

Information Ethics

Course Name: Information Ethics

Course Code: GEN315

Credit hours: 3

Knowledge Domain: General Fundamentals.

Prerequisite(s): Introduction to IT (ITF101) - Introduction to Computer Systems (CAS101) – Introduction to Web Technology (NWE101)

Learning Objectives

Upon completion of this course, the student will be able to:

1. Present Ethics concepts in general and professional ethics in particular.
2. Classify computer crime and different attacks.
3. Realize legal issues and law enforcement and its effect on privacy.

Learning Outcomes:

1. Grasping the main concepts of professional ethics with a sample of two codes of ethics (IEEE and ACM).
2. Acquaintance with the basics of computer crime.
3. Acquaintance with Intellectual Property issues, law enforcement and effects on privacy.

Overview and Syllabus

Introduction to ethics. Professional codes of ethics. Computer crime. Software privacy. Intellectual Property issues. Hacking viruses and Denial of Service. Unreliable computer. Law enforcement and privacy.

Course Outline

	Topic
1	<u>Module 01: Introduction to Ethics</u> Introduction Objectives Lesson 01: What is Ethics? Lesson 02: The difference between Ethics and Morality Lesson 03: Ethics and other perspectives Lesson 04: Ethics, Law, and Religion Lesson 05: The Source of moral values

	<p>Lesson 06: The Relationship between ethical and practical life</p> <p>Summary</p> <p>Assessment</p>
2	<p><u>Module 02: Professional Codes of Ethics</u></p> <p>Introduction</p> <p>Objectives</p> <p>Lesson 01: What is Profession?</p> <p>Lesson 02: What Does it Mean to be a Professional?</p> <p>Lesson 03: Why We Need a Code of Ethics?</p> <p>Lesson 04: The IEEE Code of Ethics</p> <p>Lesson 05: The ACM Code of Ethics</p> <p>Summary</p> <p>Assessment</p>
3	<p><u>Module 03: Computer and Internet Crime</u></p> <p>Introduction</p> <p>Objectives</p> <p>Lesson 01: What is Computer Crime?</p> <p>Lesson 02: Why Computer Incidents are so Prevalent?</p> <p>Lesson 03: Types of Exploits</p> <p>Lesson 04: Types of Perpetrators</p> <p>Lesson 05: Federal Laws for Prosecuting Computer Attacks</p> <p>Summary</p> <p>Assessment</p>
4	<p><u>Module 04: Software Privacy</u></p> <p>Introduction</p> <p>Objectives</p> <p>Lesson 01: Information Privacy: Concepts, Theories, and Controversies</p> <p>Lesson 02: Privacy And Information Control Privacy And Information</p> <p>Lesson 03: Problems of Software Privacy</p> <p>Lesson 04: Key Privacy and Anonymity Issues</p> <p>Lesson 05: Ethics in Software Engineering</p> <p>Summary</p> <p>Assessment</p>
5	<p><u>Module 05: Intellectual Property Issues</u></p> <p>Introduction</p> <p>Objectives</p> <p>Lesson 01: Intellectual Property: Legal and Moral Challenges of Online Files Sharing.</p> <p>Lesson 02: Intangible property, privacy, power and information control.</p> <p>Lesson 03: Are patents and copyrights morally justified? Software patents</p> <p>Lesson 04: Trade Secrets Reverse Engineering</p> <p>Lesson 05: Key Intellectual Property Issues</p> <p>Summary</p> <p>Assessment</p>
6	<p><u>Module 06: Unreliable Computer System</u></p> <p>Introduction</p>

Objectives

Lesson 01: Can we trust computer?

Lesson 02: What is Computer Reliability?

Lesson 03: Complex Systems And Reliability

Lesson 04: The Contingency Planning

Lesson 05: System Crashes

Summary

Assessment