Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 3 :Professional Ethics in Cybersecurity

- Course: CBS221/A Ethics and Legal Issues in Cybersecurity
- Week 3: 19-23/10/2025
- Lecturer: Prof. Dr. Qaysar Mahdy

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Introduction

- Definition of Ethics:
- Ethics is the study of moral principles guiding human behavior.
- Cybersecurity Ethics:
- - Involves principles that guide responsible behavior in protecting information systems.
- - Prevents misuse of technology and ensures trust, accountability, and security.
- Importance:
- - Protect sensitive data
- - Avoid legal consequences
- - Build trust in digital systems

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Professional Codes of Ethics

Overview:

Codes of ethics provide guidance for professional behavior.

Key Codes:

1. ACM Code of Ethics

2. IEEE Code of Ethics

3. ISACA Code of Professional Ethics

Tishk International University
Faculty of Applied Science
Cybersecurity Department

ACM Code of Ethics – Detailed Principles

Contribute	Contribute to society and human well-being
Avoid	Avoid harm to others
Be	Be honest and trustworthy
Be	Be fair and take action not to discriminate
Honor	Honor privacy and confidentiality
Maintain	Maintain professional competence
Avoid	Example: Avoid using hacking skills for personal gain; report vulnerabilities responsibly.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Codes of Ethics in Cybersecurity

- ACM, IEEE, ISC² Codes → honesty, integrity, competence, avoid harm.
- ACM - Association for Computing Machinery

The ACM Code of Ethics and Professional Conduct largely focuses on an ethics of the means to avoid harm, but does not clearly define ethical ends that computing systems should aim to achieve.

→ The code is ineffective in flagging unjust and undesirable goals for which technologies are built or used.

→ The code should embrace goals such as achieving equality and overturning unjust social and economic structures through technological inventions.

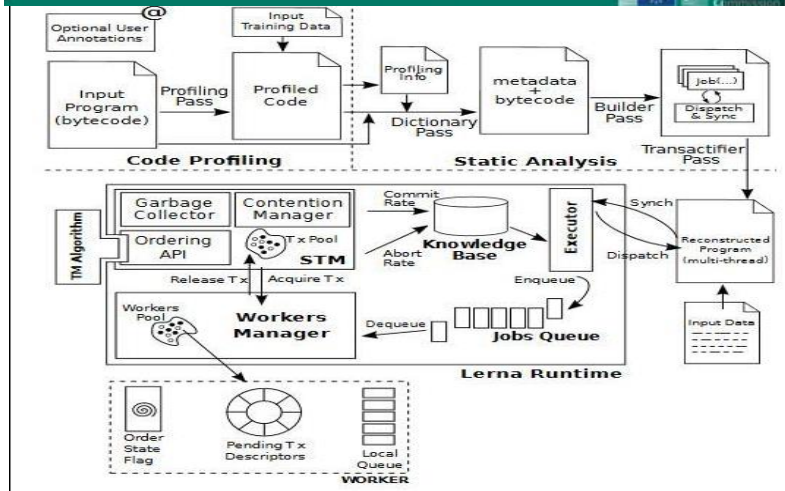


Figure 1: Lerna's Architecture and Workflow

Tishk International University
Faculty of Applied Science
Cybersecurity Department

IEEE Code of Ethics – Highlights

Tishk International University
Faculty of Applied Science
Cybersecurity Department

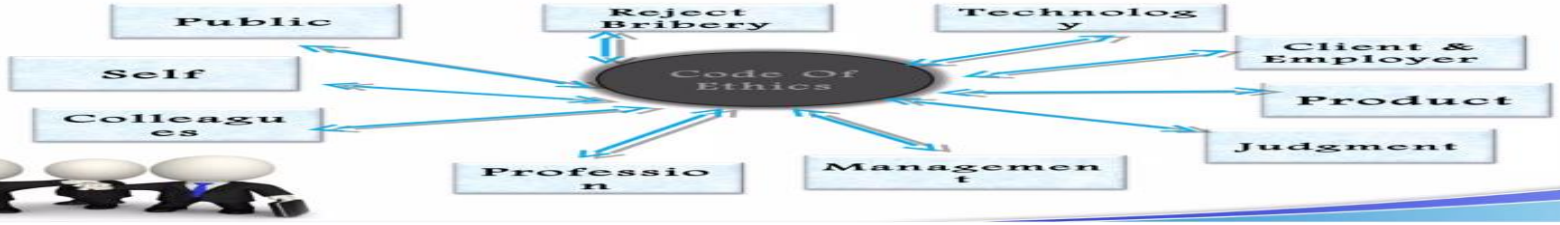
What is IEEE?

- The Institute of Electrical and Electronics Engineers
- An international non-profit, professional organization
- Advancement of technology related to electricity and to electronic applications.

IEEE Code of Ethics

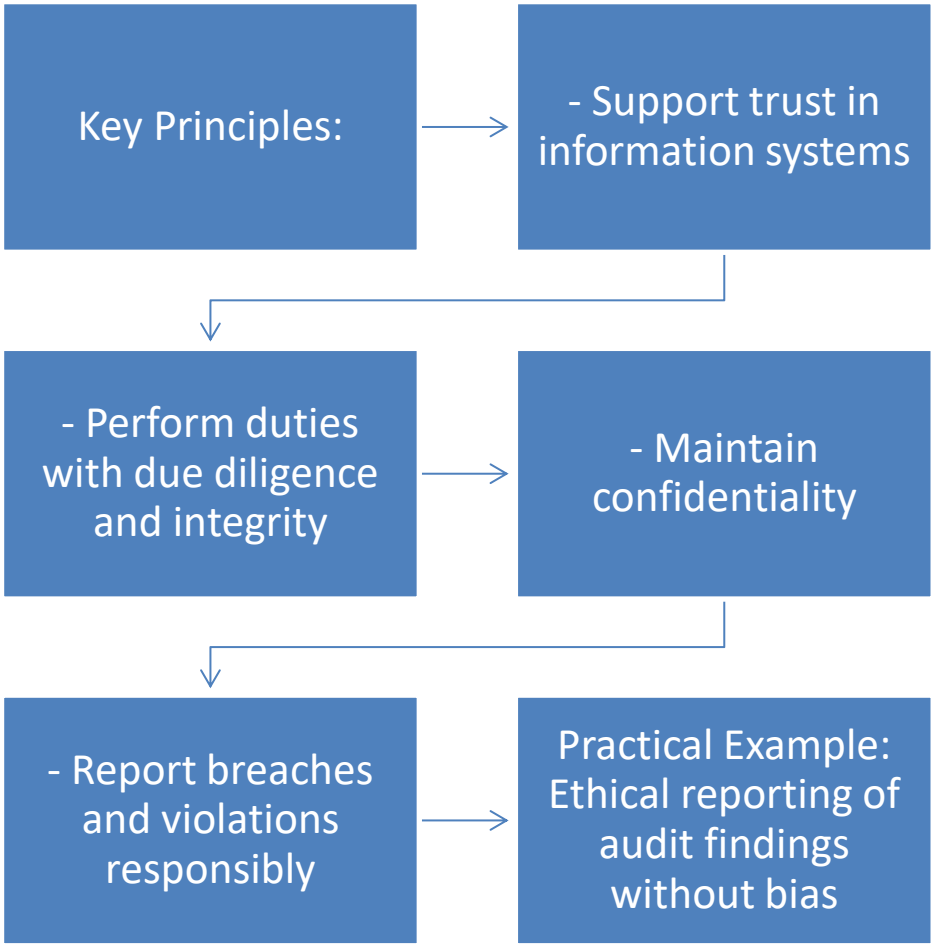
- Formed in 1963 as a merger of AIEE (American Institute of Electrical Engineers) and IRA (Institute of Radio Engineers)
- Worlds largest professional/technical organization for advancement of technology
- IEEE membership requires follow IEEE code of ethics

10 Key Principles



Tishk International University
Faculty of Applied Science
Cybersecurity Department

ISACA Code of Ethics – Highlights



Tishk International University
Faculty of Applied Science
Cybersecurity Department

The ISC² Code of Ethics is a set of four fundamental ethical canons that all certified information security professionals must follow, including protecting society and the public trust, acting with integrity, serving their principals diligently, and advancing the profession. Adherence to the Code is a mandatory condition for ISC² certification and guides ethical decision-making and professional conduct.

The Four Canons of the ISC² Code of Ethics

Protect society, the common good, necessary public trust and confidence, and the infrastructure

.This means ensuring actions contribute to the betterment of society, not harmful activities like unethical hacking.

Act honorably, honestly, justly, responsibly, and legally

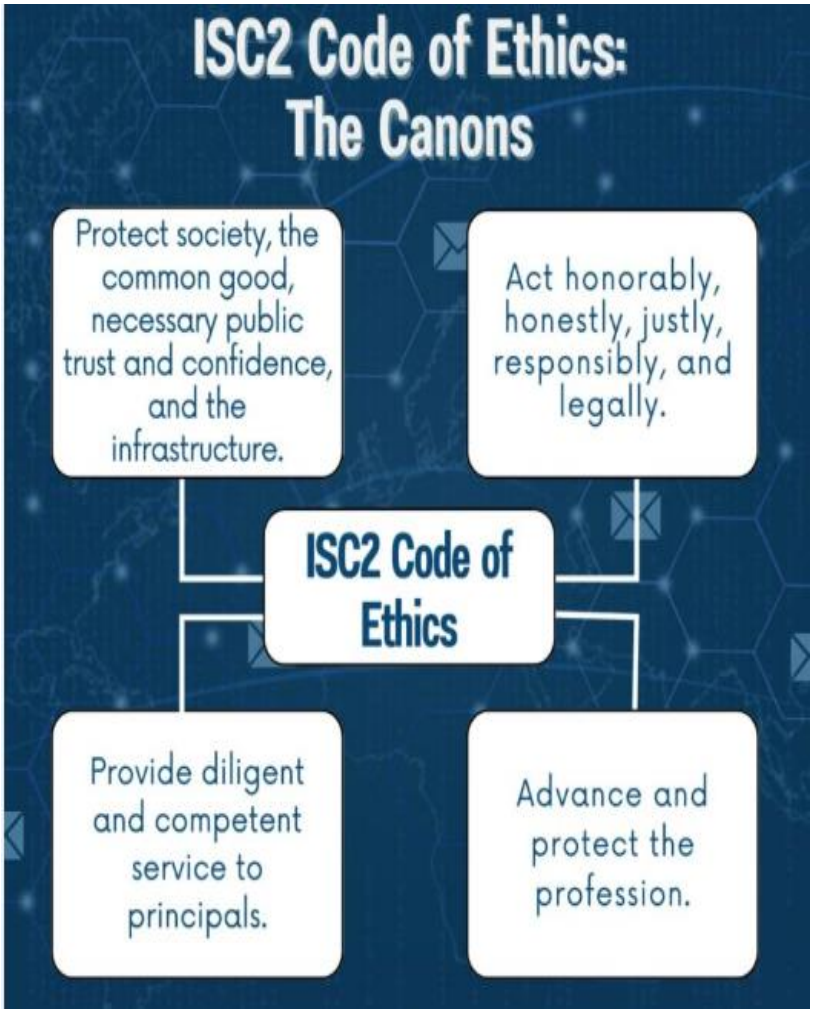
.Violations include breaking the law, lying, or covering up security errors.

Provide diligent and competent service to principals

.Principals can be employers or clients; this canon requires fulfilling assigned duties competently.

Advance and protect the profession

.This involves taking actions that benefit the profession as a whole, not engaging in activities like unauthorized exam assistance.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Responsibilities of Cybersecurity Professionals

- Protecting Systems and Data: Prevent unauthorized access, ensure integrity.
- Legal Compliance: Follow laws, regulations, and industry standards.
- Ethical Decision Making: Apply codes of ethics in daily tasks.
- Continuous Learning: Stay updated on evolving threats and technology.
- Accountability: Accept responsibility for mistakes or lapses

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Common Ethical Dilemmas

Examples:

1. Using company resources for personal projects
2. Reporting security vulnerabilities discovered by accident
3. Privacy concerns with employee monitoring

Approach:

- Identify stakeholders
- Evaluate consequences
- Consult codes of ethics
- Make transparent decisions

Ethical Dilemma

- Ethical dilemma: is a situation with uncertainty about what is right to do from a moral or ethical perspective.
- For example, the manager of a company may be put in a position in which he must choose between the interests of his employees and his investors. Give more profits or increase the salary?

Ethical Dilemma Defined

- **Example 2 :**
- A new technology is being launched which is good for the company as well as the customers. But, if this is brought into use, a lesser man-power is required for the organization.
- The entrepreneur is now in an ethical dilemma whether he wants to better his clients with good services or be loyal to his employees who have helped the company grow.
- The unpleasantness of the situation arises when neither the clients nor the employees deserve to suffer and it is the entrepreneur's call to take.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Case Study

Scenario: Security analyst discovers a colleague leaking sensitive data.

Discussion Points:

- Ethical responsibilities

- Legal obligations

- Reporting channels

Key Lesson: Professional ethics guides proper handling of real-world situations

Summary

- Ethics is essential in guiding cybersecurity professionals
- ACM, IEEE, ISACA codes provide structured ethical frameworks
- Responsibilities include protecting systems, following the law, and ethical decision-making
- Real-life dilemmas highlight the importance of applying ethics consistently

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Quiz / Discussion

Q1: What is the primary goal of professional ethics in cybersecurity?

Q2: Name 2 principles from ACM or IEEE code of ethics.

Q3: What steps would you take if you discover a colleague violating security policies?

References

- ACM Code of Ethics – https://www.acm.org/code-of-ethics
- IEEE Code of Ethics – https://www.ieee.org/about/corporate/governance/p7-8.html
- ISACA Code of Professional Ethics – https://www.isaca.org/code-of-professional-ethics
- Whitman, M., & Mattord, H. Principles of Information Security (7th Edition)

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Thank you for your listening