Course Specification

Published Date:	29-Apr-2024
Produced By:	Multi Type Usr Record For All Personnel
Status:	Validated

Core Information

Awarding Body / Institution:	University of Wolverhampton		
School / Institute:	School of Engineering, Computing, and Mathematical Sciences		
Course Code(s):	CS019H01UV CS019H31UV	Full-time Part-time	3 Years 6 Years
UCAS Code:	I161		
Course Title:	BSc (Hons) Cybersecurity		
Hierarchy of Awards:	Bachelor of Science with Honours Cybersecurity Bachelor of Science Cybersecurity Diploma of Higher Education Cybersecurity Certificate of Higher Education Cybersecurity University Statement of Credit University Statement of Credit		
Language of Study:	English		
Date of DAG approval:	26/Sep/2016		
Last Review:	2015/6		
Course Specification valid from:	2015/6		
Course Specification valid to:	2021/2		

Academic Staff

Course Leader:	MD ARAFATUR RAHMAN
Head of Department:	Dr Consolee Mbarushimana

Course Information

Location of Delivery:	University of Wolverhampton
Category of Partnership:	Not delivered in partnership
Teaching Institution:	University of Wolverhampton
Open / Closed Course:	This course is open to all suitably qualified candidates.

Entry Requirements:

Entry requirements are subject to regular review. The entry requirements applicable to a particular academic year will be published on the University website (and externally as appropriate e.g. UCAS

- 96 UCAS points
- A Levels - grades CCC / BCD
- BTEC L3 Extended Diploma or OCR Cambridge L3 Technical Extended Diploma – grades MMM
- Access to HE Diploma (60 credits) of which a minimum of 45 must be at Level 3 (96 UCAS point equivalence, minimum 45 credits at merit)
- Successful completion of the Science and Engineering with International Foundation Year

Other Requirements:

Students must usually have studied for a minimum of two years post GCSE level. However, we will consider applications from mature students who do not have two years of post-16 study, where they have relevant work experience. Please see http://wlv.ac.uk/mature for further information.

If you've got other qualifications or relevant experience, please contact The Gateway for further advice before applying.

International entry requirements and application guidance can be found at

http://www.wlv.ac.uk/international/apply

English language requirements also apply.

Distinctive Features of the Course:

The BSc (Hons) Cybersecurity program is designed to provide students with a distinctive set of skills and knowledge crucial for a successful career in the field of cybersecurity. Throughout the course, students will develop a deep understanding of the principles, practices, and applications of security, emphasizing the protection of computer systems and networks from cyber threats.

The curriculum starts by introducing core principles in computer science, including programming, problem-solving, and computational mathematics. As students progress, the focus shifts to specialized areas within cybersecurity, such as secure software development, network security, cryptography, ethical hacking, and incident response. The program ensures a comprehensive exploration of topics essential for securing digital assets in today's interconnected world.

One key feature of the BSc Cybersecurity program is its emphasis on hands-on experience and practical skills. Students will have the opportunity to engage in real-world scenarios, simulated environments, and industry-relevant projects. This approach equips graduates with the practical know-how needed to address contemporary cybersecurity challenges.

Moreover, the course encourages critical thinking and ethical considerations, instilling a sense of responsibility in students to protect information and digital infrastructure. This aligns with the increasing demand for cybersecurity professionals who not only possess technical expertise but also uphold ethical standards and understand the legal implications of their actions.

As a distinct feature, the program offers flexibility through elective modules, allowing students to tailor their learning experience to specific areas of interest within cybersecurity. This ensures that graduates are well-rounded professionals with expertise in their chosen niche.

Upon completion of the BSc Cybersecurity program, graduates will be well-prepared for employment in cybersecurity-related roles, including but not limited to information security analyst, penetration tester, security consultant, and cybersecurity engineer. The course equips students with transferable skills in problem-solving, communication, project management, and critical analysis, enhancing their overall employability and adaptability in the rapidly evolving field of cybersecurity.

Educational Aims of the Course:

The BSc (Hons) Cybersecurity course aims to cultivate graduates who can adeptly navigate the dynamic landscape of the cybersecurity field, seamlessly transitioning from academic study to impactful contributions in the global cybersecurity industry. This goal is realized by providing students with a comprehensive understanding of the fundamental principles of cybersecurity and integrating this knowledge with a diverse range of cybersecurity tools, methodologies, and techniques employed by cybersecurity professionals worldwide.

Our Cybersecurity program offers a flexible and specialized learning experience, allowing students to delve into specific areas of interest within the cybersecurity domain. Whether focusing on secure software development, network security, cryptography, ethical hacking, or incident response, students will gain in-depth knowledge and practical skills relevant to their chosen cybersecurity specialties. The course is designed to not only meet current industry demands but also to prepare students for the ongoing evolution of cybersecurity technologies and practices.

By emphasizing practical, hands-on experience and exposing students to real-world scenarios and projects, the course ensures that graduates are not only well-versed in theoretical concepts but also possess the practical skills necessary to address contemporary cybersecurity challenges. The aim is to produce cybersecurity professionals who not only understand the technical aspects of their field but also uphold ethical standards, appreciate legal considerations, and can effectively contribute to the ever-expanding realm of cybersecurity.

Upon completion of the BSc Cybersecurity course, graduates will be equipped with the educational foundation, technical expertise, and critical thinking skills necessary for successful careers in cybersecurity. The course's overarching aim is to produce cybersecurity professionals capable of making meaningful and immediate contributions to the global cybersecurity landscape, ensuring the security and integrity of digital systems and information in an ever-evolving technological environment.

Intakes:

September

Major Source of Funding:

Office for Students (OFS)

Tuition Fees:

Tuition fees are reviewed on an annual basis. The fees applicable to a particular academic year will be published on the University website.

Year	Status	Mode	Amount
2020/1	H	Full Time / Sandwich	£9250.00
2020/1	Overseas	Full Time / Sandwich	£12250.00
2020/1	H	Part Time	£3050.00
2020/1	Overseas	Part Time	£6125.00
2021/2	H	Full Time / Sandwich	£9250.00
2021/2	Overseas	Full Time / Sandwich	£12950.00
2021/2	H	Part Time	£3100.00
2022/3	H	Full Time / Sandwich	£9250.00
2022/3	Overseas	Full Time / Sandwich	£13450.00
2022/3	H	Part Time	£3120.00
2023/4	H	Full Time / Sandwich	£9250.00
2023/4	Overseas	Full Time / Sandwich	£14450.00
2023/4	H	Part Time	£4625
2024/5	H	Full Time / Sandwich	£9250.00
2024/5	Overseas	Full Time / Sandwich	£14950.00
2024/5	H	Part Time	£4625.00

PSRB:

None

Course Structure:

September (Full-time)

Full time and Sandwich Undergraduate Honours students normally study 120 credits per academic year; 60 credits semester 1 and 60 credits semester 2.

Module	Title	Credits	Period	Type
4CS001	Introductory Programming And Problem Solving	20	SEM1	Core
4CS015	Fundamentals of Computing	20	SEM1	Core
4CS020	Interactive 3D Applications and Academic Skills	20	SEM2	Core
4CS017	Internet Software Architecture and Databases	20	SEM1	Core
4MM013	Computational Mathematics	20	SEM2	Core
4CS012	Server Management and Virtualisation	20	SEM2	Core

September (Full-time)

Full time and Sandwich Undergraduate Honours students normally study 120 credits per academic year; 60 credits semester 1 and 60 credits semester 2.

Module	Title	Credits	Period	Type
5CS032	Computer Networking	20	SEM1	Core
5CS018	Cybersecurity Architecture and Operations	20	SEM1	Core
5CS031	Network Security	20	SEM2	Core
5CS035	Ethical Hacking	20	SEM2	Core
5CS024	Collaborative Development	20	SEM2	Core

Group 01 | Min Value: 20 | Max Value: 20

5CS021	Numerical Methods and Concurrency	20	SEM1	
5CS045	Full stack Development	20	SEM1	

Continuing students will follow the programme indicated below:

September (Full-time)

Full time and Sandwich Undergraduate Honours students normally study 120 credits per academic year; 60 credits semester 1 and 60 credits semester 2.

Module	Title	Credits	Period	Type
5CS032	Computer Networking	20	SEM1	Core
5CS018	Cybersecurity Architecture and Operations	20	SEM1	Core
5CS031	Network Security	20	SEM2	Core
5CS035	Ethical Hacking	20	SEM2	Core
5CS024	Collaborative Development	20	SEM2	Core

Group 01 | Min Value: 20 | Max Value: 20

5CI021	Data Mining	20	SEM1	
5CS023	Web Development	20	SEM1	

Continuing students will follow the programme indicated below:

September (Full-time)

Full time and Sandwich Undergraduate Honours students normally study 120 credits per academic year; 60 credits semester 1 and 60 credits semester 2.

Module	Title	Credits	Period	Type
6CS007	Project and Professionalism	40	YEAR	Core
6CS032	Risk and Cybersecurity Management	20	SEM2	Core
6CS010	Digital Forensics	20	SEM1	Core

Group 01 | Min Value: 20 | Max Value: 20

6CS031	Cyber Threat Intelligence	20	SEM1	
6CS026	Systems Architecture and Internet of Things	20	SEM1	

Group 01 | Min Value: 20 | Max Value: 20

6CS029	Advanced Networks	20	SEM2	
6CS028	Advanced Web Development	20	SEM2	

September (Full-time)

Full time and Sandwich Undergraduate Honours students normally study 120 credits per academic year; 60 credits semester 1 and 60 credits semester 2.

Module	Title	Credits	Period	Type
6CS007	Project and Professionalism	40	YEAR	Core
6CS032	Risk and Cybersecurity Management	20	SEM2	Core
6CS010	Digital Forensics	20	SEM1	Core

Group 01 | Min Value: 20 | Max Value: 20

6CS056	Advanced Full Stack Development	20	SEM1	
6CS031	Cyber Threat Intelligence	20	SEM1	

Group 01 | Min Value: 20 | Max Value: 20

6CS030	Big Data	20	SEM2	
6CS029	Advanced Networks	20	SEM2	

Please note: Optional modules might not run every year, the course team will decide on an annual basis which options will be running, based on student demand and academic factors, to create the best learning experience.

Learning, Teaching and Assessment

Academic Regulations Exemption:

None.

Reference Points:

The course is designed with reference to the most up-to-date QAA Subject Benchmark for Computing and the accreditation requirements of BCS The Chartered Institute for IT. In addition reference has also been made to;

1. Quality Code - Part A: Setting and Maintaining Academic Standards. Including;
2. Qualifications Frameworks Characteristics Statements
3. Credit Frameworks
4. Subject Benchmark Statements - Computing
5. Quality Code - Part B: Assuring and Enhancing Academic Quality
6. University Policies and Regulations
7. Equality Act (2010).

Overview of Assessment:

As part of the course approval process, the course learning outcomes were mapped to each of the modules forming the diet of the programme of study. This process confirmed that all course learning outcomes can be met through successful completion of the modules. This mapping applies to the final award as well as to all of the intermediate awards.

Learning Outcomes	Modules
CERTHE01 Apply appropriate theory, tools and techniques (e.g. theory and practice of programming, object-oriented design and analysis, design and construction of data systems, concurrent and distributed systems) to the analysis, design and synthesis of solutions to requirements in the domain of Cybersecurity.	
CERTHE02 Demonstrate mastery of the essential facts, concepts, principles, theories and practices enabling graduate employment in applications of Cybersecurity (e.g. Software development, media computing, systems analysis).	
CERTHE03 Demonstrate a range of transferable skills in: problem solving; communication; project management; working individually and in teams; self-management; and the ability to gather, evaluate and reflect on information from relevant sources and synthesize new knowledge and solutions to requirements in the domain of applications of Cybersecurity.	
CERTHE04 Demonstrate a range of social, legal, ethical and professional skills required for continuing professional development in Computing and Information Technology disciplines within a world-wide context.	
DIPHE01 Apply appropriate theory, tools and techniques (e.g. theory and practice of programming, object-oriented design and analysis, design and construction of data systems,	

Learning Outcomes	Modules
concurrent and distributed systems) to the analysis, design and synthesis of solutions to requirements in the domain of Cybersecurity.	
DIPHE02 Demonstrate mastery of the essential facts, concepts, principles, theories and practices enabling graduate employment in applications of Cybersecurity (e.g. Software development, media computing, systems analysis).	
DIPHE03 Demonstrate a range of transferable skills in: problem solving; communication; project management; working individually and in teams; self-management; and the ability to gather, evaluate and reflect on information from relevant sources and synthesize new knowledge and solutions to requirements in the domain of applications of Cybersecurity.	
DIPHE04 Demonstrate a range of social, legal, ethical and professional skills required for continuing professional development in Computing and Information Technology disciplines within a world-wide context.	
BHONSN01 Apply appropriate theory, tools and techniques (e.g. theory and practice of programming, object-oriented design and analysis, design and construction of data systems, concurrent and distributed systems) to the analysis, design and synthesis of solutions to requirements in the domain of Cybersecurity.	
BHONSN02 Demonstrate mastery of the essential facts, concepts, principles, theories and practices enabling graduate employment in applications of Cybersecurity (e.g. Software development, media computing, systems analysis).	
BHONSN03 Demonstrate a range of transferable skills in: problem solving; communication; project management; working individually and in teams; self-management; and the ability to gather, evaluate and reflect on information from relevant sources and synthesize new knowledge and solutions to requirements in the domain of applications of Cybersecurity	
BHONSN04 Demonstrate a range of social, legal, ethical and professional skills required for continuing professional development in Computing and Information Technology disciplines within a world-wide context.	
BHONS01 Apply appropriate theory, tools and techniques (e.g. theory and practice of programming, object-oriented design and analysis, design and construction of data systems, concurrent and distributed systems) to the analysis, design and synthesis of solutions to requirements in the domain of Cybersecurity.	
BHONS02 Demonstrate mastery of the essential facts, concepts, principles, theories and practices enabling graduate employment in applications of Cybersecurity (e.g. Software development, media computing, systems analysis).	
BHONS03 Demonstrate a range of transferable skills in: problem solving; communication; project management; working individually and in teams; self-management; and the ability to gather, evaluate and reflect on information from relevant sources and synthesize new knowledge and solutions to requirements in the domain of applications of Cybersecurity.	
BHONS04 Demonstrate a range of social, legal, ethical and professional skills required for continuing professional development in Computing and Information Technology	

Teaching, Learning and Assessment:

The learning activities on your course will develop distinctive graduate attributes that will make you stand out and enhance your employability. These skills will be embedded into the curriculum throughout your course. Examples include:

Digitally Literacy: All Cybersecurity graduates will surely be users of advanced technologies. However, on your course you will develop your skills to encompass literacy more fully such as learning how to find information and how to take best advantage of digital resources and the Internet to make you effective in the Information Age.

Global Citizenship: On each level of your course you will learn about the social aspects of Mathematics, which will broaden your understanding of the way the world works and how communication and collaboration are evolving.

Knowledgeable and Enterprising: Throughout your course you will build up your professional and employability skills and learn to apply the knowledge you have acquired in an enterprising way. You will constantly nurture your own intellectual curiosity. The tools, methodologies and techniques that you will learn have been carefully selected to prepare you with the skills that employers demand and the opportunities for work based learning and placements will allow you to gain the vital experience that they often expect. Formative assessments provide feedback and are not used in the grading process. Their purpose is to provide both tutors and students with a gauge of progress. Summative assessments are used in the grading process. Most summative assessments (with a notable exception of exams) also have a formative aspect to them in that tutors provide written feedback on the work. Students should use this feedback to improve their performance on future assessments. Feedback on an assessment on one module may help with assessments on other modules.

Assessment methods are closely linked to the learning and teaching approaches used. Below are examples of the assessment methods that you may encounter.

Assignments – task based and report based assignments. Coursework frequently requires the writing of reports documenting the development of solutions. It is frequent practice to ask students to reflect on their learning experience as part of the coursework.

Case studies – based on realistic scenarios. Analysis, application and evaluation skills are developed via case studies as appropriate for the topic areas.

Practical exercises – tutorials and workshop sessions. These aid understanding and application of knowledge using a variety of IT tools within practical settings in workshops as well as assessing depth and breadth of understanding and application of subject knowledge. Practical exercises are the primary mechanisms for assessing analysis and evaluation. The tasks undertaken involve well-defined problems with varied level of complexity. Some practical exercise may involve interactive learning tools that are able to provide formative feedback.

Portfolios / e-portfolios – contain samples of work demonstrating what the student has accomplished. This is a good way to assess learning and development which is illustrated by multiple examples of work, opportunities for self-assessment and reflection chartering over a period of time. Tasks set relate to outcomes being assessed thus documenting evidence of development towards mastering the identified outcomes and skills. Enhances the assessment process by demonstrating a range of skills and understandings of the subject area by the student. Some portfolios are sometimes called Learning Journals.

Formal presentations - you may be required to present your work to a group of tutors or to the rest of the class. This may be a demonstration of practical work or something you developed or built or may present the results of a study. These are an important way of assessing your communication skills.

Examinations and Time-Constrained Assessments (tests) - may follow a traditional format or on-line alternatives. They are used to ensure breadth of knowledge has been acquired. TCA and examinations, some of which are case study based, emphasise application of knowledge and skills.

Group Project Work - where group work is assessed, mechanisms are used to allow individual contributions to be reflected in the grading as appropriate e.g. peer assessment of individual group members, individual reflection on the process and the product.

Peer-group assessment – using student feedback, particularly in group assessments to identify each student's contribution to the work.

Individual Project Work - All courses require at least one module of individual project work where students work individually on a large task. This type of work is supported by either regular meetings with a named project supervisor or through seminars.

Work-based assessments – used to assess the student's work-based modules and enable feedback from work placement organisations. These are usually used for students who are industry-based and doing their course part-time or students doing a placement.

Assessments will also focus on skills such as team working, time-management and developing Continuing Professional Development (CPD) awareness, as well as discipline-specific skills related to the analysis, design, development, implementation, testing and evaluation of systems.

Typical tasks include: production of technical documentation, reports for differing target audiences, presentations, demonstrations and viva, allowing assessment of the breadth and depth of knowledge, analysis and synthesis, communication, and evaluation within the subject area.

Assessment Methods:

At the University of Wolverhampton, a variety of modes of assessment will be used to support and test your learning and progress and to help you develop capabilities that are valued beyond your University studies and into your working life. Your course may include a variety of assessment activities:

Written examinations (including online examinations, open and closed book examinations and quizzes)
Coursework (for example, essays, reports, portfolios, project proposals and briefs, CVs, poster presentation)
Practical (for example, oral and video presentations, laboratory work, performances, practical skills assessment)

In the final year of your undergraduate degree, and at the end of your postgraduate degree, you are likely to be expected to write an extended piece of work or research, such as a dissertation or a practice-based piece of research.

Student Support:

Course support:

At the start of each year of your course you will be assigned a Personal Tutor who will guide you through the induction process and provide support and academic counselling throughout the year on an appointment basis. They should be able to offer you advice and guidance to help you liaise with other staff and support facilities in the Faculty and University. You should meet your Personal Tutor at least 3 times a year, which must include meetings that you are invited to at critical points in your course.

The Personal Tutor provides academic counselling and will be accessible throughout the week on a drop-in or appointment basis to discuss timetables, requests for extensions, requests for extenuating circumstances, general concerns about study and student life and general programme planning. The Personal Tutor will act as a first point of contact in relation to leave of absence (including returning after leave), withdrawal, transferring to another course (internal and external) and changes to mode of attendance. Your Programme Leader will be available thereafter for meetings by appointment to discuss leave of absence, withdrawal, transferring to another course (internal and external), changes to mode of attendance, returning after leave of absence and direct entrants.

Subject support:

Tutorials, workshops, seminars, and meetings - provide the primary opportunities for students to interact with staff on topics relating to modules. All modules provide at least one of these forms of face-to-face support.

Formative feedback - tutors provide personalised written feedback on most summative assessments. The mechanism for feedback from purely formative tasks varies between assessments but will always be provided in some form. On-line formative tasks often provide feedback straight away. On occasions tutors may provide generalised verbal feedback to the whole class on points relating to an assessment. Assessment and subject-based surgeries provide additional student support for subjects that students often need extra help with. They are often concentrated around the times when assessments take place. Revision sessions are provided for many modules that have tests and enable you to interact with tutors to review parts of the course. Mock exams and tests may provide opportunities to experience an examination environment before the final summative test and give you feedback on your understanding.

Employability in the Curriculum:

Throughout your course you will build up your professional and employability skills and learn to apply the knowledge you have acquired in an enterprising way. You will constantly nurture your own intellectual curiosity. The tools, methodologies, and techniques that you will learn have been carefully selected to prepare you with the skills that employers demand and the opportunities for work-based learning and placements will allow you to gain the vital experience that they often expect.