University of Suffolk

DEFINITIVE COURSE RECORD

Course Title	**BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst)**
Awarding Body	**University of Suffolk**
Level of Award[1]	**FHEQ Level 6**
Professional, Statutory and Regulatory Bodies Recognition	**Tech Skills**
Credit Structure[2]	**360 Credits** **Level 4: 120 Credits** **Level 5: 120 Credits** **Level 6: 120 Credits**
Mode of Attendance	**Part-time**
Standard Length of Course[3]	**3 years 1 semester part time OR 4 years part-time**
Intended Award	**BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst)**
Named Exit Awards	**CertHE Digital & Technology Solutions (Cyber Security Analyst)** **DipHE Digital & Technology Solutions (Cyber Security)**
Entry Requirements[4]	**Typical offer: Applicants should normally have BBC at A-level or DMM at BTEC (112 UCAS tariff points).** **All applicants must have Level 2 English and Maths at GCSE grade C or above (or equivalent).** **All applicants must additionally be on the appropriate apprenticeship scheme with an employer**
Delivering Institution(s)	**University of Suffolk**
UCAS Code	**N/A**

This definitive record sets out the essential features and characteristics of the BSc (Hons) Digital & Technology Solutions (Cyber Analyst) course. The information provided is accurate for students entering level 4 in the 2023-24 academic year[5].

Course Summary

The BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst) degree programme at the University of Suffolk is fully accredited as meeting the standard of the Digital & Solutions Technology Professionals degree apprenticeship. It equips graduates with the knowledge and hands on skills required by employers in the IT and telecommunications sectors. They are

[1] For an explanation of the levels of higher education study, see the QAA Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies (2014)
[2] All academic credit awarded as a result of study at the University adheres to the Higher education credit framework for England.
[3] Where the course is delivered both full-time and part-time, the standard length of course is provided for the full-time mode of attendance only. The length of the part-time course is variable and dependent upon the intensity of study. Further information about mode of study and maximum registration periods can be found in the Framework and Regulations for Undergraduate Awards.
[4] Details of standard entry requirements can be found in the Admissions Policy and further details about Disclosure and Barring Checks (DBS) can be found on the University's DBS webpage.
[5] The University reserves the right to make changes to course content, structure, teaching and assessment as outlined in the Admissions Policy.

designed to give students opportunities to acquire the specialist academic knowledge, practical skills and industrial certification that will help secure employment in this competitive economy. Graduates will have achieved core competencies in network engineering, software engineering, data analysis, cyber security, business analysis and project management. In addition, graduates will have achieved the specialist competency of Cyber Security Analyst on the Digital & Technology Solutions framework, and additionally covered the knowledge and skills expected of Data Analysts and Cyber Security Analysts.

Course Aims

- Provide students with a sound knowledge and understanding of software engineering.
- Enable students to be proficient in the specification, design, creation, testing and roll-out of software products.
- Provide students with comprehensive knowledge and understanding of cyber security for networks, software and systems.
- Enable students to be proficient in the design and implementation of cyber security elements of networks, software and systems.
- Provide students with sound knowledge, understanding and practical skills in advanced cyber security topics (including strategy, assurance, penetration testing and digital forensics).
- Enable all apprentices on the Cyber Security Analyst Pathway to achieve the specialist competencies of Cyber Security Analyst on the Digital & Technology Solutions framework
- Enable all apprentices on the Cyber Security Analyst Pathway to successfully achieve their end-point competency as Cyber Security Analysts
- Help students develop competencies in effective interpersonal and business communication, presentation skills, business and project management;
- Help students develop the personal qualities and professional attributes required by employers (these include: reliability, integrity, ethical approach, dependability, team work and reflection);
- Encourage students to understand their own technological responsibilities in the context of the client organisation and its commercial and business operation;
- Develop students' ability to take responsibility for their own learning and professional development.

Course Learning Outcomes

The following statements define what students graduating from the BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst) course will have been judged to have demonstrated in order to achieve the award. These statements, known as learning outcomes, have been formally approved as aligned with the generic qualification descriptor for level 6 awards as set out by the UK Quality Assurance Agency (QAA)[6].

1. Express and employ detailed knowledge and systematic understanding of essential facts, concepts, principles and theories, both established and emergent, relating to cyber security for software, networks, and systems.

2. Express and employ detailed knowledge and systematic understanding of essential

[6] As set out in the QAA Frameworks for Higher Education Qualifications of UK Degree-Awarding Bodies (2014)

facts, concepts, principles and theories, both established and emergent, relating to advanced topics in computing.

3. Utilise knowledge and skills relating to cyber security to analyse, develop and deploy ethical “cyber attacks” for essential penetration testing of software, networks and systems, and to analyse, develop and deploy cyber defences in depth to protect software, networks, and systems, using both established and bleeding-edge techniques as appropriate.

4. Utilise knowledge and skills relating to advanced topics in cyber security to analyse cyber security issues in multiple domains and scale, and to identify and deploy relevant solutions to appropriate problems, using both established and bleeding-edge techniques as appropriate.

5. Understand, describe, and comment upon the literature and cutting edge research in cyber security and specific areas of computing, and appreciate the associated uncertainties, ambiguities, and limits to knowledge at the forefront of the discipline.

6. Apply methods and techniques learned in cyber security to consolidate, extend, and apply knowledge and understanding to extended realistic and real-world projects.

7. Apply detailed knowledge, systematic understanding, and mastered techniques to initiate and execute their endpoint project in cyber security and multiple minor projects in different topic areas.

8. Critically evaluate arguments, concepts, requirements, constraints and data in order to make rational judgements on appropriate algorithms, methods, and configurations leading to the assessment and production of a cyber security solution or identification of a class of solutions to significant problems

9. Present ideas, information, analyses, designs, implementations, tests and results relating to cyber security, critically, comprehensibly and succinctly to both specialist and non-specialist audiences.

10. Deploy appropriate established and/or cutting edge theory, practices and tools for the successful attack and defence of software, networks and systems.

11. Recognise the legal, ethical and professional issues in all aspects of cyber security, and be able to exercise initiative and personal responsibility in cyber security.

12. Research, analyse, evaluate implement, test, utilise and document cyber security solutions to address specific problems, using their knowledge, understanding and technical skills in cyber security,

13. Develop an understanding of a specialist subject or problem area in software to a level where they can effectively evaluate it, analyse possible solutions, design an appropriate solution and bring that solution to a successful conclusion in a defined time-frame, showing by doing so their capabilities and readiness for lifelong learning

and professional training.

14. Evidence the qualities and transferable skills necessary for graduate-level employment requiring the exercising of initiative, personal responsibility, and decision making, through working individually and in groups on mini-projects, extended case studies and scenarios, and their major project in cyber security.

15. Identify appropriate practices considering equality, diversity, and inclusion (EDI) as well as any economic, social, and environmental impact.

Course Design
The design of this course has been guided by the following QAA Benchmarks and Apprenticeship Standards:

- QAA Subject Benchmark in Computing (2022)
- Digital & Technology Solutions Professional apprenticeship standard (version 2.1, 2016)

Course Structure
The BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst) comprises modules at levels 4, 5 and 6.

Module Specifications for each of these modules are included within the course handbook, available to students on-line at the beginning of each academic year.

	Module	Credits	Module Type[7]
Level 4			
	Computing Fundamentals	20	R
	Introduction to Networking	20	R
	Personal and Professional Development	20	R
	Introduction to Programming	20	R
	Operating Systems	20	R
	Foundations of Management	20	R
Level 5			
	Relational Databases	20	R
	Advanced Networking Concepts	20	R
	Software Design Development and Engineering	20	R
	Cyber Security Fundamentals	20	R
	Research Skills	20	M
	Cyber Security Tools and Techniques	20	R
Level 6			

[7] Modules are designated as either mandatory (M), requisite (R) or optional (O). For definitions, see the Framework and Regulations for Undergraduate Awards

	Cyber Security for the Enterprise	20	R
	Cyber Security: Attack	20	R
	Cyber Security: Defence	20	R
	Applied Cyber Security	20	R
	Emergent Technologies	10	R
	Synoptic Project (Cyber Security Analyst)	30	M

Awards
On successful completion of the course, students will be awarded a BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst). Students who leave the course early may be eligible for a DipHE Digital & Technology Solutions (Cyber Security Analyst) on successful completion of 240 credits including the mandatory module at level 5, or a CertHE Digital & Technology Solutions (Cyber Security Analyst) on successful completion of 120 credits.

Course Delivery
The course is delivered at Ipswich. Students studying full-time on BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst) are likely to have approximately 228 contact hours for level 4, 228 contact hours for level 5 and 198 contact hours for level 6. The contact hours will be a mix of lectures, practicals, seminars and workshops according to the nature of the module. As students will be apprentices, they will also be in full-time work-based employment and training with their employer when not at university. Students will normally be expected to undertake at least 6 hours per module of independent study in an average week, but should be prepared for this to vary based on assignment deadlines and class exercises.

Course Assessment
A variety of assessments will be used on the course to enable students to experience and adapt to different assessment styles. The assessment methods used will be appropriate to assess each module's intended learning outcomes. Assessment on the course overall will be mostly coursework (including assignments, dissertations, essays, reports, presentations, group work, reflective learning journals and research projects), and five examinations and practical time-constrained assessments.

End Point Assessment
All students on the course undertake an End Point Assessment (EPA) to complete their Digital & Technology Solutions Professional apprenticeship Students will be expected to undertake the EPA as part of their degree. The EPA will be delivered by the University. The EPA will be 100% coursework (including project, dissertation and presentation). Following successful completion of the EPA students will achieve their Digital & Technology Solutions Professional (Cyber Security Analyst) apprenticeship and BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst) degree.

Special Features
The BSc (Hons) Digital Technology Solutions (Cyber Security Analyst) [degree apprenticeship] course meets the requirements of the Digital Technology Solutions Professional (integrated degree) apprenticeship standard and is accredited as Tech Industry Gold by Tech Skills, the digital sector's industry accreditation body.

Course Team

The academic staff delivering this course are drawn from a team that includes teaching specialists, active researchers and current practitioners. All staff are qualified in their subjects with their own specialist knowledge to contribute.

Course Costs

Students undertaking BSc (Hons) Digital & Technology Solutions (Cyber Security Analyst) will not be charged tuition fees directly. Tuition fees will be agreed between the University and a student's employer. Students will be required to sign a commitment statement before starting their apprenticeship which will detail the student's, employer's and University's expectations under the apprenticeship agreement.

Students may choose to enrol onto certification exams – details of the costs of these will be advised when available. Taking certification exams is not a mandatory part of the degree.

Academic Framework and Regulations

This course is delivered according to the Framework and Regulations for Undergraduate Awards and other academic policies and procedures of the University and published on the website.