Level 4 Certificate in Networking (107) 129 Credits

Unit: Network Security **Exam Paper No.:** 5	**Guided Learning Hours:** 220 **Number of Credits:** 22
Prerequisites: Basic knowledge in the use of Microsoft Windows Applications.	**Corequisites:** A pass or higher in Diploma in Information Technology or equivalence
Aim: This unit provides the learner with key concepts and fundamentals of Network Security. Network security is a major issue for enterprises, with breaches of security possibly being punished by legal sanctions, financial loss, or loss of customer confidence; hence the aim of this unit is to highlight these issues. Topics covered include security appliances; firewalls, proxies, Intrusion Detection Systems; security services such as confidentiality, integrity and authentication; and technologies - IPSec, SSL, etc. The unit conveys an in-depth exploration of the issues that apply to network security. The Network Security unit provides critical foundational information concerning firewall technology, security risks and remediation, as well as network security design concepts, implementation and considerations. Additionally, learners will learn how to configure and implement firewall appliances, and extend firewall capabilities using rules, security applications and other network specific functions, and troubleshooting techniques. The unit also cover: IPSec overview; VPN; Network Address Translation; Configuring the Firewall; Working with Zones, Groups, and Objects; Security Services; Demilitarized Zone (DMZ), FW Services, Routing and Policies, Proxy Relay, load Balancing and Failover, Probe and Monitor. On completion learners will be well placed to contribute to the security solution of a modern organisation.	
Required Materials: Recommended Learning Resources.	**Supplementary Materials:** Lecture notes and tutor extra reading recommendations.
Special Requirements: The unit requires a combination of lectures, demonstrations, discussions, and hands-on labs.	
Intended Learning Outcomes:	**Assessment Criteria:**
1. The security terminology; information security legal issues and grasping new identity theft prevention tactics.	1.1 Review security terminology 1.2 Describe steps in safeguarding data and information 1.3 Describe security attacks 1.4 Describe hacking technologies 1.5 Define confidentiality, integrity and accountability
2. Management security decisions; identify administrative and technical security; Information systems security issues and decisions for businesses and the key factors for security management.	2.1 Describe risk analysis stages 2.2 Describe network standards and architecture 2.3 Describe organisational security policies 2.4 Conduct an information security assessment
3. The basic elements of cryptography; computer security issues and threats; symmetrical cryptography vs asymmetrical cryptography.	3.1 Define cryptography 3.2 Explain encryption concepts and the different types of encryption 3.3 Describe computer security issues and threats 3.4 Describe the hashing algorithm
4. The popular cryptographic standards and identifying issues with viruses, trojan horses and worms.	4.1 Define VPN 4.2 Define SSL/TLS 4.3 Describe wireless LAN security 4.4 Describe the different types of intrusion detection system

5. Central authentication and analysing how central authentication servers receive data.	5.1 Describe access control systems 5.2 Explain access cards and tokens 5.3 Describe biometric authentication 5.4 Identify Public key infrastructure 5.5 Describe RADIUS authentication
6. Understand the importance of firewalls and the implementation of a firewall.	6.1 Describe firewall operation 6.2 Explain the firewall architecture concepts 6.3 Describe the type of firewalls
7. The elements of host data; important computer security threats and technologies.	7.1 Describe host threats 7.2 Describe server threats 7.3 Analyse Unix security issues 7.4 Describe Windows security issues
8. The steps in securing network applications in both client-side and server side security.	8.1 Describe application security threats 8.2 Explore web and ecommerce services 8.3 Identify browser security issues and protections available 8.4 Describe email security issues 8.5 Describe VOIP security threats 8.6 Describe other internet technology application security concerns 8.7 Describe TCP/IP supervisory protocols 8.8 Describe the internet architecture 8.9 Be able to explain database server security issues 8.10 Describe wireless security issues
9. Different ways of responding to incidents, disasters and the recovery plans.	9.1 Describe the process of responding to an intrusion 9.2 Analyse cybercrime international laws 9.3 Describe backup processes 9.4 Define risk 9.5 Describe the components of risk
Methods of Evaluation: A 2-hour written examination paper with Section A and Section B. Section A has 40 multiple choice questions. Section B has three essay questions, each carrying 20 marks. Candidates are required to answer all questions. Candidates also undertake project/coursework in Network Security with a weighting of 100%.	

Recommended Learning Resources: Network Security

Text Books	- Network Security: Private Communication in a Public World (2nd Edition) by Charlie Kaufman, Radia Perlman, and Mike Speciner ISBN-10: 0130460192 - Network Security Essentials: Applications and Standards by William Stallings ISBN-10: 0136108059 - Microsoft Windows Security Essentials by Darril Gibson. ISBN-13 : 978-1118016848
Study Manuals	BCE produced study packs
CD ROM	Power-point slides
Software	Server Operating System (Optional)