University of Suffolk

DEFINITIVE COURSE RECORD

Course Title	**BSc (Hons) Cyber Security**
Awarding Bodies	**University of Suffolk**
Level of Award[1]	**FHEQ Level 6**
Professional, Statutory and Regulatory Bodies Recognition	**None**
Credit Structure[2]	**360 Credits** **Level 4: 120 Credits** **Level 5: 120 Credits** **Level 6: 120 Credits**
Mode of Attendance	**Full-time**
Standard Length of Course[3]	**3 years full-time**
Intended Award	**BSc (Hons) Cyber Security**
Named Exit Awards	**DipHE Cyber Security** **CertHE Cyber Security**
Entry Requirements[4]	**112 UCAS tariff points (or above)** **BBC (A-Level), DMM (BTEC)** **GCSE mathematics at Grade C or equivalent**
Delivering Institution(s)	**Ipswich**
UCAS Code	**I102**

This definitive record sets out the essential features and characteristics of the BSc (Hons) Cyber Security course. The information provided is accurate for students entering level 4 in the 2018-19 academic year[5].

Course Summary

Our society has become entirely dependent on information technology, and we are at constant risk of attack by hackers and cyber criminals. Designing, creating testing and rolling-out secure software requires high degrees of skill. Big and Rich Data are driving innovation and growth across the economy – representing, storing, and transforming data to derive insights requires expertise. Data, networks, software, systems and organisations require effective security to protect personal information, business value, our very lives and liberty.

[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
[5] The University reserves the right to make changes to course content, structure, teaching and assessment as outlined in the Admissions Policy.

DEFINITIVE COURSE RECORD

This degree will provide you with an in-depth technical knowledge and hands-on skills in every dimension of cyber security – data, hardware, networks, software, systems and organisations. This is complemented with additional competencies in networks, operating systems, computer programming, software engineering, relational databases, and big data. Therefore, the course will help you become highly-competent sought after professional graduates.

Course Aims

The course aims are:

- Provide students with a sound knowledge and understanding of software engineering and data analysis
- Enable students to be proficient in the specification, design, creation, testing and roll-out of software products.
- Enable students to be proficient in the specification, design, creation, manipulation and usage of database and information engineering solutions
- Provide students with comprehensive knowledge and understanding of cyber security for data, networks, software, systems and organisations.
- Enable students to be proficient in the design and implementation of cyber security elements of data, networks, software, systems and organisations
- 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) Cyber Security 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 4/5/6 awards as set out by the UK Quality Assurance Agency (QAA)[6].

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

Knowledge and understanding

1. Express and employ detailed knowledge and systematic understanding of essential facts, concepts, principles and theories, both established and emergent, relating to advanced topics in cyber security and forensics

2. Express and employ detailed knowledge and systematic understanding of essential facts, concepts, principles and theories, both established and emergent, relating to advanced topics in information engineering

3. Utilise knowledge and skills relating to cyber security to analyse, develop and deploy advanced cyber techniques to attack and defend systems using both established and bleeding-edge techniques as appropriate.

4. Utilise knowledge and skills relating to advanced topics in information engineering, cyber forensics and computing to analyse, specify, develop and deploy technical 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.

Cognitive skills

6. Apply methods and techniques learned in cyber security, forensics and advanced topics in data analysis 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 final-year project 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, designs, methods, and configurations leading to the necessary analysis, design, implementation, and/or testing of a 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, forensics data analysis or computing, critically, comprehensibly and succinctly to both specialist and non-specialist audiences.

Subject-specific skills

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, design, implement, test, utilise and document computing solutions to address specific problems, using their knowledge, understanding and technical skills in cyber security, forensics, data analysis, and computing.

Key/transferable skills

13. Develop an understanding of a specialist subject or problem area in cyber security or computing 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

Course Design

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

- the QAA 2016 Computing subject benchmark (http://www.qaa.ac.uk/en/Publications/Documents/Subject-benchmark-statement-Computing.aspx.pdf)
- the Framework for Higher Education Qualifications (2008, 2014) (FHEQ)
- the emerging standard for the Cyber Security Technical Professional Level 6 degree apprenticeship.

Course Structure

The BSc (Hons) Cyber Security comprises modules at levels 4, 5 and 6.

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

	Module	Credits	Module Type[7]
Level 4			
	Platforms	20	R
	Networking Overview	20	R
	Introduction to Programming	20	R
	Operating Systems	20	R
	Introduction to Cyber-Security	20	Mandatory

[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: Management, Ethics and Law	20	R
Level 5			
	Software Design and Development	40	R
	Introduction to Relational Databases	20	R
	Advanced Networking Concepts	20	R
	Human and System Cyber-Security	20	R
	Research Skills	20	M
Level 6			
	Cyber-Physical Security	20	R
	Strategic Cyber-Security	20	R
	Cyber Forensics and Intrusion Management	20	R
	Information Engineering	20	R
	Project and Dissertation	40	M

Awards

On successful completion of the course, students will be awarded a BSc (Hons) Cyber Security. Students who leave the course early may be eligible for a DipHE Cyber Security on successful completion of 240 credits including all mandatory modules at levels 4 and 5, or a CertHE Cyber Security on successful completion of 120 credits including all mandatory modules at level 4.

Course Delivery

The course is delivered at Ipswich. Students studying full-time on BSc (Hons) Cyber Security are likely to have approximately 228 contact hours for level 4, 224 contact hours for level 5 and 180 contact hours for level 6 The contact hours will be a mix of lectures, seminars, practical classes, and tutorials. Students will normally be expected to undertake 30 hours 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 approximately 83% coursework (including essays, reports, presentations, software projects, software portfolios, research projects and dissertation) and 17% time-constrained practical assessments (5 in total).

Course Team

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

Course Costs

Students undertaking BSc (Hons) Cyber Security will be charged tuition fees as detailed below.

Student Group	Tuition Fees
Full-time UK/EU	£9,250 per year
Part-time UK/EU	£1,454 per 20 credit module
Full-time International	£13,000 per year
Part-time International	£2,165 per 20 credit module

Payment of tuition fees is due at the time of enrolment and is managed in accordance with the Tuition Fee Policy.

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.

There is no regular requirement for students to pay additional course fees. Where supplementary activities are offered there may be a small charge to cover their cost (for example, for transport).

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.