INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

"Approved"

2025 y. "__" _____

Programme	**LEVEL 4 EXTENDED DIPLOMA IN CYBER SECURITY**		
Unit Number/ Unit Title	**UNIT 5 APPLICATION SECURITY**		
Cohort Code:	L04APS-U5		
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 aims to provide students with a comprehensive understanding of operating system security principles and practices. It prepares students to secure various operating systems by implementing appropriate security measures and addressing potential 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** • Stuttard, D., & Pinto, M. (2011). "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws." Wiley. • OWASP Foundation. (2021). "OWASP Top 10: The Ten Most Critical Web Application Security Risks." OWASP Foundation. • Six, J. (2011). "Application Security for the Android Platform: Processes, Permissions, and Other Safeguards." O'Reilly Media. • Viega, J., & McGraw, G. (2001). "Building Secure Software: How to Avoid Security Problems the Right Way." Addison-Wesley Professional. • Scambray, J., Liu, V., & Sima, C. (2010). "Hacking Exposed Web Applications: Web Application Security Secrets and Solutions." McGraw-Hill Education. • Wong, C. (2011). "Security Metrics, A Beginner's Guide." McGraw-Hill Education.

Learning Outcome	Assessment Criteria
LO1. Understand the Basics of Business Computing	- Define fundamental concepts of business computing, including hardware, software, and networks. - Explain the role of information technology in supporting business operations and decision-making.
LO2. Demonstrate Proficiency in Office Applications	- Use office applications (e.g., word processing, spreadsheets, presentations) to create and manipulate business documents. - Apply formatting and advanced features to enhance the quality of documents. - Solve business problems using office applications.
LO3. Explore Database Management Concepts	- Understand database management concepts, including data organization, retrieval, and data integrity. - Design and create simple databases to store and retrieve business information - Execute basic queries to extract meaningful insights from databases
LO4. Introduce Business Information Systems	- Define business information systems and their components (e.g., ERP, CRM, MIS). - Explore how information systems support various business functions. - Analyze the impact of information systems on organizational efficiency and decision-making.
LO5. Apply Security and Ethical Considerations in Computing	- Identify common security threats and vulnerabilities in business computing environments. - Implement basic security measures to protect business information and systems. - Discuss ethical considerations related to business computing and information technology.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Core Concepts of Business IT Security**	**Core Concepts of Business IT Security** CIA Triad in business contexts (e.g., CRM data confidentiality)	LO1: Foundations of Secure Business Computing	
2	**Hardware Security**	**Hardware Security** Endpoint protection, BYOD policies, encryption for business devices	LO1: Foundations of Secure Business Computing	
3	**Software Security**	**Software Security** Secure SDLC, patch management for business applications	LO1: Foundations of Secure Business Computing	
4	**Network Security for Business**	**Network Security for Business** VPNs, secure Wi-Fi, firewall configurations for SMBs	LO1: Foundations of Secure Business Computing	
5	**IT's Role in Secure Business Operations**	**IT's Role in Secure Business Operations** Case study: POS system breaches (e.g., Target 2013)	LO1: Foundations of Secure Business Computing	
6	**Document Security Best Practices**	**Document Security Best Practices** Password-protected files, digital signatures (Word/PDF)	LO2: Secure Use of Office Applications	
7	**Spreadsheet Security**	**Spreadsheet Security** Data validation, macro security, sensitive data masking (Excel)	LO2: Secure Use of Office Applications	
8	Review	- Review of LO1 topics - Practice questions and mock assessment	LO1 LO2	

9	**Presentation Security**	**Presentation Security** Secure sharing, metadata removal (PowerPoint)	LO2: Secure Use of Office Applications	
10	**Advanced Features for Security**	**Advanced Features for Security** Track Changes (audit trails), version control in Office 365	LO2: Secure Use of Office Applications	
11	**Solving Business Problems Securely**	**Solving Business Problems Securely** Secure financial modeling, redacting PII in documents	LO2: Secure Use of Office Applications	
12	**Database Security Fundamentals**	**Database Security Fundamentals** SQL injection, role-based access (e.g., MySQL, Access)	LO3: Database Security & Management	
13	**Data Organization & Integrity**	**Data Organization & Integrity** Constraints, ACID properties, backup strategies	LO3: Database Security & Management	
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	**Secure Database Design**	**Secure Database Design** Normalization with security considerations	LO3: Database Security & Management	
18	**Query Security**	**Query Security** Parameterized queries, preventing data leakage	LO3: Database Security & Management	
19	**Business Insights with Security**	**Business Insights with Security** Anonymized reporting (k-anonymity in queries)	LO3: Database Security & Management	

20	**ERP Security**	**ERP Security** SAP/Odoo user roles, segregation of duties	LO4: Securing Business Information Systems	
21	**CRM Security**	**CRM Security** Encryption of customer data (Salesforce, HubSpot)	LO4: Securing Business Information Systems	
22	**MIS Security**	**MIS Security** Secure dashboards, access logs for decision-making systems	LO4: Securing Business Information Systems	
23	Review	**Project** Design a security policy for a small business IT environment	LO4: Securing Business Information Systems	
24	**Impact of Security on Efficiency**	**Impact of Security on Efficiency** Trade-offs: Security vs. usability in business systems	LO4: Securing Business Information Systems	
25	**Case Study: System Breaches**	**Case Study: System Breaches** Equifax (CRM), Colonial Pipeline (ERP)	LO4: Securing Business Information Systems	
26	**Threat Identification**	**Threat Identification** Phishing simulations, malware awareness for staff	LO5: Security & Ethics in Practice	
27	**Basic Security Measures**	**Basic Security Measures** MFA, email encryption, secure file sharing	LO5: Security & Ethics in Practice	
28	**Ethical Computing**	**Ethical Computing** Data privacy laws (GDPR/CCPA), employee monitoring ethics	LO5: Security & Ethics in Practice	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	