<table>
<tr><td>PROGRAMME SPECIFICATION
(Taught Postgraduate)</td><td>Newcastle University</td></tr>
</table>

1	**Awarding Institution**	Newcastle University
2	**Teaching Institution**	Newcastle University
3	**Final Award**	MSc Cyber Security and Degree Apprenticeship
4	**Programme Title**	Digital and Technology Solutions Specialist Integrated Degree Apprenticeship - Cyber Security Specialist
5	**Programme Code**	5418P
6	**Programme Accreditation**	N/A
7	**QAA Subject Benchmark(s)**	Computing
8	**FHEQ Level**	Level 7
9	**Last updated**	May 2023

10 Programme Aims

1. To develop the multi-disciplinary skills, essential to fulfil the role profile, skills, knowledge and behaviours defined in the DA standard ST0482
2. To develop the multi-disciplinary skills, knowledge and behaviours essential to produce the L7 experts in Cyber Security required by academia and industry
3. To provide the fundamental computational knowledge and expertise required to tackle complex cyber security system design and strategic challenges
4. To provide and understanding of the most commonly used methods, approaches and algorithms for the design and management of secure computer and information systems
5. To provide leadership skills and behaviours as well as an understanding of technology & innovation management methods and approaches.
6. To develop and improve skills in the use of literacy resources and information technology
7. To encourage the development of creativity and problem-solving skills
8. To provide a qualification that enhances employment prospects in cyber security
9. To provide a programme that meets the accreditation requirements of the appropriate professional bodies, thus providing a basis for further professional development and lifelong learning.
10. To provide a programme that meets the FHEQ at Masters Level and takes appropriate account of subject benchmarks in QAA Computer Science at Masters Level and UK professional standards.

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 QAA benchmark statements for Computing and Business & Management.

Knowledge and Understanding

On completing the programme students should have:

A1. Understanding of the theory and principles underpinning dependability, security and resilience in computer-based systems
A2. Knowledge of advanced techniques for assessing information security
A3. Knowledge of the major methods for assessing system security

A4. Knowledge of the major dependability techniques applicable in computing system design

A5. An understanding of major professional, legal and ethical issues associated with cyber security

A6. An understanding of the design of complex IT enabled business process, and the ability to design technology roadmaps, and transformation or change plans.

A7. An understanding of leadership and change management approaches and values in the digital era.

Teaching and Learning Methods

Technology specialist knowledge (A1-A5) is imparted largely through direct student contact (lectures and tutorials) and online blended delivery of content, supplemented by practical sessions that may take the form of computing sessions, problem solving and assessed coursework, and project work. Student understanding and learning is enhanced by the use of computing and numerical exercises, problem solving, literature reviews, teamwork and practical work.

Core (professional) skills knowledge (A6, A7) is similarly imparted through direct student contact (lectures), but with a yet stronger emphasis on online blended delivery of context, supplemented by problem solving, team work and project work.

Student understanding and learning for A1 through A7 is enhanced by the integration of case studies (including on the job), seminars, expert discussions, company presentations and practical individual and teamwork.

Independent learning is encouraged through the provision of reading lists, literature reviews and critical analysis of research papers, and ready access to online information sources. Adequate time is provided in all modules for private study for independent learning. The thesis will be integrated with the on-the-job DA capstone project of the degree apprenticeship and will enable students to devote extensive time to developing a deep understanding of a practically important specialist area.

Assessment Strategy

A mix of formative and summative strategies are used to assess problem solving and programming skills, group work and research exercises. Additional formative feedback, provided both in-person and online, is included to provide student feedback throughout the course, without contributing to module marks. Formal feedback is provided for each piece of assessed coursework in the form of an individual pro-forma and a review session in subsequent lectures. Summative strategies, in the form of extended project work, are used to assess a student's learning achievements, for key modules.

Alongside module assessments, student learning throughout the programme is tracked through evidence of students' reflective practice. Students will develop reflective logs and personalized action plans to articulate their personal development by mapping key learning outcomes embedded in assessed project work. Individual meetings between students and the DA tutors will support students in developing their reflective practice and will act as a common thread of dialogue between students and the course team throughout the programme.

Intellectual Skills

On completing the programme students should be able to:

B1. Propose, carry out and write an extended cyber security project involving, where appropriate, a literature and information review, problem specification, design, implementation and evaluation.

B2. Apply their knowledge of specific security assessment and enhancement techniques to complex existing computer and information systems and designs.

B3. Propose, carry out (lead) and write a technology transformation plan involving, where appropriate, a literature and information review, aim and objectives specification, design and assessment criteria. This includes technology review, business implication and change management approaches.

Teaching and Learning Methods
Intellectual skills are imparted by a combination of lectures, practicals, case studies, a group project and an in-depth capstone project tailored to individual interests. Modules are delivered in the form of 'short fat' modules that augment formally taught material with more directed self-learning including the use of interactive tutorials (both tutor and student led), self-directed study, laboratory practicals, problem-based learning and investigative work. The short fat modules are scheduled to support a day release model (up to two days a week during certain periods).   The use of short fat modules has several advantages; (i) key skills development and deep learning is enhanced due to increased student participation and interest; (ii) learning is concentrated, allowing the student to focus in depth on one subject at a time; (iii) modules have the potential to be made available as short courses aimed at continuing professional development (for industry or academia); and (iv) enables future extension of module choices. Practical sessions and problem-solving exercises are used to develop cyber security assessment and enhancement skills (B1-B2). Real-life case studies with a possible on-the-job element are used to develop strategic planning skills required in (B3). Tutorials support the interaction of the DA student with a designated tutor (B1-B3).

Assessment Strategy
Intellectual skills are continuously assessed through written reports, practical write-ups, case study documentation, literature and information projects, oral presentations, poster presentation and a capstone project. The assessment methods aim to evaluate the students' understanding and ability to apply computational techniques that form the basis for the interdisciplinary occupation as cyber security technologist or analyst (B1-B2). It also aims to assess the ability to design and carry out strategic technology change programmes (B3).

Practical Skills
On completing the programme students should be able to: C1. Critically evaluate research, literature and popular information related to cyber security aspects in the role as cyber security technologist or analyst C2. Solve cyber security system design and assessment challenges using appropriate tools and techniques C3. Plan, articulate, socialize and carry out strategic technology change efforts, including working in teams and with specialists, based on a critical appraisal of methods known in literature and the practical adoption of leadership and change management methods.

Teaching and Learning Methods
Critical evaluation of current techniques and methods (C1 and C3) will be developed through literature searching, searching through online sources, coursework exercises and in the capstone project. The ability to address cyber security challenges (C2) will be acquired through practical sessions and self-directed learning, as well as tutorials and group discussions. The practical skills associated with change management, and the leadership in technology transformation (C3), will be acquired through expert presentations, group discussions and practical projects associated with the change management and leadership modules.

Assessment Strategy
Practical skills (C1-C3) are primarily assessed continuously in the form of individual reports from practical studies, literature and information reviews, tutorial exercises, group project reports and the capstone project report. Data and information handling and interpretation (C2) are a strong component of many modules and are also assessed through continuously assessed problem solving exercises. Practical skills in leadership, change management and technology strategy are assessed through reports for case studies, with a potential on-the-job component.

Transferable/Key Skills
On completing the programme students should have the following skills:

D1. Communicate complex matters orally successfully to a wide audience
D2. Use written communication skills to communicate technology strategy to a wide audience
D3. Use computer based literacy resources
D4. Work as part of a team and the ability to use leadership skills
D5. Deploy skills to manage for change in a digital age

Teaching and Learning Methods

Oral presentation skills (D1) are exercised by group discussions in tutorial sessions, by communicating during group exercises (also D4) and by preparation of oral presentations on specific research topics. Written communication skills (D2) are developed during independent study, the preparation of coursework, the writing of essays, poster presentation and through the completion of group project report as well as capstone project report. Formal lectures and practicals address the use of online literacy resources, reinforced through the use of practice exercises (D3). Group project, on-the-job components of exercises and projects as well as student-led tutorials are used to develop team skills (D4), while leadership skills (D4) are developed in addition through participation in lectures as well as exercises. Change management skills (D5) are developed through participation in projects, and during the capstone project.

Assessment Strategy

Written communication skills are assessed by report preparation, the capstone project report and literature reviews. Oral communication skills are assessed in oral presentations. The ability to use computer-based literacy resources is assessed through the preparation of literature and online information reviews and through peer- and self-assessment. Team work is formally evaluated using group-based problem solving and technology exercises. Independent work is assessed in literature and information reviews and projects. Leadership as well as change managerial skills are assessed through exercises and as element in the capstone project.

12	Programme Curriculum, Structure and Features

Basic structure of the programme

The programme is studied over two years, and follows the degree apprenticeship rules of 20% of-the-job training and education. The programme consists of three parts: (1) a Specialist Skills taught component of 60 credits that runs in term time, (2) a Core Skills taught component of 60 credits that runs between term times and (3) a 60 credits capstone project that runs at the end of the two year period. The programme is centred in the School of Computing, where the students will be based, and draws resources and leadership from Newcastle University's £2m strategic project 'Institute of Coding' (until July 31st, 2021). Due to the interdisciplinary nature of the course, some modules are delivered by members of Newcastle University Business School.

The programme consists of mandatory modules and the major capstone project and the End Point Assessment. The programme provides comprehensive training in interdisciplinary aspects of Computing Science and Business. The taught component of the course accounts for 120 credits, the capstone project for 60 credits.

Key features of the programme (including what makes the programme distinctive)

The DA in Cyber Security will deliver trained postgraduate students who have advanced knowledge, skills and behaviours that will equip them for a career as cyber security technologist or analyst. Particular features of the programme are:

Industry participation: DA students are employed by industry, with a 20% off-the-job interaction with the degree programme. The participation of industry includes the provisioning of on-the-job project opportunities and hosting the capstone project of the student. The students will thus receive general disciplinary knowledge and skills as well as aspects of the course tailored to participants' interests. The employment of the student ensures meaningful industry engagement for each DA student.

Flexible learning: given the non-standard interaction of DA students with the MSc, we are exploring and are investing in blended learning approaches to facilitate participation from a broad range of candidates. Novel assessment methods centred around extended project work and reflective interviews augment the Cyber Security and Resilience MSc that forms the basis of this L7 degree apprenticeship degree. These offer an alternative to written examination, more amenable to industry participation, and support students to develop a rich portfolio of experience in the area of Cyber Security.

Tailoring provision of sectoral and organisational variations: Our teaching provision is designed to be scalable, while accommodating tool preferences of participants, their employers and the broader sector. Taught concepts are situated in context, drawing on application areas relevant to participants.

Project Work: Every DA student will conduct their capstone project within the company, while receiving input from Degree Apprenticeship tutors and their workplace mentors. These work-based capstone projects are tailored to the needs of the DA student and the company, and participants will document a work-based project to apply their skills obtained during the course, for real problems faced by the employer. This will be underpinned by a portfolio of evidence, with supporting reflective accounts.

Programme regulations (link to on-line version)

-R5418P.pdf (ncl.ac.uk)

---

13   Support for Student Learning

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

---

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

Accreditation reports
This programme is not accredited by any professional body.

Additional mechanisms
Turnitin and MOSS are routinely used by the School to detect plagiarism where appropriate.

---

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/

Degree Programme and University Regulations: http://www.ncl.ac.uk/regulations/docs/

21-Aug-23