Unit Title	Cyber Security Principles (blended)
FHEQ Level	Level 5
Unit Code	CLC20205
Credit Value	30
Unit Type	Subject

Learning Hours (Blended)			
Staff – Student Contact Hours		**Independent Study Hours**	
Classes	45	Independent study	200
Supervised access to Ravensbourne resources	30	Preparation for assessment	25
Total		300	

Unit Description

The unit aims to provide students with a foundation in the specification, design, implementation and evaluation of secure systems. This includes coverage of formal, pattern-based and domain-specifics approaches to development, as well as the human factors relevant to secure systems.

With more connectivity, cyber-attacks are increasing around the globe. Just like our homes and organisations, it is equally important to keep our digital assets safe from attackers.

This Cyber Security unit will develop awareness about potential threats, possible solutions and mitigating strategies.

Most digital devices are connected with the internet, from a smart watch and a light bulb to autonomous vehicles and satellites. Day to day activities such as booking holidays to banking and from healthcare information to sensitive military data is all dependant on connectivity and internet.

Cyber Security needs to be considered at every stage of digital deployment. From analysing user requirements, development of software and deployment of databases up to the connectivity with the internet and cloud, every element of the communication and storage should be secured from hackers.

The Five Principles underpin the Mindsets and Skillsets Manifesto and are the foundation upon which all course curriculum frameworks and unit specifications are based. The relevant Principles as stated below have been mapped against the Learning Outcomes relevant to each course unit and at each level (see Programme Specifications for full description of the Five Principles):

1. Cultivate / Where the individual thrives.
2. Collaborate / Where disciplines evolve.
3. Integrate / Where education engages industry.
4. Advocate / Where purpose meets practice.
5. Originate / creativity meets technology.

Unit Indicative Content

Cyber Security

Industry-wide Knowledge

- Risk assessment and regulations
- ISO Standards for IT Security
- Network Security Protocols
- Malware & Attack Technologies
- Public and Private Key cryptography
- Hardware and Software Security
- Directory services and group policies
- Network Security Testing
- NAT, DMZ
- Access/Permissions Control
- Authentication
- Disaster Recovery
- Encryption
- Identity Management
- Risk/Compliance
- QoS and QoE (Quality of Service and Quality of Experience)

AWS Specific Knowledge Area

- Cognito
- Identity Management and Access
- Inspector

CyBOK knowledge areas

- Malware & Attack Technologies
- Authentication, Authorisation & Accountability (AAA)
- Security Operations & Incident Management

Unit Aims
To understand current Cyber Security environment and risk mitigation.
To apply appropriate cyber security techniques for a selected industry.
To identify Secure software development approaches and their advantages
To apply network security concepts and protocols to IoT, mobile or contemporary technologies.
To evaluate current Malware and attack technologies and suggest preventive measures.
Critically evaluate the role of a security policies, compliance and regulations for protecting information assets. Critically evaluate the role of security policies, compliance, and regulations for protecting information assets.

Unit Learning Outcomes
LO 1 Research/Inspiration Analyse and interpret information gathering techniques using a wide range of sources, providing visual, contextual and industry case-study research as appropriate. Related Principle: ORIGINATE
LO 5 Presentation /Storytelling for Influence Select and employ effective methods of presentation and communication of projects in considering the audience/client and the purpose of the work, whether in visual, oral or written form. Related Principle: ADVOCATE
LO 6 Critical and creative mindsets Analyse conceptions of diverse practice and use this to inform a course of action Related Principle: ORIGINATE
LO 8 Professional Identity Investigate specific professional contexts to situate your own practice Related Principle: CULTIVATE

Learning and Teaching Methods
This unit will be delivered using a combination of: ● Lectures / Seminars ● Online activities ● Self-directed independent study ● Peer learning, group discussion, guest speakers

Assessment methods and tasks	
Assessment tasks	**Weighting (%)** *(one grade or multi-grade unit)*
Project portfolio	40%
Online Test	30%
Individual Presentation	30%

Indicative Assessment Criteria

Students will choose an industry of their choice (consumer, creative arts, media, healthcare, banking, retail etc.) to answer the following:

Analyse Cyber Security environment of your selection and determine appropriate approaches for continuity of operations and risk mitigation (LO1, LO6)

Propose appropriate cyber-security solutions (LO5, LO8)

Analyse secure software development approaches and their advantages (LO1)

Apply network security concepts and protocols to IoT, mobile or contemporary technologies. (LO5)

Evaluate current Malware and attack technologies and suggest preventive measures for selected industry. (LO6)

Critically evaluate the role of security policies, compliance and regulations for protecting information assets. (LO6, LO8)

Essential Reading list

The Cyber Security Body of Knowledge. (2019). 1st ed. The National Cyber Security Centre.

Prowse, D. (2017). CompTIA Security+ SYO-501 Cert Guide, Academic Edition (Pearson It Cybersecurity Curriculum (Itcc)). Pearson IT Certification.

Easttom, C. (2016). Computer Security Fundamentals, Third Edition. 3rd ed. Pearson.

Recommended Reading List

Gupta, Aditya. The IoT Hacker's Handbook: a Practical Guide to Hacking the Internet of Things. Apress., 2019.

Beasley, J. and Nilkaew, P. (2018). Networking essentials. Pearson. (ISBN 9780789758743)

Meyers, M. and Weissman, J. (2018). Mike Meyers CompTIA Network+ Guide to Managing and Troubleshooting Networks Lab Manual, Fifth Edition (Exam N10-007). ßMcGraw-Hill Education;.

Gupta, B., Perez, G., Agrawal, D. and Gupta, D. (2020). *Handbook of Computer Networks and Cyber Security*. Cham: Springer.

Stallings, W. (2017). *Network security essentials*. Boston [etc.]: Pearson.

Further reading and resources will be identified in your Project Brief.