Level 5 Diploma in Internet Security (615) 177 Credits

<table>
<tr><td><b>Unit:</b> Cyber Security

<b>Exam Paper No.:</b> 3</td><td><b>Guided Learning Hours:</b> 200

<b>Number of Credits:</b> 20</td></tr>
<tr><td><b>Prerequisites:</b> Basic networking concepts and network protocol technology knowledge</td><td><b>Corequisites:</b> Internet technology.</td></tr>
<tr><td colspan="2"><b>Aim:</b> Cyber security is important to all business entities. Types range from hacking, ranson ware, social engineering, viruses/malware and physical security attacks. There are many challenges regarding cyber security mainly because of the sheer number of devices connected to the internet. Because of the number of data breaches and services management online; cyber security is a growing field. Knowledge in cyber security leads to opportunities in different organisations.

Unfortunately, cyber security threats are always evolving, and each latest attack becoming more prevalent and sophisticated; hence knowledge in this field is also constantly revolving. There are many reasons for learning cyber security; including:
• Not many people have the skill sets
• The world is becoming more networked and someone is looking to take advantage of insecure connections.
• There is demand Cyber security specialists especially from small businesses who not have the resources and knowhow</td></tr>
<tr><td><b>Required Materials:</b> Recommended Learning Resources.</td><td><b>Supplementary Materials:</b> Lecture notes and tutor extra reading recommendations.</td></tr>
<tr><td colspan="2"><b>Special Requirements:</b> This is a hands-on unit, hence practical use of computers is essential. Requires intensive lab work outside of class time.</td></tr>
<tr><td><b>Intended Learning Outcomes:</b>
<i><b>Learners to do Network Security first</b></i></td><td><b>Assessment Criteria:</b>
<i>Learners to do Network Security first</i></td></tr>
<tr><td>1. Understand the mechanism of Cyber Security including data protection, Confidentiality, Integrity and Availability (CIA)</td><td>1.1 Describe cyber security
1.2 Demonstrate implementation of cyber security
1.3 Describe implementation of network security
1.4 Identify web applications vulnerabilities
1.5 Be able to describe different cyber attacks
1.6 Describe cyber security challenges
1.7 Discuss recent cyber-crimes around the world</td></tr>
<tr><td>2. Understand causes and effects of security incidents; including why they occur and how to prevent data breaches.</td><td>2.1 Describe data breach phases
2.2 Describe cryptographic techniques
2.3 Demonstrate private browsing
2.4 Demonstrate steps in protecting a computer from viruses
2.5 Be able to conduct malware analysis</td></tr>
<tr><td>3. Understand SSL certificates, different SSL certificate providers and why certificates are important in authenticating a website's identity and enabling an encrypted connection.</td><td>3.1 Describe functions of SSL certificates
3.2 Describe fraud detection techniques
3.3 Describe different types of network attacks
3.4 Discuss benefits of cyber laws.</td></tr>
</table>

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 coursework/projects in Cyber Security.

Recommended Learning Resources: Cyber Security

Text Books	• Computer Networking and Cybersecurity by Quinn Kiser. ISBN-13 : 979-8682990887 • Confident Cyber Security by Jessica Barker . ISBN-13 : 978-1789663402 • Cybersecurity: The Beginner's Guide. by Dr. Erdal Ozkaya. ISBN-13 : 978-1789616194
Study Manuals	BCE produced study packs
CD ROM	Power-point slides
Software	N/A