Level 5 Diploma in PC Engineering & Structured Cabling (108)
133 Credits

Unit: Computer Security **Exam Paper No.:** 5	**Guided Learning Hours:** 220 **Number of Credits:** 22
Prerequisites: Knowledge in Windows Operating System.	**Corequisites:** A pass or better in Certificate in Networking or equivalence.
Aim: Ensuring the security of the vast and complex infrastructure of computers, servers and networks is an immense challenge. Whenever computing technology is used to provide new or improved services, it gives potential attackers new opportunities to cause damage by accessing or modifying sensitive information. This unit incorporates theory and practice of designing and building secure computer systems that protects information and resists attacks. It aims to equip learners with all the required theoretical and practical knowledge to enter a career in development of security systems, or information security consultancy. The unit provide learners the advanced skills needed to learn how to protect networks, secure electronic assets, prevent attacks, insure the customer privacy, and build secure infrastructures. The knowledge gained in this unit will be of great use to numerous fields including network security, forensics, audit, security leadership, and application security.	
Required Materials: Recommended Learning Resources.	**Supplementary Materials:** Lecture notes and tutor extra reading recommendations.
Special Requirements: The course requires a combination of lectures, demonstrations and class discussions.	
Major Learning Outcomes:	**Assessment Criteria:**
1. How throughout the world organisations are increasingly targeted by overlapping surges of cyber attacks.	1.1 Describe security problems 1.2 Analyse and narrate security incidents 1.3 Analysing and identify security threats 1.4 Identify LAN, cloud computing and eCommerce security issues
2. Computer and information security terminology concepts and administering security features.	2.1 Define security terminology 2.2 Analyse access control 2.3 Define authentication 2.4 Describe security models
3. Organisational security systems; the role of people in security and data breaches caused by people rather than technical failure.	3.1 Describe organisational security policies, procedures, standards and guidelines 3.2 Identify physical security aspects 3.3 Describe electromagnetic eavesdropping 3.4 Identify poor security practices 3.5 Describe application vulnerabilities
4. The avenues for exploiting and compromising web servers using brute force password guessing attacks and web application attacks.	4.1 Describe encryption algorithms 4.2 Describe hashing methods/formulas 4.3 Distinguish symmetric and asymmetric encryption 4.4 Identify and analyse the purpose of encryption
5. How Public Key Infrastructure (PKI) enable users unsecure public network such as the Internet to securely and privately exchange data and money.	5.1 Analyse the public key framework 5.2 Describe certificate technology and verification techniques 5.3 Identify certificate classes and architectural models 5.4 Identify PKI standards and protocols 5.5 Analyse interoperability issues with PKI standards
6. How Encrypting folders and files as a way of protecting them from unwanted access and firewalls offers security.	6.1 Describe Encrypting File System (EFS) 6.2 Describe how physical security affects network security 6.3 Explain steps to mitigate security risks 6.4 Describe network architecture and components 6.5 Describe network security concerns

	6.6 Describe network security design topologies
7. Connection and authentication issues in remote access and how users cannot reach locations beyond the remote access server.	7.1 Describe remote access protocols and procedures 7.2 Describe wireless security implications 7.3 Define Virtual Private Network (VPN) 7.4 Define Internet Protocol Security (IPSec)
8. The concepts of Intrusion Detection Systems (IDS), how they work, what sorts of things they monitor for, what the results mean.	8.1 Describe the origins of intrusion detection system 8.2 Identify the purpose of IDS 8.3 Analyse incident response plan steps
9. Understand how to establish a well defined security configuration baseline hardware and applications that run on computer devices.	9.1 Be able to create a password policy 9.2 Describe operating system and network hardening 9.3 Develop an organisational security baseline 9.4 Produce a security baseline checklist 9.5 Create a corporate security baseline for Windows Operating System
10. How organisations prevent computer and network attacks using routers and firewalls to help control access to a home computer.	10.1 Analyse the different categories of attacks 10.2 Describe malicious software 10.3 Define auditing 10.4 Analyse email security issues 10.5 Discuss email security practices 10.6 Examine web components and services 10.7 Describe web security protocols 10.8 Describe the difference between network intrusion prevention and network detection systems
Methods of Evaluation: A 2½-hour written examination paper with five essay questions, each carrying 20 marks. Candidates are required to answer all questions. Candidates also undertake project/coursework in Computer Security with a weighting of 100%.	

Recommended Learning Resources: Computer Security

Text Books	• Computer Security by Dieter Gollmann ISBN-10: 0470741155 • Security in Computing by Charles P. Pfleeger and Shari Lawrence Pfleeger ISBN-10: 0132390779 • Computer Security: Principles and Practice by William Stallings and Lawrence Brown ISBN-10: 013513711X
Study Manuals 	BCE produced study packs
CD ROM 	Power-point slides
Software 	Windows Server