Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 5 : Cybersecurity and Professional Responsibility

Course: CBS221/A: Ethics and Legal Issues in Cybersecurity

Week 5: 02-06/11/2025

Lecturer: Prof.Dr.Qaysar Salih Mahdi

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Introduction

- Professional responsibility = duty to protect systems, data, and users. Goes beyond legal compliance.
- Key principle: Accountability & trust.
- Equation: ERS = (Impact × Likelihood)/Mitigation
- Example: Insider threat in a corporate network.
- Exercise: Analyst ignores repeated malware alerts → ethical issue?
- Solution: Breach of professional duty & accountability.
- Problem: Calculate ERS if Impact=8, Likelihood=0.5, Mitigation=2. Solution: ERS=2
- Image Link: https://cdn-icons-png.flaticon.com/512/3003/3003180.png
- Conclusion: Professional responsibility is central to cybersecurity ethics.
- References: Quinn, Ethics for the Information Age (2023); Whitman & Mattord, Principles of Info Security (2024)

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.

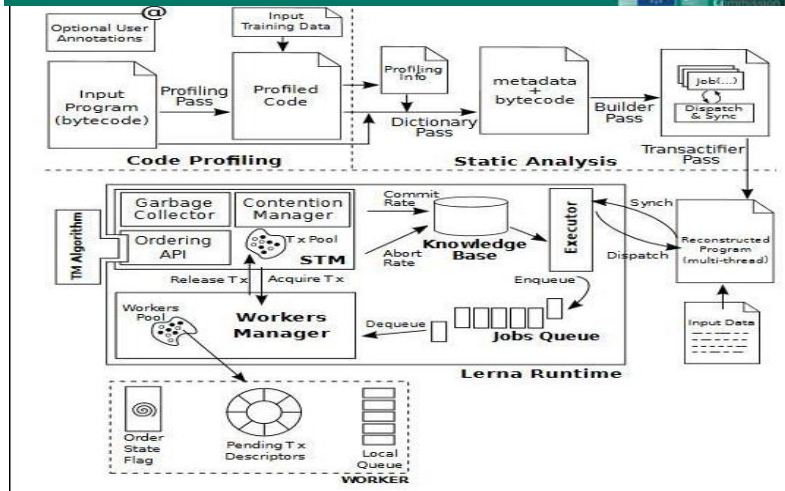


Figure 1: Lerna's Architecture and Workflow

Tishk International University
Faculty of Applied Science
Cybersecurity Department

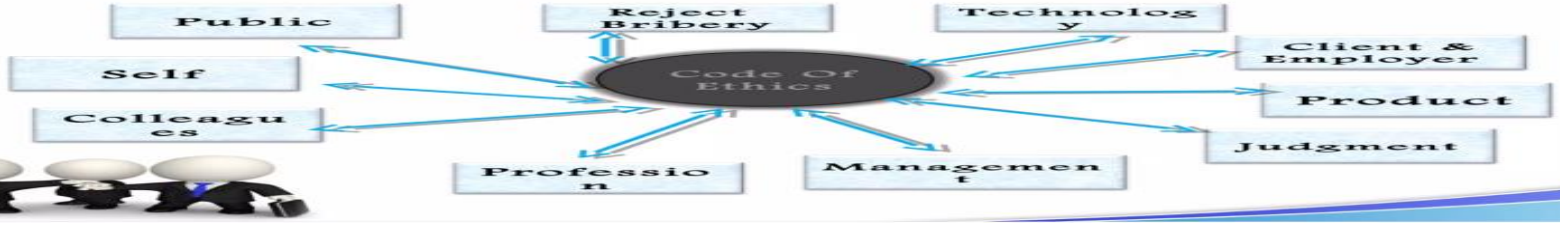
What is IEEE?

- 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

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

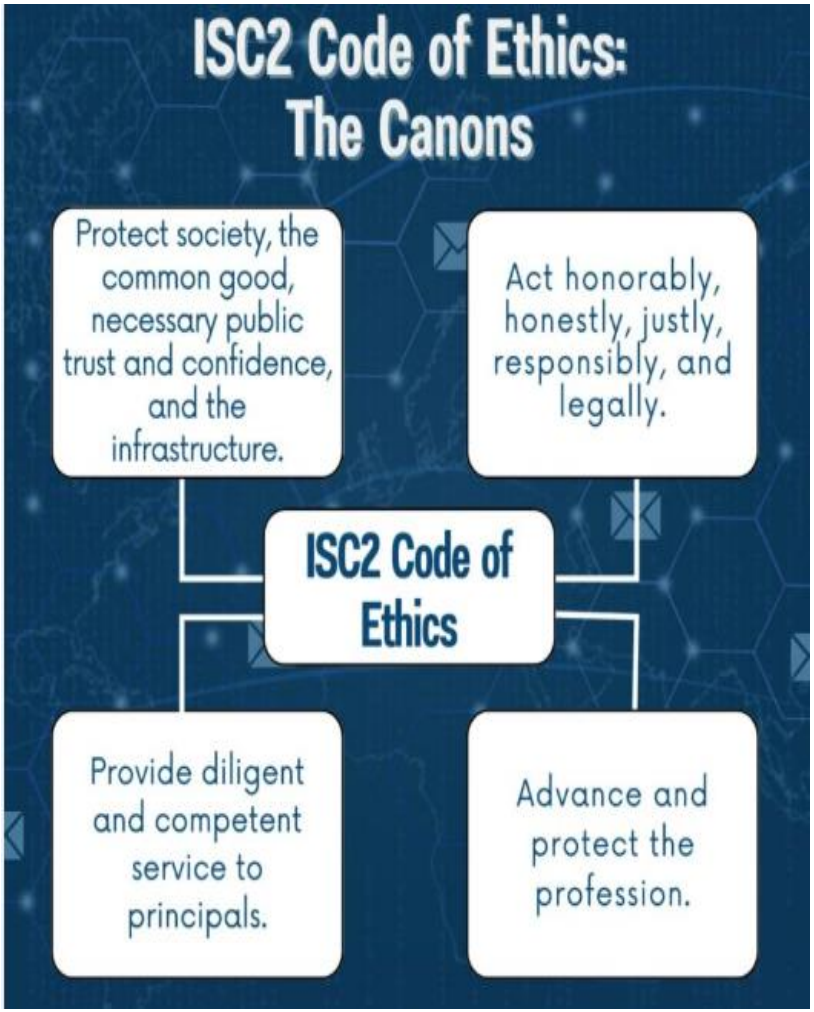
.Violations include breaking the law, lying, or covering up security errors.

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.



Exercise: Employee finds vulnerability → responsible disclosure.

Problem: Compare ACM vs IEEE code → identify 3 key differences.

Solution: ACM emphasizes public interest, IEEE emphasizes avoiding conflicts, ISC² emphasizes competence and legal compliance.

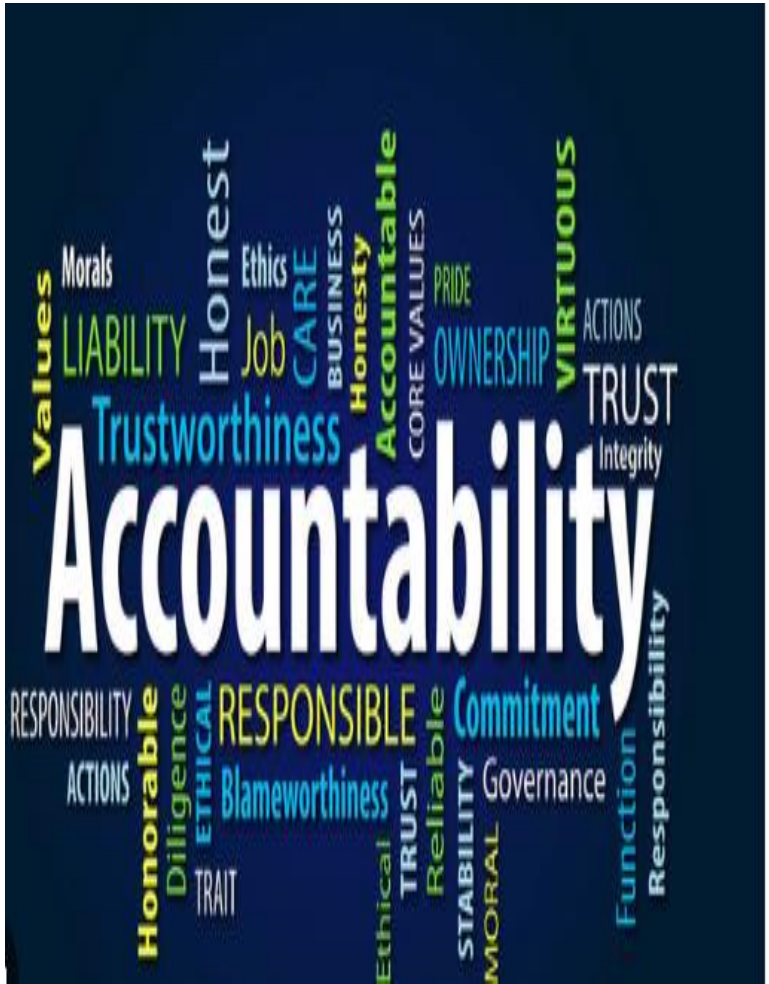
Conclusion: Codes guide decision-making & professional behavior.

References: ACM, IEEE, ISC² Codes (2024 updates)

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Accountability and Liability

- Accountability: professionals answer for actions & decisions. Liability: legal responsibility.
- Equation: LR = Probability of breach × Potential damage × (1 - Compliance factor)
- Example: Failure to patch → company liable.
- Exercise: Outsourced IT without verifying security → who accountable? Solution: Company still accountable.
- Problem: Compute LR if breach probability=0.2, damage=$100,000, compliance factor=0.5. Solution: LR=$10,000
- Conclusion: Professionals must understand ethical & legal accountability.
- References: Whitman & Mattord (2024), Tavani, Ethics and Technology (2023)



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Confidentiality and Privacy Obligations

- Maintain confidentiality of sensitive info; comply with privacy laws.
- Exercise: Sharing colleague's password → ethical violation? Solution: Yes, breaches confidentiality.
- Problem: Analyst sends encrypted files to personal email → breach? Solution: Yes, violates policy.
- Conclusion: Confidentiality = core professional obligation.
- References: Solove & Schwartz, Information Privacy Law (2024)

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Integrity and Honesty

- Accurate reporting, no deception.
- Exercise: Misreporting minor breach → ethical issue? Solution: Violates integrity principle.
- Problem: Employee exaggerates impact of vulnerability for recognition → ethical?
- Solution: No, violates honesty & integrity.
- Conclusion: Integrity = trustworthiness in profession.
- References: ACM Code of Ethics, IEEE Code of Ethics

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Professional Competence

- Maintain skills; do not act beyond expertise.
- Exercise: Attempting advanced exploit without knowledge → ethical issue?
- Solution: Yes, violates competence.
- Problem: Identify competence violations in 3 cases → misconfigured firewall, untested scripts, ignoring standards.
- Image Link: https://cdn-icons-png.flaticon.com/512/2896/2896761.png
- Conclusion: Competence ensures safe, ethical decisions.
- References: ISC² Code of Ethics, Whitman & Mattord (2024)

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Conflicts of Interest

- Avoid personal vs professional duty conflicts.
- Exercise: Analyst invests in competitor → ethical action? Solution: Disclose conflict & recuse.
- Problem: Employee receives vendor gift → conflict? Solution: Must report.
- Conclusion: Managing conflicts preserves professional integrity.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Responsible Disclosure

- Ethical handling of vulnerabilities: identify → verify → report → remediate.
- Exercise: Found vulnerability → correct steps? Solution: Document, report to client, do not exploit.
- Problem: Company ignores flaw → consequences? Solution: User harm, legal liability, reputational damage.
- Conclusion: Protects users & systems.
- References: ISO/IEC 27034, ACM & IEEE Codes of Ethics

Case Study: Ethical Dilemma

- **Scenario: Employee discovers zero-day vulnerability. Decision: report or delay for gain?**
- **Exercise/Solution: Report immediately → aligns with professional responsibility & ethical codes.**
- **Problem: Identify ethical principles violated if employee delays → Integrity, accountability, user safety.**
- **Conclusion: Practice real-world ethical decision-making.**

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.

Homework

- **1. Essay: Importance of professional responsibility in cybersecurity with examples.**
- **2. Problems: Identify ethical violations in 5 given scenarios (integrity, competence, confidentiality).**
- **Solutions: Provided in handout for self-review.**

Summary & References

- **Professional responsibility = accountability, competence, integrity, confidentiality, privacy, conflict management.**
- **Codes of ethics (ACM, IEEE, ISC²) guide ethical decision-making.**
- **References/Textbooks:**
- **Quinn, Ethics for the Information Age (2023)**
- **Whitman & Mattord, Principles of Information Security, 7th Ed. (2024)**
- **ACM, IEEE, ISC² Codes of Ethics (2024)**
- **Tavani, Ethics and Technology, 6th Ed. (2023)**

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Thank you for your listening