**Meru University of Science and Technology**

**School of Computing and Informatics**

**Department of Computer Science**

---

**Course code:** CCF 3100 **Course Title**: Fundamentals of PC Security and Privacy

**Year of study:** First **Semester**: Second **Academic year:** 2025

**Pre-requisite** None

**Contact Hours** 45

## COURSE PURPOSE

This course introduces students to the various potential threats and sources of attacks to network security and a solid understanding issues related to privacy of computer systems and networks.

## EXPECTED LEARNING OUTCOMES

By the end of the course the student should be able to:

a. Discuss various issues related to computer security and network attacks.
b. Assess the risks on a computer system;
c. Develop suitable security policies for an organization
d. Choose appropriate security mechanisms to ensure data protection.
e. Assess the capabilities and limitations of current security techniques and protocols, identification and authentication, access controls, security models;
f. Elaborate on ethical and legal issues in information systems security.
g. Explain how privacy is related to computer technology.
h. Describe privacy enhancing technologies

**COURSE CONTENT**

| WEEK | MAIN | TOPIC SUB-TOPIC |
|---|---|---|
| 1 | **Students Semester Registrations** | |
| 2 | **Introduction to Computer Systems and Network Security** | Security and the human aspect; Fundamentals of information security principles and concepts; Identification and authentication |
| 3 | **CIA Triage– Confidentiality Integrity Availability** | Security services and requirements; Confidentiality, Integrity, Availability, Authentication, Non Repudiation; Security Mechanisms; Security Attacks |
| 4 | **Password Protection** | Password Protection and Management; guidelines in creating password; user education on password management |
| 5 | **Malicious Software and Intruders** | Viruses and Other Malicious Content, Distributed Denial of Service Attacks (DDoS), Countermeasures; Intruders |
| 6 | **CAT 1** | |
| 7 | **Access Control** | Access control matrix, access control lists and capabilities: Lattice Based Access Control: information flow policies, military lattice, Access control models: Bell-La Padula model, Chinese Wall lattice, Clark Wilson, Role-Based Access Control, RBAC policies and management; Intrusion detection and prevention. |
| 8 | **Operating System Security** | Introduction to Operating system security, operating system security goals; Security designs of different operating systems e.g. Windows, Linux, Unix and Android |

| | | |
|---|---|---|
| 9 | **Network Security** | Firewalls, Trusted Systems, Network attacks and defenses like IDS and IPS; Web and Cyber security, Cybercrimes and defenses; IP security |
| 10 | **CAT 2** | |
| 11 | **Introduction to Privacy** | Security support for popular web application frameworks and technologies. Aspects of privacy, privacy laws, privacy acts referencing countries like Kenya |
| 12 | **Privacy metrics and Privacy enhancing technologies** | Cookies, P3P (Platform for Privacy Preferences) and Audit Trail, Dataset partitioning**,** Tokenization and randomization**,** K-anonymity**,** Differential Privacy |
| 13 | **Cryptography Algorithms and Key Managements** | Introduction to Cryptographic Algorithms: Symmetric and Asymmetric; Security Keys Management |
| 14 & 15 | **Examination** | |

**Mode of delivery**

- Lectures
- Tutorials
- Directed reading
- Hands-on laboratory sessions
- Projects.
- Audio-visual equipment, whiteboard, PCs and networking equipment for lab simulations.
- Security software tools.

**Instructional Materials/ Equipment**

Whiteboard, Markers, Charts, Handouts, Software, LCD projector and Desktop Computers.

**Course Assessment**

| Type | Weighting (%) |
|---|---|
| Examination | 70 |
| Continuous Assessment | 30 |
| Total | 100 |

**Core Reading Material**


1. Randell J.B. & Raymond R. P. (2013). Corporate Computer Security. 3rd Edition. Pearson
2. Bishop, M. (2003). *Computer Security: Art and Science*. Addison-Wesley Professional.


**Recommended Reading Material**


1. McClure, S., Scambray, J., & Kurtz, G. (2012). *Hacking Exposed 7: Network Security Secrets and Solutions*. McGraw Hill Professional.
2. Nichols. (2006). *Wireless Security*. McGraw-Hill Education (India) Pvt Limited.
3. Project, H. (2004). *Know Your Enemy: Learning about Security Threats*. Addison-Wesley.


**NAME OF LECTURER(S):** **SIGN:** **DATE:**

…… …….. ……