Ravensbourne University London

COURSE SPECIFICATION

Course Title	BSc (Hons) Cyber Security
Final Award	BSc (Hons) Cyber Security
Interim Awards	Certificate of Higher Education in Cyber Security Diploma of Higher Education in Cyber Security BSc Cyber Security
Awarding Body	Ravensbourne University London
Teaching Institution	Ravensbourne University London
UCAS Code	I110
HECOS code (with Subject percentage Splits if applicable)	
QAA Subject Benchmark	Computing (2022)
External Accrediting Bodies	N/A
Apprenticeship Standard used to inform the development of the course (if applicable)	
Accelerated Degree Option	☒ No
Level 6 Top Up Option (online only)	☒ No
Study Load	☒ Full-time ☒ Part-time
Mode of study	☒ Face-to-face
Delivery Location(s)	☒ Ravensbourne University campus
Length(s) of Course(s)	3 years full time 6 years part time
Type (open/closed)	Open
Validation period	Five years (September 2022 – September 2027)
Intended First Cohort Start Date	September 2022
Date produced/amended	3/3/22
Course Leader	Samuel Onalo
Course Development Team Members	
Course Administrative Contact	Kevin Cahill

Course Description

This degree is designed with the view to provide access to knowledge about latest developments in the industry. This programme has been developed in line with the Cyber Security Body of Knowledge (CyBOK 1.1) framework at this level.

The course covers a range of requisite skills, knowledge and industry standard technologies related to cyber security and its implementation in various sectors. Cyber Security is regarded as a highly valuable and specialist profession.

The framework used for development of this programme aligns well with the Key Knowledge Areas of CyBOK 1.1 which is a comprehensive Body of Knowledge to inform and underpin educational and professional training for the cyber security sector. CyBOK is funded by the National Cyber Security Centre. A mapping with CyBOK version 1.1 is given at the end of this document.

A typical role of a cyber security expert includes implementation and maintenance of security controls on digital assets of an organisation. The role also involves ensuring that security technologies and practices are operating in accordance with the organisation's policies and standards. In order to become a successful cyber security expert, you will need a broad understanding of computer networks, software engineering processes, web technologies and databases to mitigate against the potential threats.

Alongside covering the technical content and practices underpinning relevant knowledge areas, the programme is designed to develop soft skills such as communication, team work, creativity, project management and leadership. This is achieved by students working in groups and regular participation in in-class activities.

This programme equips the students with a strong understanding of what cyber security entails. Based on numerous case studies, labs, workshops and online resources, students will utilise current tools and methodologies to learn about Cyber Security. Upon completion, students will be able to evaluate Cyber Security issues, recognise best practices, and analyse and evaluate possible solutions to overcome any potential threats.

This programme covers six key areas of cyber security which include Networking, Databases, Software Development and Management, Cyber Security, Artificial Intelligence and Machine Learning and Ethics and Regulations.

As almost all or the majority of organisations are directly or indirectly users of computing and cloud technologies, it is imperative for Ravensbourne to develop programmes which are meeting the needs and demands of the industry

Potential Careers in Cyber Security:

1. Cyber Security Consultant
2. Security Architect
3. Cyber Security Analyst
4. Information and Cyber Security Manager
5. Software Developer
6. Network Administrator
7. Cyber Incident Manager
8. Cyber Project Manager
9. Security Management

10. Penetration Tester
11. Ethical Hacker

Course Aims
• To prepare market ready Cyber Security graduates with 3 year's vocational experience on the latest technologies.
• Be able to research, analyse, model, assess and manage cyber security risks
• Design, develop, justify, manage and operate secure solutions; and detect and respond to incidents.
• Work in accordance with applicable laws, regulations, standards and ethics
• Develop a specialist understanding of computer hardware, network architecture, operating systems and virtual environments.
• Develop an in-depth understanding of vulnerabilities related to local and cloud-based networks
• Web design and databases: To develop comprehensive understanding and application of web-based database systems, Big Data, Data Lakes, Data Management and how to secure them
• Software Development: To gain requisite skills in software architecture, software development lifecycle and approaches to developing secure software
• Artificial Intelligence and Machine Learning: Develop a strong understanding of various models and how AI/ML work hand in hand to develop intelligent tools for security, decision making and automation.

Course Learning Outcomes

The course provides opportunities for students to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas. On completion of the **BSc (Hons) Cyber Security** students will be able to:	
Explore	Evidence and contextualise capacity for utilising and synthesising Cyber Security specific knowledge, elegant theories, critical & computational thinking, algorithmic thinking, evaluation and reflection, supporting deeper understanding of subject knowledge and innovative complex problem solving. (CLO1)
Create	Critically engage with the cognitive development of ideas, materials, tests and outcomes that may inform practical and theoretical development in physical, written and oral forms aligned to Computing Disciplines Evidence ability to synthesise idea development, experimentation, and technical ability supporting fully resolved outcomes and systems regarding communication and presentation for Cyber Security (CLO2)
Influence	Evidence a methodical working approach and ethos that critically identifies consideration of social, ethical and environmentally responsible working methods and how this aligns and supports personal development and professional working practices in relation to Cyber Security (CLO3)
Integrate	Evidence a critical ability to successfully synthesise collaboration, industry interactions & practices and professional working models in order to facilitate self-efficacy, personal agency and professional development in relation to Cyber Security (CLO4)

Where a student does not complete the full course, but exits with an Ordinary Degree, they will have had the opportunity to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas. On completion of the **BSc Cyber Security** students will be able to:	
Explore	Evidence and contextualise capacity for utilising and synthesising Cyber Security specific knowledge, critical thinking and reflection, supporting deeper understanding of subject knowledge and problem solving. (CLO1)
Create	Evidence ability to consider ideas, materials, tests and outcomes that may inform practical and theoretical development in physical, written and oral forms aligned to cyber security. Evidence ability to synthesise idea development, experimentation, and technical ability supporting resolved outcomes regarding communication and presentation for cyber security. (CLO2)
Influence	Evidence a coherent working approach and ethos that identifies consideration of social ethically and environmentally responsible working methods and how this aligns and supports personal development in relation to cyber security. (CLO3)
Integrate	Evidence ability to effectively synthesise collaboration, industry interactions & practices and professional working models in order to facilitate self-efficacy, personal agency and professional development in relation to cyber security. (CLO4)

Where a student does not complete the full course, but exits with a Diploma in Higher Education, they will have had the opportunity to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas. On completion of the **Diploma of Higher Education in Cyber Security** students will be able to:	
Explore	Evidence evolving ability to utilise research and critical reflection to support developing understanding of subject knowledge and ability to problem solve in relation to cyber security (CLO1)
Create	Evidence capacity to combine ideas, materials, tests and outcomes into solutions that inform and guide practical and theoretical development in physical, written and oral forms aligned to cyber security. Exhibit developed technical competencies, supporting ideation, communication and presentation in relation to cyber security. (CLO2)
Influence	Evidence developing working processes that identify consideration and interpretation of social, ethically and environmentally responsible working methods and how this guides personal professional practice in relation to cyber security (CLO3)
Integrate	Evidence evolving ability to engage with collaborative working to support academic development, industry interactions & practices to enhance and progress self-efficacy and professional development in relation to cyber security (CLO4)

Where a student does not complete the full course, but exits with a Certificate of Higher Education, they will have had the opportunity to develop and demonstrate knowledge and understanding, qualities, skills and other attributes in the following areas. On completion of the **Certificate of Higher Education in Cyber Security** students will be able to:	
Explore	Demonstrate capacity for engaging with research and critical thinking, developing cyber security specific knowledge and emerging ability to problem solve. (CLO1)
Create	Demonstrate capacity to consider ideas, materials, tests and outcomes that may inform practical and theoretical development in physical, written and oral forms in relation to cyber security Exhibit emerging technical competencies, supporting ideation, communication and presentation in relation to cyber security (CLO2)
Influence	Demonstrate emerging working approach/attitude that identifies consideration of social, ethical and environmentally responsible working methods and how this informs personal practice in relation to cyber security (CLO3)
Integrate	Demonstrate emerging capacity to engage with collaboration, teamwork, industry interactions, and professional working practices to support self-efficacy and professional development in relation to cyber security (CLO4)

Ravensbourne University Assessment Criteria	
Explore	Research and Analysis Subject Knowledge Critical Thinking and Reflection Problem Solving
Create	Ideation Experimentation Technical Competence Communication and Presentation
Influence	Social Impact Ethical Impact Environmental Impact
Integrate	Collaboration Entrepreneurship and Enterprise Professional Development

Core Competencies
Each module learning outcome should be aligned to at least one competency.

Competency	Definition	Aligned Assessment Criteria
Cognitive	The ability to acquire, retain and use knowledge, recognise, pose and solve problems. Attributes may include: • Evaluate their own beliefs, biases and assumptions • Evaluate strengths, weaknesses, and fallacies of logic in arguments and information • Apply lesson from the past or learned knowledge and skills to new and varied situations • Perform basic computations or approach practical problems by choosing appropriately from a variety of mathematical techniques • Devise and defend a logical hypothesis to explain observed phenomenon • Recognise a problem and devise and implement a plan of action	**Explore, Create, Integrate, Influence**
Creative	The ability to generate new ideas, express themselves creatively, innovate and/ or solve complex problems in an original way.	**Create**
Professional	The ability to understand and effectively meet the expectations of industry partners, through outputs and behaviours.	**Integrate, Influence**
Emotional, Social and Physical	Emotional -The intrapersonal ability to identify, assess, and regulate one's own emotions and moods; to discriminate among them and to use this information to guide one's thinking and actions and where one has to make consequential decisions for oneself. Attributes may include:	**Explore, Influence, Integrate**

	• Self-awareness & regulation (including metacognition) • Mindfulness • Cognitive flexibility • Emotional resilience • Motivation • Ethical decision- making	
	Social - The interpersonal ability to identify & understand the underlying emotions of individuals and groups, enhancing communication efficacy, empathy and influence. Attributes may include:	
	• Managing your audience • Coordinating with others • Negotiation • Creativity • People management • Leadership & entrepreneurship • Service orientation • Active listening • Coaching and mentoring	
	Physical - The ability to perceive and optimise physiological activity and responses to influence emotion, solve problems or otherwise effect behaviour. Physical intelligence engages the body to train neuron pathways to help change an inappropriate response to an appropriate response. Attributes may include	
	• Self-discipline & management • Attention • Reaction & response time • Cognitive & muscle memory • Managing stress • Physical resilience	
Cultural	The capability to relate to and work effectively across cultures including intercultural engagement, cultural understanding and intercultural communication.	**Influence, Integrate**

Enterprise and Entrepreneurial	The generation and application of ideas within a practical setting. It combines creativity, idea generation and design thinking, with problem identification, problem solving, and innovation followed by practical action. This can, but does not exclusively, lead to venture creation (UK Quality Assurance Agency, Enterprise and Entrepreneurship Education 2018).	**Create, Influence, Integrate**
Digital	The confident adoption of applications, new devices, software and services and the ability to stay up to date with ICT as it evolves. The ability to deal with failures and problems of ICT and to design and implement solutions (Jisc Digital Capabilities Framework)	**Explore, Create, Integrate, Influence**
Ravensbourne Return	Engagement with inhouse activities including mentoring other students, volunteering, acting as a student rep or ambassador. Demonstrate a knowledge of current events and social issues Identify their personal convictions and explore options for putting these convictions into practice Engagement with the external community through (from) employment, volunteering, participation in a Professional Life or other programme-based project.	**Explore, Create, Influence, Integrate,**

Learning, Teaching and Assessment

Learning and Teaching methods	Assessment Strategy
Level 4: At Level 4 Learning & teaching will be delivered through a combination of workshops, laboratory sessions, lectures, seminars and group exercises, self-directed study, as well as individual or group tutorials. • Lecture • Seminar • Tutorial • Guest Lecture • Technical Demonstration • Practical Classes and Workshops • External Visits • Independent Study • Directed Study • Hybrid Approach Level 4 will also introduce students to the Professional Life Practice modules that are embedded in each undergraduate learning level. These modules specifically support collaborative experimental practice, entrepreneurship, and enterprise, helping to catalyse, develop and showcase interdisciplinary working methods interaction and innovation. The Modules will also facilitate opportunities to integrate with industry partners in order to establish professional currency at the start of the undergraduate journey, and to drive enterprise and employability through the degree experience. The Professional Life Practice Modules integrate the emerging subject knowledge of each student with working methods from a range of disciplines to create a multidisciplinary synthesis of practice, skills and learning. Students will develop social, cultural, emotional, and cognitive intelligence	For all levels of the Course: Oral Assessment – content and form Presentation Portfolio Practical Assignment Artefact and demonstrations Presentations Reflective Written Document Industry Focussed Report Personal Progress Review (PPR) **Formative Assessment** is used in all modules of the programme to assess students progress relating to module briefs and an opportunity to offer feedback, feedforward and a diagnostic response. This is typically within a group or individual review held midway throughout each module though for latter modules in level six there are more formative assessment points. **Summative Assessment** is held in the latter stages of each module and is the definitive assessment point where each assessment requirement is assessed. All Assessment involves moderation and verification. Written or oral feedback and clear feedforward will be provided shortly after assessment and there are opportunities for tutorials if you need further classification before the start of the next module.

through projects that facilitate community and industry connections aligned to the Ravensbourne Core Competencies. **Level 5:** Skills acquired at Level 5 are developed further through a combination of workshops, lectures, seminars, group exercises, self-directed study, as well as individual or group tutorials. Students will test their developing disciplinary knowledge in collaborative scenarios with the opportunity to take part in the Professional Life Practice Modules, and Work Based Learning Modules, offering collaborative and industry aligned opportunities both within Ravensbourne and in external contexts. Visiting speakers and industry specialists will be invited to deliver lectures or practical workshops, bringing their own specialism and examples of industry work into the sessions. The Professional Life Practice Modules at Level 5 supports practical, theoretical and industry focused engagement facilitating expertise, experience and interactions with professional aspects of the games and games programming disciplines. All Level 5 students will have the opportunity to undertake a Work Based Learning modules at the end of Semester 2. The Work Based Learning module will offer students the ability to engage with industry-led experience supporting industry interactions, entrepreneurship and employability skills. The placements will be supported by the careers team at Ravensbourne. **Level 6**	Assessment will be aligned to the Ravensbourne Core Competencies.

Skills acquired at Level 4 and 5 will be developed and perfected at Level 6 through lectures, seminars, workshops, self-directed study and individual tutorials. Students are expected to take on professional attitudes to time and project management. Visiting lecturers may be invited to deliver lectures and/or practical sessions related to their area of work and students will develop an outward facing portfolio to aid graduate progression. Written work will focus upon critical analysis and reflection of project-based work, with a view to encouraging ongoing development. Within the sphere of theoretical study, students will expand their ability to write reflexively and critically about their discipline and competently be able to contextualise their personal practice. Students will be expected to interface directly with industry through mentoring, competition, and research.	

Work-Based Learning

Student are encouraged from Level 4 to engage with industry and seek internship opportunities within the industry at Level 5. The careers team within Student Services can facilitate outreach for students to contact companies. Students are provided with membership of industry bodies that can assist with placements.

Students are likely to apply for specific internship or work experience placements with development or publishing companies. They might also apply for zero hours casual work as quality assurance engineers.

Students are encouraged to find industry mentors to assist professional development.

A number of opportunities are advertised through the virtual learning environment.

Course Structure

Module Code	Module Title	Shared Module	Mandatory / Elective	Credits
Level 4				
CYS22101	Software Design and Development	x	Mandatory	20
CYS22102	Computer Networks & Technology	x	Mandatory	20
PLP22103	Professional Life Practice "Developing your Practice"	x	Mandatory	20
CYS22104	Web Design and Databases	x	Mandatory	20
CYS22105	Cyber Security Principles	x	Mandatory	20
PLP22106	Professional Life Practice "Exploring your Practice"	x	Mandatory	20
			Total	**120**
Level 5				
CYS22201	Operating Systems and Cloud	x	Mandatory	20
CYS22202	Computer Vision & AI	x	Mandatory	20
CYS22204	Ethical Hacking	x	Mandatory	40
PLP22203	Professional Life Practice "Applying your Practice"	x	Mandatory	20
PLP22206	Work-Based Learning		Mandatory	20
				120
			Total	**240**
Level 6				
CYS22301	Advanced Secure Programming	x	Mandatory	40
PLP22303	Professional Life Practice "Situating your Practice"	x	Mandatory	20
CYS22302	Final Project	x	Mandatory	40
CYS22304	Ethics, Risk and Project Management	x	Mandatory	20
				120
			Total	**360**

Learning Hours

Learning Hours (per 20 credit module excluding the Work-Based Learning)			
Staff – Student Contact Hours		**Independent Study Hours**	
Taught hours	48	Independent study, self-directed study and assessment	152
Total			200

Course Regulations

Entry Requirements
Please refer to the institutional regulations on the expected minimum entry requirements (found under Section 5 of the General Academic Regulations found on the website here), and the course page on the Ravensbourne University website for course specific entry requirements. In addition, students will be required to have obtained GCSE Mathematics Grade 4/C or above.
Accreditation of Prior Learning (if applicable)
Applications are welcomed from those who may not possess formal entry qualifications, mature students, those with work experience or with qualifications other than those listed above. Such applicants should demonstrate sufficient aptitude and potential to complete the course successfully. Applicants will be assessed at interview in accordance with Ravensbourne's Accreditation of Prior Learning Policy and Procedure and Student Transfer Plan.
Conditions for Progression
Students will be deemed to have passed a module if they achieve a 40% for undergraduate students; or a 50% for postgraduate students. A student who has passed all assessments to date but has not yet reached the end of a level (or stage) will be permitted to proceed into the following term by the Interim Assessment Board.
Reassessment of Failed Elements
Failure in any component will result in a Fail grade for the component. Non-submission in any component will result in a non-submission for the component. Students must then successfully retrieve the failed or non-submitted component by resubmission of assessment in order to pass the module. Where a student does successfully retrieve a component failure, the grade for the component will be capped at 40% (undergraduate) or 50% (postgraduate) (except where Extenuating Circumstances have been approved). The overall grade for the module will be calculated using all achieved grades where there are 2 or more components.
Conditions for the Granting of Awards

A student who completes an approved course of study, shall be awarded BSc (Hons) Cyber Security.

Those students who exit the Course without completing it may be entitled to exit with an award of either a:

1. Certificate of Higher Education in Cyber Security, provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.
2. Diploma of Higher Education in Cyber Security, provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.
3. BSc Cyber Security (ordinary degree), provided they complete an approved course of modules and the learning outcomes for such award as set out in the Course Specification.

Any derogation(s) from the Regulations required?	
N/A	
Student Support	https://www.ravensbourne.ac.uk/student-services
Assessment Regulations	https://www.ravensbourne.ac.uk/staff-and-student-policies

Course Learning Outcomes	**CLO1**	**CLO2**	**CLO3**	**CLO4**
Level 4 Modules				
CYS22101 Software Design and Development	X		X	X
CYS22102 Computer Networks and Technology		X	X	X
PLP22103 Professional Life Practice Developing your Practice	X	X	X	X
CYS22104 Web Design and Databases	X		X	
CYS22105 Cyber Security Principles		X		X
PLP22106 Professional Life Practice Exploring your Practice	X	X	X	X
Level 5 Modules				
CYS22201 Operating Systems and Cloud	X			X
CYS22202 Computer Vision and AI	X		X	
CYS22204 Ethical Hacking		X	X	
PLP22203 Professional Life Practice Applying your Practice	X		X	
PLP22206 Work-Based Learning				X
Level 6 Modules				
CYS22301 Advanced Secure Programming	X		X	
CYS22304 Ethics, Risk and Project Management	X	X		X
PLP22303 Professional Life Practice Situating your Practice	X	X	X	
CYS22302 Final Project		X		X

Course Diagram

<table>
<tr><td></td><td>Semester 1</td><td colspan="2">Semester 2</td></tr>
<tr><td rowspan="3">Level 4

120 credits</td><td>CYS22101 Software Design and Development
20 credits</td><td colspan="2">CYS22104 Web Design and Databases
20 credits</td></tr>
<tr><td>CYS22102 Computer Networks and Technology
20 credits</td><td colspan="2">CYS22105 Cyber Security Principles
20 credits</td></tr>
<tr><td>PLP22103 Professional Life Practice Developing your Practice
20 credits</td><td colspan="2">PLP22106 Professional Life Practice Exploring your Practice
20 credits</td></tr>
<tr><td colspan="2">Semester 1</td><td colspan="2">Semester 2</td></tr>
<tr><td rowspan="3">Level 5

120 credits</td><td>CYS22201 Operating Systems and Cloud
20 credits</td><td rowspan="3">CYS22204 Ethical Hacking
40 credits</td><td rowspan="3">PLP22206 Work-Based Learning
20 credits</td></tr>
<tr><td>CYS22202 Computer Vision and AI
20 credits</td></tr>
<tr><td>PLP22203 Professional Life Practice Applying your Practice
20 credits</td></tr>
<tr><td colspan="2">Semester 1</td><td colspan="2">Semester 2</td></tr>
<tr><td rowspan="2">Level 6

120 credits</td><td>CYS22301 Advanced Security Programming
40 credits</td><td rowspan="2">CYS22302 Final Project
40 credits</td><td rowspan="2">CYS22304 Ethics, Risk and Project Management
20 credits</td></tr>
<tr><td>PLP22303 Professional Life Practice Situating your Practice
20 credits</td></tr>
</table>