exchange.

14	**Methods for evaluating and improving the quality and standards of teaching and learning**

Generic information regarding University provision is available at the following link.
Generic Information

Additional mechanisms None.

15	Regulation of assessment
Generic information regarding University provision is available at the following link. Generic Information	
In addition, information relating to the programme is provided in:	
The University Prospectus: https://www.ncl.ac.uk/postgraduate/degrees/ Degree Programme and University Regulations: http://www.ncl.ac.uk/regulations/docs/	
Please note. This specification provides a concise summary of the main features of the programme and of the learning outcomes that a typical student might reasonably be expected to achieve if she/he takes full advantage of the learning opportunities provided.	