University of Bedfordshire

Course Information Form

This Course Information Form provides the definitive record of the designated course

Section A: General Course Information

Course Title	Cybersecurity; Cybersecurity (with Professional Placement Year); Cybersecurity (with Foundation Year) - COPY
Final Award	BSc (Hons)
Route Code	BSCYSAAF /BSCYPAAF/BSCYFAAF
Intermediate Qualification(s)	
FHEQ Level	6
Location of Delivery	University Square Campus, Luton
Mode(s) and length of study	Full-time over 3 years Full-time with Professional Practice Year over 4 years Part-time pathway typically over 6 years
Standard intake points (months)	October and February
External Reference Points as applicable including Subject Benchmark	QAA Subject Benchmark Statement Computing (2016) QAA FHEQ level descriptors (2014) SEEC Credit Level Descriptors (2016)
Professional, Statutory or Regulatory Body (PSRB) accreditation or endorsement	N/A

HECoS code(s)	100376
UCAS Course Code	I190

Course Aims	This BSc (Hons) degree will provide you with a programme of learning designed to meet your career ambitions focusing on the following educational aims: Develop your critical understanding of the cybersecurity theories, methodologies and techniques used by Information cybersecurity consultants Be able to understand and analyse multistage cyber-attacks and provide proper controls in place to mitigate their risks and impact in a holistic approach to improve cyber defence capabilities Understand information governance, risk, and compliance frameworks, standards and their implications to an Information security management system To be exposed to a wide range of pedagogical approaches to increase critical synthesis skills required to produce innovative solutions in both tactical and operational security. To gain in-depth understanding in technical aspects around network defence and offence with strong system administration elements embedded in the learning process Exhibit the ability to design, develop, test, and debug secure software using industry based software development life cycle methodologies Enhance logical thinking and be able to demonstrate a "security mind set" in both autonomous and collaborative tasks around network and systems' defence

Upon successful completion of your course you should meet the appropriate learning outcomes for your award shown in the table below

	Outcome	Award
1	Define and justify security access policies for an information security management system given knowledge of its core architecture, security requirements, secure software development, and threat/risk landscape.	BSc (Hons) Cybersecurity

Course Learning Outcomes	2	Demonstrate a systematic understanding of technologies, methodologies and processes related to systems and network security, and develop decision making and problem solving capabilities.	BSc (Hons) Cybersecurity
	3	Acquire strong technical expertise and a critical awareness of security implications, methodologies and frameworks applied to modern information security management systems to safeguard organisations and their assets.	BSc (Hons) Cybersecurity
	4	Adapt knowledge of legal and regulatory requirements and guidelines in governance, risk, and compliance processes and evaluate their performance in multiple organisational contexts.	BSc (Hons) Cybersecurity
	5	Perform a business impact analysis in response to a security incident and follow a disaster recovery plan to meet elements of a given business continuity policy.	BSc (Hons) Cybersecurity
	6	Apply critical thinking and problem solving skills in order to undertake a series of team-based activities in security auditing and analysis; adhering to national and international laws, professional ethics, and codes of conduct in the context of cybersecurity.	BSc (Hons) Cybersecurity
	7	Demonstrate your transferable skills (oral and written communication, and personal reflection) to analyse self and other actions in enabling a wide range of vocational outputs within an organisational context.	BSc (Hons) Cybersecurity
	8	Undertake a substantial independent piece of work that tackles a complex problem in the area of cybersecurity, using incomplete information. The work undertaken should demonstrate the ability to analyse, evaluate and synthesise available information and apply an appropriate problem solving approach.	BSc (Hons) Cybersecurity
	9	Demonstrate knowledge and analytical understanding of professional practice by successfully completing an approved period of approved work place practice.	BSc (Hons) Cybersecurity (with Professional Practice year)

Learning and Teaching

A wide variety of teaching modes will be used throughout this course. The most important aspect will be a student-centred approach, and we will encourage you (through relevant guidance) to become an independent thinker who can take responsibility for your own learning. We will also help you to develop skills so that you can adapt to a wide variety of different situations. The

	course will make use of traditional lectures and practical sessions as well as encouraging you to engage in various scenarios (e.g. managing your own projects, team working etc.). In addition, some units will use podcasts/videos to provide you with an overview/summary of different topics.
	All the teaching resources are available in a web site – a virtual learning environment that includes references and links, general unit and course information, discussion groups, tests and assessments. This VLE (Virtual Learning Environment) is available outside of the University to enrolled students.
	The unit 'Agile Project Management' in particular requires you to work in a team so as to apply a current project management methodology that embraces all of these knowledge areas in an integrated way while going through the stages of planning, execution and project control; you will work as part of a team, take responsibility and make autonomous decisions that impact on the project team performance.
	In addition, the honours project fosters independent and autonomous study, typically derived from your own ideas, in collaboration with a dedicated member of the teaching staff as project supervisor. That gives the ability to initiate discussion and project ideas that enrich the academic context in your studies and provide the foundations for a solid, relevant, and strong thesis.
	The diverse skillset around management of security as delivered in the course will equip you with a meaningful Governance, Risk and Compliance (GRC) knowledge and relevant experience to excel in your career prospects. This is quite prominent due to the problem recruiters having to get hold off security managers with these skills. Interactive sessions in the form of demonstrations will also be delivered by the teaching staff and guest speakers to further leverage understanding and stimulate attention towards relevant and pragmatic issues linked to existing challenges, issues, and opportunities in your subject area.
Teaching, learning and assessment strategies	The final year devotes 60 credits to the honours project. While the undergraduate project relates to the student working as an individual the 30 credit unit Agile Project Management addresses student interaction within a professional environment. The students have to work in a group and make decisions within professionally arranged project meetings.
	Our teaching is centred upon students, aiming to build their confidence by providing timely and informative feedback under the guidance of their tutor.
	Assessment
	You are assessed in a variety of ways. The majority of units are assessed through coursework, group and individual projects, portfolios, essays, presentations or exams. You will also produce software artefacts in the area of your specialism. Constant feedback and advice from a supervisory or unit team will be provided to support you in your studies.
	You are required to comprehend the basic range of intellectual concepts which form the foundations of the subject and application area, and will be assessed on your ability to articulate such concepts in a coherent manner. There are opportunities for formative assessment particularly through guided learning. Written assessments are used to allow the students to reflect on their

experiences in the workplace and to consider steps they could take to apply their learning. E-Portfolios allow students to collect evidence of work they have completed as well as examples and applications of their knowledge from course. Students may also be required to make technical presentations.

At level 4 you are assessed on your understanding of the fundamental concepts of Computer Science and its applications. Students will also be introduced to fundamental theory around data analytics and its applications to network defence underpinned by the basics of information security principles.

At level 5 you are assessed on your ability to apply the basic concepts of the disciplines introduced in level 4 to existing controversies and issues on which there is already a body of research and critical opinion.

At level 6 you will be required to demonstrate independent thinking and initiative. This may be in the form of analysing and criticising current approaches and theory within cybersecurity, malware analysis, and GRC frameworks. In all cases, you will be expected to show an awareness of the major theories and practices of the discipline. You will progress from well-defined briefs to more open-ended and challenging assessments, which culminate in the honours project – where you will be given freedom to choose your area of work.

Learning support	The University's comprehensive student support service includes: Student Information Desk, a one-stop shop for any initial enquiries; Student Support team advising and supporting those with physical or learning needs or more general student well being; Study Hub team providing academic skills guidance; Personal Academic Tutoring system; a student managed Peer-Assisted Learning scheme; support from your lecturers
Admissions Criteria	https://www.beds.ac.uk/entryrequirements **Approved Variations and Additions to Standard Admission** N/A
Assessment Regulations	https://www.beds.ac.uk/about-us/our-university/academic-information **Note: Be aware that our regulations change every year** **Approved Variations and Additions to Standard Assessment Regulations'** N/A

Section B: Course Structure

The Units which make up the course are listed below. Each unit contributes to the achievement of the course learning outcomes either through teaching (T), general development of skills and knowledge (D) or in your assessments (A).

Unit	Unit Name	Level	Credits	Core or Option	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CIS093-1	Mathematics and Concepts for Computational Thinking	4	30	Core		T12					T2								
CIS095-1	Databases and Computer Networks	4	30	Core	T12	T1						T2							
CIS096-1	Principles of Programming and Data Structures	4	30	Core	T12	T12	T12												
CIS097-1	Principles of Information Security	4	30	Core	T1							T2							
CIS022-2	Wireless communications and Networking	5	30	Option	D12							D2							
CIS121-2	Cyber Defence and Information Governance	5	15	Core	D12	D12	D12	D12	D12	D12	D2								
CIS122-2	Ethical Hacking	5	15	Core		D12					D12	D12							
CIS123-2	Information Security Management and Emerging Technologies	5	30	Core	D12					D12									
CIS124-2	Network Programming	5	30	Option			D12	D12	D12	D12									
CIS125-2	Switching and Routing	5	30	Core		D1					D2								
CIS009-3	Incident Response	6	30	Core					A12	A12		A12							
CIS047-3	Agile Project Management	6	30	Core				A2		A12		A12							
CIS055-3	Undergraduate Project in Cybersecurity	6	60	Core	A12	A12	A12	A12	A12	A12	A12	A12							

Unit	Unit Name	Level	Credits	Core or Option	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CIS097-2	Professional Practice Year (Computer Science and Technology)	5	0	Core									DA12						

Section C: Assessment Plan

The course is assessed as follows :

BSCYSAAF- Cybersecurity

Unit Code	Level	Period	Core/Option	Ass 1 Type code	Ass 1 Submit wk	Ass 2 Type code	Ass 2 Submit wk	Ass 3 Type code	Ass 3 Submit wk	Ass 4 Type code	Ass 4 Submit wk
CIS093-1	4	SEMESTER 1	Core	IT-PT	6	PJ-ART	15				
CIS097-1	4	SEMESTER 1	Core	WR-GR	10	PR-OR	12				
CIS095-1	4	SEMESTER 2	Core	CW-CS	9	IT-PT	12				
CIS096-1	4	SEMESTER 2	Core	IT-PT	6	PJ-ART	13				
CIS121-2	5	SEMESTER 1	Core	WR-I	7	PJ-ART	14				
CIS122-2	5	SEMESTER 1	Core	WR-I	7	PJ-ART	12				
CIS123-2	5	SEMESTER 1	Core	PJ-ART	10	IT-PT	14				
CIS022-2	5	SEMESTER 2	Option	WR-GR	7	EX	15				
CIS124-2	5	SEMESTER 2	Option	IT-PT	8	PJ-ART	13				

CIS125-2	5	SEMESTER 2	Core	IT-PT	13	PR-OT	14			
CIS055-3	6	AY	Core	PJ-ART	11	PJ-PRO	12	PR-OR	15	
CIS009-3	6	SEMESTER 1	Core	WR-PR	9	CW-ESS	15			
CIS047-3	6	SEMESTER 2	Core	IT-PT	10	PJ-ART	15			

BSCYPAAF- Cybersecurity (with Professional Practice Year)

Unit Code	Level	Period	Core/Option	Ass 1 Type code	Ass 1 Submit wk	Ass 2 Type code	Ass 2 Submit wk	Ass 3 Type code	Ass 3 Submit wk	Ass 4 Type code	Ass 4 Submit wk
CIS097-2	5	TY	Core	CW-PO	33						

Glossary of Terms for Assessment Type Codes	
CW-CS	Coursework - Case Study
CW-ESS	Coursework - Essay
CW-PO	Coursework - Portfolio
EX	Exam (Invigilated)
IT-PT	Summative in-class test or phase test
PJ-ART	Coursework - Artefact
PJ-PRO	Coursework - Project Report
PR-OR	Practical - Oral Presentation
PR-OT	Practical - Other Skills Assessment
WR-GR	Coursework - Group Report
WR-I	Coursework - Individual Report
WR-PR	Coursework - Problem Based Report

Administrative Information	
Faculty	Creative Arts Technologies and Science
School	School of Computer Science and Technology
Head of School/Department	Paul Sant
Course Coordinator	Ali Mansour