INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «__» _____

Programme	**LEVEL 4 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 1 INTRODUCTION TO CYBER SECURITY**		
Cohort Code:	L04ICS-U1		
Unit Level	Level 4		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	20 CATS/ 10 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This module is designed to provide students with a comprehensive introduction to the field of cyber security, equipping them with the foundational knowledge and skills necessary to understand and address various cyber threats and vulnerabilities.
Differentiation Strategies *(e.g. planned activities or support for individual learners according to their needs)*	The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students' needs will be adopted throughout the lesson. Such will include: 1. Progressive tasks 2. Digital resources

	3. Verbal support 4. Variable outcomes 5. Collaborative learning 6. Ongoing assessment 7. Flexible-pace learning
Equality & Diversity	Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met.
Safeguarding & Prevent	Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff.
Health & Safety	SIRM H&S policies will be maintained.
Learning Resources	**Teaching and Learning Materials** • Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning. • Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional. • Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Learning Outcome	Assessment Criteria
LO1. Understand fundamental concepts and principles of cyber security.	Written Assessments: Explain key concepts, terminologies, and principles of cyber security. Identify common cyber threats and vulnerabilities. Demonstrate knowledge of basic cyber security tools and techniques.
LO2. Develop skills to identify and mitigate cyber security risks	Oral Assessments: Assess the security posture of an information system. Implement basic security measures to protect information assets. Evaluate the effectiveness of different cyber security strategies.
LO3. Develop effective communication skills in English, both orally and in writing, to convey ideas clearly and coherently fostering intercultural understanding and empathy.	Reading and Research Assessments: Write coherent and well-organized reports and essays demonstrating an understanding of cyber security topics. Articulate ideas clearly and effectively in spoken English during presentations and discussions. Use appropriate communication strategies for different contexts, including technical and non- technical audiences.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cyber Security**	**Introduction to Cyber Security** CIA Triad (Confidentiality, Integrity, Availability), security vs. privacy	LO1: Cyber Security Fundamentals	
2	**Cyber Security Terminologies**	**Cyber Security Terminologies** Threats, vulnerabilities, risks, attacks, countermeasures	LO1: Cyber Security Fundamentals	
3	**Common Cyber Threats**	**Common Cyber Threats** Malware (viruses, ransomware), phishing, DDoS, insider threats	LO1: Cyber Security Fundamentals	
4	**Types of Vulnerabilities**	**Types of Vulnerabilities** Software flaws, misconfigurations, human factors	LO1: Cyber Security Fundamentals	
5	**Security Principles & Frameworks**	**Security Principles & Frameworks** Defense-in-depth, least privilege, NIST CSF	LO1: Cyber Security Fundamentals	
6	**Risk Assessment Fundamentals**	**Risk Assessment Fundamentals** Risk matrices, qualitative vs. quantitative analysis	LO2: Risk Identification & Mitigation	
7	**Security Posture Evaluation**	**Security Posture Evaluation** Asset inventory, vulnerability scanning (Nessus, OpenVAS)	LO2: Risk Identification & Mitigation	
8	Half-Term Exam	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	

9	**Network Security Basics**	**Network Security Basics** Firewalls, IDS/IPS, encryption (SSL/TLS)	LO2: Risk Identification & Mitigation	
10	**Endpoint Protection**	**Endpoint Protection** Antivirus, patch management, device hardening	LO2: Risk Identification & Mitigation	
11	**Incident Response Process**	**Incident Response Process** Detection, containment, eradication, recovery	LO2: Risk Identification & Mitigation	
12	**Basic Security Tools**	**Basic Security Tools** Wireshark (packet analysis), Nmap (network scanning)	LO2: Risk Identification & Mitigation	
13	**Password Security & MFA**	**Password Security & MFA** Password managers, biometrics, OTPs	LO2: Risk Identification & Mitigation	
14	Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	Midterm	- **Midterm assessment** covering all learning outcomes (theory and practical elements)		
16	Feedback & Reflection	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**Security Policies & Awareness**	**Security Policies & Awareness** Acceptable use policies, social engineering training	LO2: Risk Identification & Mitigation	

18	**Cryptography Basics**	**Cryptography Basics** Symmetric vs. asymmetric encryption, hashing	LO2: Risk Identification & Mitigation	
19	**Case Study: Major Cyber Attacks**	**Case Study: Major Cyber Attacks** Equifax breach, WannaCry ransomware	LO3: Security Tools & Techniques	
20	**Technical Report Writing**	**Technical Report Writing** Structure, clarity, referencing (APA/IEEE)	LO3: Security Tools & Techniques	
21	**Cyber Security Presentations**	**Cyber Security Presentations** Audience adaptation, visual aids, Q&A handling	LO3: Security Tools & Techniques	
22	**Stakeholder Communication**	**Stakeholder Communication** Translating technical risks for executives	LO3: Security Tools & Techniques	
23	Half-Term Exam	**Hands-On Lab: Security Tools** Wireshark traffic analysis, malware detection		
24	**Intercultural Cyber Security**	**Intercultural Cyber Security** Global regulations (GDPR vs. CCPA), cross-border threats	LO3: Security Tools & Techniques	
25	**Ethical & Legal Considerations**	**Ethical & Legal Considerations** Ethical hacking, cyber laws, whistleblowing	LO3: Security Tools & Techniques	
26	**Simulation: Phishing Awareness**	**Simulation: Phishing Awareness** Identifying phishing emails, reporting procedures	LO3: Security Tools & Techniques	
27	**Role-Play: Incident Response**	**Role-Play: Incident Response** Mock breach scenario with team coordination	LO3: Security Tools & Techniques	
28	**Final Knowledge Check**	**Final Knowledge Check** Written exam + practical demonstration	LO3: Security Tools & Techniques	

29	Final Exam Preparation & Review	LO1, LO2, LO3	LO1, LO2, LO3	
30	Final Exam		LO1, LO2, LO3	