ZETECH UNIVERSITY
Inventing the future

F-7-16

Unit Code:	**DCF 221**
Unit Title:	**CYBER SECURITY ESSENTIALS**
Program(s):	DCF
Lecturer Name:	Brian Mwangi
Lecturer Contacts:	**Email:** brian.mwangi@gmail.com , **Phone No**: 0722940239
Consultation time :	08:00 AM – 09:00 PM

Purpose of the course:

The purpose of this course is to provide students with skills in cyber security. It explores the basics of cyber trends and threats, exploitation and defense techniques along with the illustration using the available Open Source tools. It provides an understanding of the fundamental principles of cyber security at a decision-making level. Cyber security Essentials is the ideal course for anyone who needs to get a good all-round understanding of Cyber security. The content of this training course represents the essentials of Cyber security, and it is designed in the way that the capabilities learned by following this training course will be used to protect organizations and the society as a whole from areas of emerging threats

Expected Learning Outcomes

By the end of this unit, the student should be able to:

1. Understand key terms and concepts in cyber security
2. Analyze and evaluate the cyber security needs of an organization.
3. Evaluate decision making outcomes of Cybersecurity scenarios
4. Analyze threats and risks within context of the Cybersecurity landscape
5. Understand and acquire comprehensive knowledge on the main concepts of Cybersecurity
6. Take steps towards creating a Cybersecurity culture within an organization

COURSE SYLLABUS AND SCHEDULE

WEEK	TOPIC	SUB - TOPIC
1	Introduction Cybersecurit	✓ A World of Wizards, Hero's and Criminals. ✓ Evolution of Cyber Threats ✓ Importance of cybersecurity in the modern world.
2	The Cybersecurity Sorcery Cube	✓ Dimensions of Cybersecurity Cube ✓ Cybersecurity Countermeasures ✓ IT Security Management Framework
3	Cybersecurity Threats, Vulnerabilities, and Attacks	✓ Top Cybersecurity Breaches ✓ Common Vulnerabilities in Systems ✓ Types of Cyber Attacks
4	Cybersecurity Awareness	✓ Elements of a Cybersecurity Awareness Program ✓ Building a Security-Conscious Organization
5	Cybersecurity Concepts and Standards	✓ Confidentiality, Integrity, and Availability (CIA Triad) ✓ Risk Management and Compliance ✓ Cybersecurity Key Standards
	Assignment 1	
6	The Art of Protecting Secrets	Cryptography Access Control Obscuring Data
7	The Art of Ensuring Integrity	✓ Types of Data Integrity Controls ✓ Digital Signatures and Certificates ✓ Database Integrity Enforcement
	CAT 1	
8	The Realm of Five Nines	High Availability Measures to Improve Availability

		✓ Disaster Recovery Planning
9	Fortifying the Kingdom	✓ Defense-in-Depth and Layered Security Models ✓ Network Segmentation and Isolation ✓ Incident Response and Management
Assignment 2		
10	Protecting a Cybersecurity Domain	✓ Defending Systems and Devices ✓ Server Hardening ✓ Network Hardening ✓ Physical Security
11	Joining the Order of Cybersecurity Specialists	✓ Cybersecurity Domains ✓ Cybersecurity Culture and Its Importance ✓ Building a Career in Cybersecurity ✓ Ethical Considerations in Cybersecurity
12	Emerging trends in cyber security.	✓ Artificial Intelligence and Machine Learning in Cybersecurity ✓ The Internet of Things (IoT) Security Challenges ✓ Zero Trust Security Models ✓ Cloud Computing ✓ Quantum Computing and Its Impact on Cybersecurity
CAT 2		
13	**Recess Week**	

Mode of Delivery

This will include face-to-face and blended learning

Teaching Methodology

Lecture method, Group activities, Class discussions, Demonstrations, illustrations and role-plays.

Instructional Materials and or Equipment

Overhead Projector, Handouts, Textbooks, white board marker, LMS, Software tools and Applications.

Assessment Criteria

Assessment Type	Frequency	Percentage
Assignment/presentation	2	10%
CATs	2	30%
Final Examination	1	60%
Total		100%

REFERENCE TEXTBOOKS

Core Textbooks

1. ALDER, A. (2023). Cyber essentials. https://doi.org/10.2307/jj.4575420
2. Cyber security and cyber risk. (2016). *Cyber Security*, 11 24. https://doi.org/10.4324/9781315575674-4
3. Trim, P., & Lee, Y. (2022). *Strategic Cyber Security Management*, 209-219. https://doi.org/10.4324/9781003244295-11

Recommended Textbooks

1. Trim, P., & Lee, Y. (2022).. *Strategic Cyber Security Management*, 1-9. https://doi.org/10.4324/9781003244295-1
2. Graham, (2016). *Cyber Security Essentials*, 17-90. https://doi.org/10.1201/b10485-5

E-Resources

1. Bradbury, R. (2021). Educating for cyber (Security). *The Oxford Handbook of Cyber Security*, 394-408. https://doi.org/10.1093/oxfordhb/9780198800682.013.24

2. Yamin, M. M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios

in cyber ranges. *Computers & Security*, *116*, 102635. https://doi.org/10.1016/j.cose.2022.102635

3. Cyber Security: Essential Principles to Secure Your Organisation. https://ebookcentral.proquest.com/lib/zetech/detail.action?docID=6176700
4. Practical AI for Cybersecurity. https://www.taylorfrancis.com/books/mono/10.1201/9781003005230/practical-ai-cybersecurity-ravi-das?context=ubx&amp;refId=4989fa69-94b6-4ba6-bfe9-f1171058adee

Approval for circulation by:

Unit Lecturer Name: …………Brian Mwangi………………………… Signature: ……Kbmw……

HOD name: David Kanyi **signature:**

ZETECH UNIVERSITY
P.O. BOX 2758 - 00200

SCHOOL OF ICT MEDIA &
ENGINEERING

Head of ICT and Engineering Department