EACO East African Communications Organisation
Communications for all in East Africa

MMU

# MULTIMEDIA UNIVERSITY OF KENYA (MMU)

## COURSE OUTLINE

**TITLE: CYBERSECURITY TRAINING COURSE**

**Duration:** **5 days**

---

# CYBERSECURITY TRAINING COURSE

**Course Overview**
The Cyber security Training Course will provide learners with principles of data and technology that frame and define cyber security. Learners will cover five key areas of cyber security:

1) Cyber security concepts
2) Security architecture principles
3) Security of networks, systems, applications and data
4) Incident response and
5) The security implications of the adoption of emerging technologies.

**Target Audience**
• Regulatory employees working in IT/Cyber Security or Information Security Departments
• Audit, Risk, Compliance, Information Security, government and legal professionals with a familiarity of basic IT/IS concepts who:

- are new to cyber security
- are interested in entering the field of cyber security
- are interested in the ISACA Cyber security Fundamentals Certificate

**Learning Objectives:**
• Explain the core information assurance (IA) principles

• Identify the key components of cybersecurity network architecture
• Apply cybersecurity architecture principles
• Describe risk management processes and practices
• Identify security tools and hardening techniques
• Distinguish system and application security threats and vulnerabilities
• Describe different classes of attacks
• Define types of incidents including categories, responses and timelines for response
• Describe new and emerging IT and IS technologies
• Analyze threats and risks within context of the cybersecurity architecture
• Appraise cybersecurity incidents to apply appropriate response
• Evaluate decision making outcomes of cybersecurity scenarios
• Access additional external resources to supplement knowledge of cybersecurity

**Course Description (5Days)**

- Day 1: Introduction to Cyber Security
    a. Cyber security objectives
    b. Cyber security roles
    c. Differences between Information Security & Cyber Security
- Day 1: Cyber Security Principles
    a. Confidentiality, integrity, & availability
    b. Authentication & nonrepudiation
- Day 2: Information Security (IS) within Lifecycle Management
    a. Lifecycle management landscape
    b. Security architecture processes
    c. Security architecture tools
    d. Intermediate lifecycle management concepts
- Day 3: Risks & Vulnerabilities
    a. Basics of risk management
    b. Operational threat environments
    c. Classes of attacks
- Day 4: Incident Response
    a. Incident categories
    b. Incident response
    c. Incident recovery
- Day 5: Future Implications & Evolving Technologies
    a. New & emerging IT & IS technologies
    b. Mobile security issues, risks, & vulnerabilities
    c. Cloud concepts around data & collaboration