2019-04-15

IT Security #10

Ethical Issues

Theme C (iv) on Management issues

Niels Christian Juul

Informatik
Datalogi
Roskilde Universitet

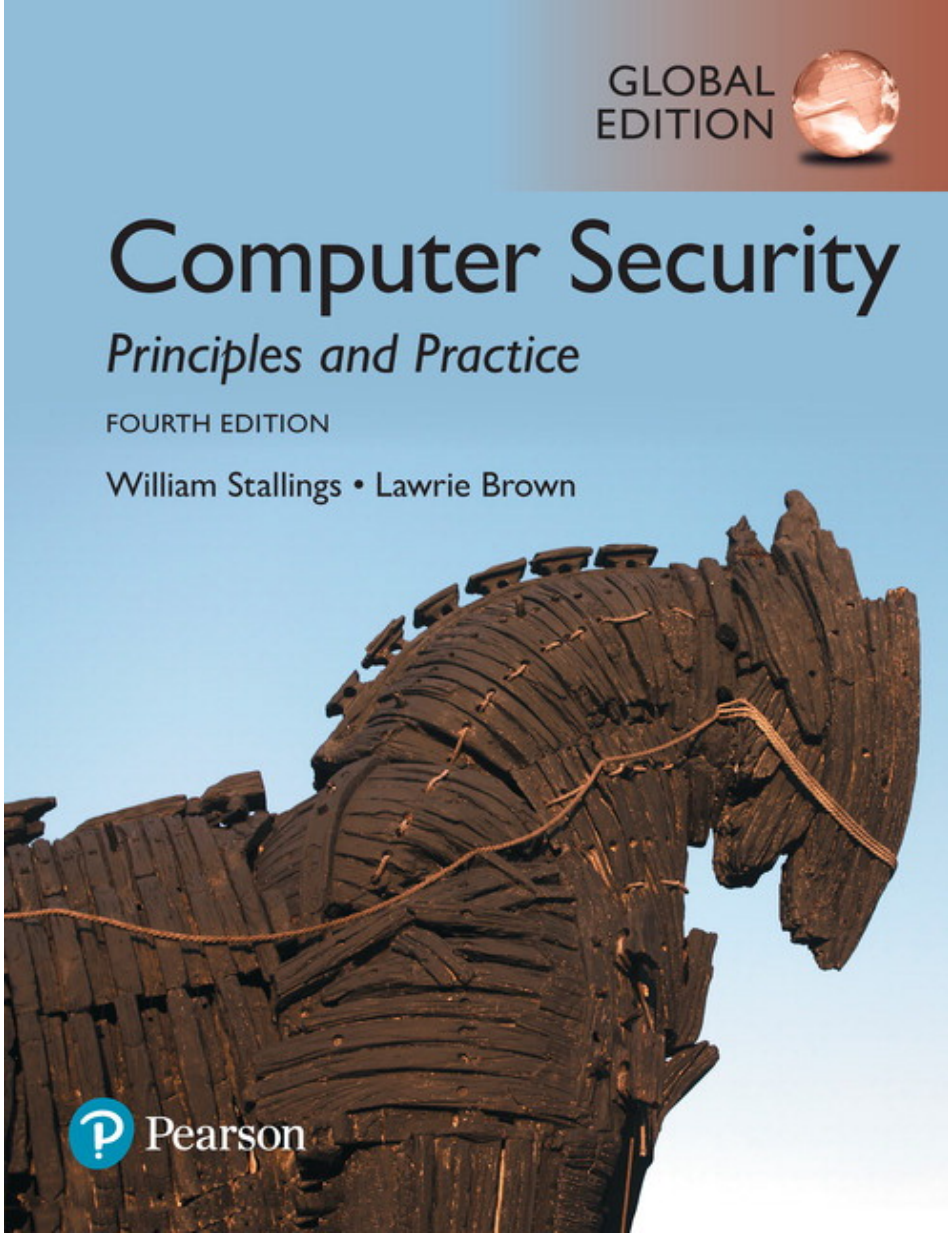
Roskilde Universitet
Niels Christian Juul
Hus 08.2-071
Universitetsvej 1
4000 Roskilde
ncjuul@ruc.dk

IT-security

Course book

- Chapter 19 (19.4)

Today on ethical issues



Learning outcome

Be able to answer:

- What is an ethical code of conduct for IT professionals?
- What are the important elements of such code of conduct?
- What are data ethics?

Exam themes/questions:

- Describe important, current data ethical dilemmas and how an ethical code of conduct can address them?

Ethics Overview

- Ethics is about how we ought to live*
- The purpose of Ethics in Information Security is not just philosophically important, it can mean the survival of a business or an industry**

Ethics is doing the right thing,
even when no one is looking

* Singer, Peter. Ethics. New York: Oxford University Press, 1994.

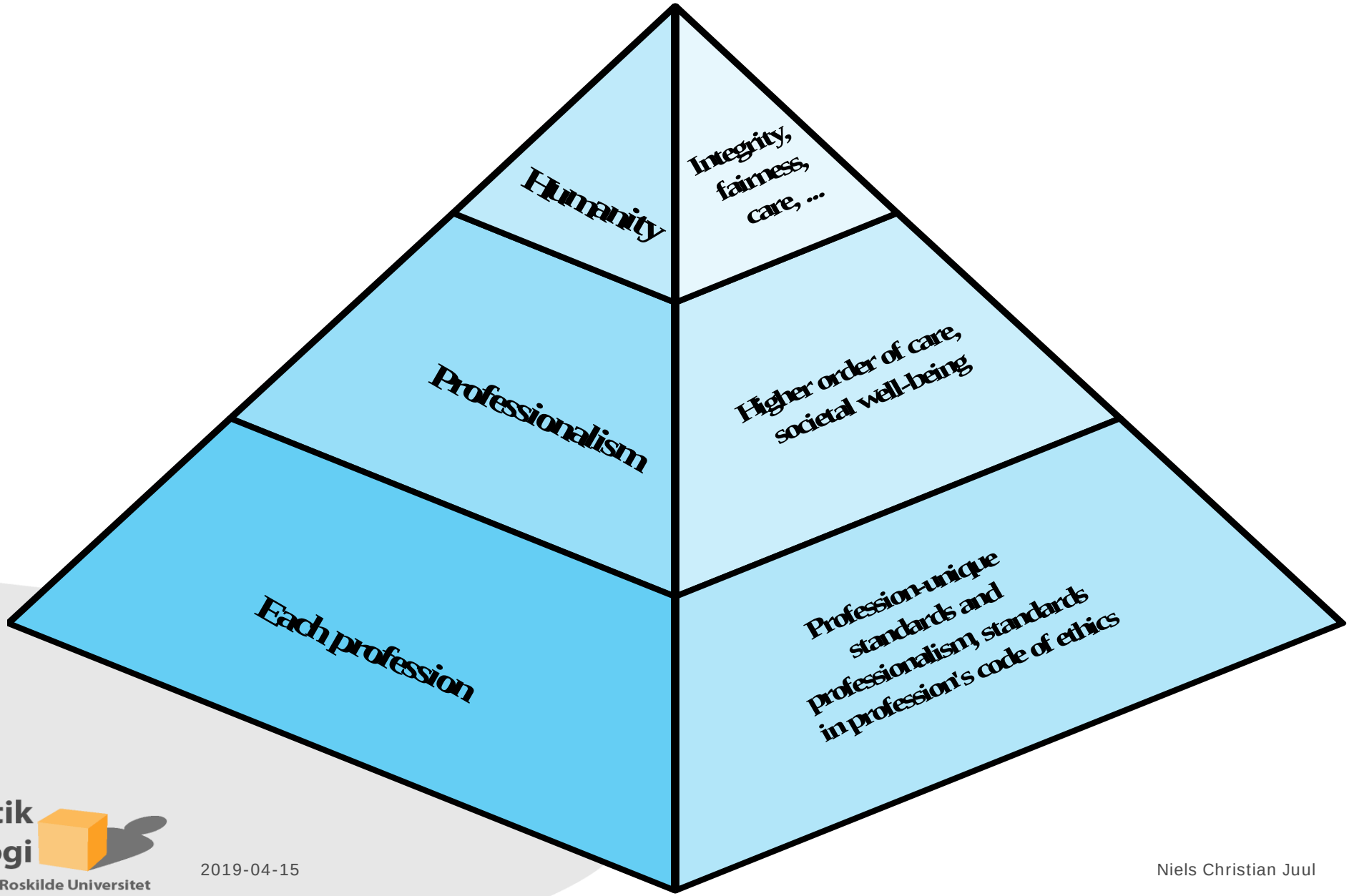
** Northcutt, Stephen. IT Ethics Handbook. Rockland: Syngress, 2004.

Ethics

“A system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions.”

Ethical Issues

- Many potential misuses and abuses of information and electronic communication that create privacy and security problems
- Basic ethical principles developed by civilizations apply
  - Unique considerations surrounding computers and information systems
  - Scale of activities not possible before
  - Creation of new types of entities for which no agreed ethical rules have previously been formed


Humanity
Integrity, fairness, care, ...
Professionalism
Higher order of care, societal well-being
Each profession
Profession-unique standards and professionalism, standards in profession's code of ethics

Class exercise

1. Why do we need an ethical code of conduct?

   Or why not?

Ethical Issues Related to Computers and Information Systems

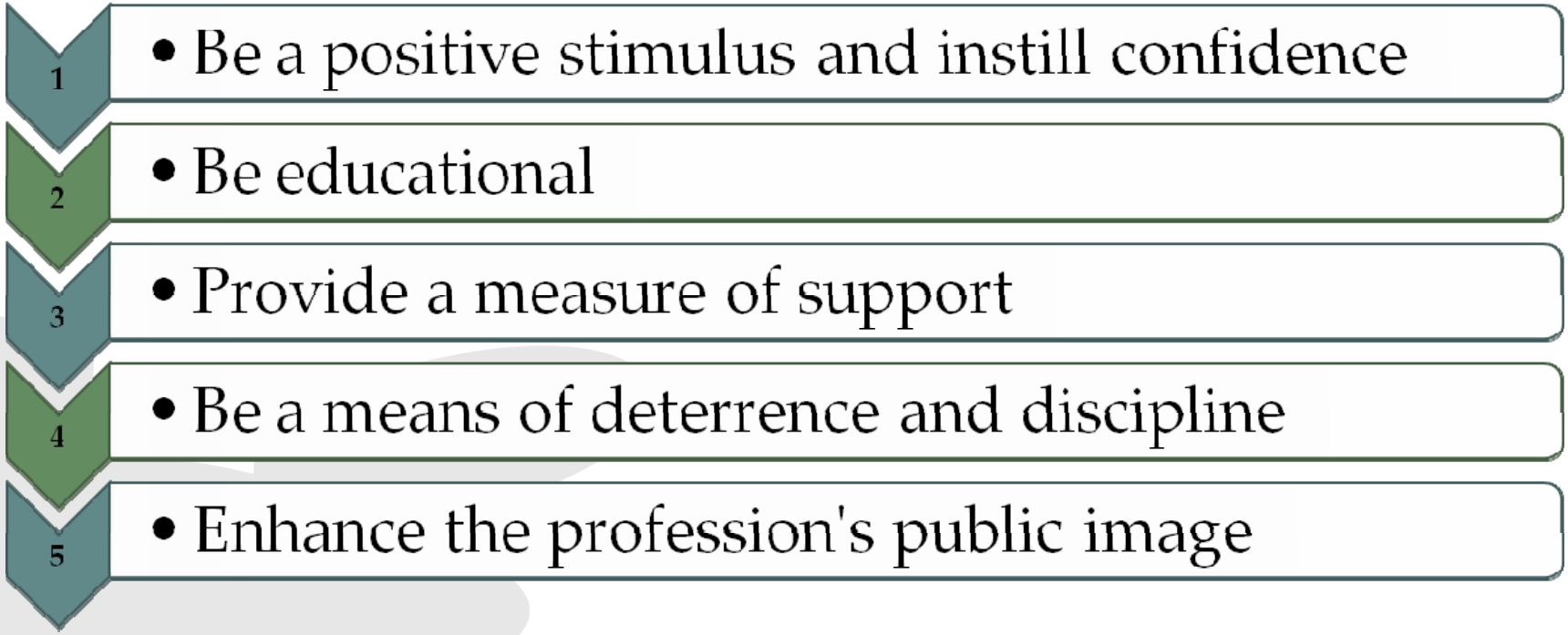
- Some ethical issues from computer use:
  - Repositories and processors of information
  - Producers of new forms and types of assets
  - Instruments of acts
  - Symbols of intimidation and deception
- Those who understand, exploit technology, and have access permission, have power over these

Professional / Ethical Responsibilities

- Concern with balancing professional responsibilities with ethical or moral responsibilities
- Types of ethical areas a computing or IT professional may face:
  - Ethical duty as a professional may come into conflict with loyalty to employer
  - “Blowing the whistle”
  - Expose a situation that can harm the public or a company’s customers
  - Potential conflict of interest
- Organizations have a duty to provide alternative, less extreme opportunities for the employee
  - In-house ombudsperson coupled with a commitment not to penalize employees for exposing problems
- Professional societies should provide a mechanism whereby society members can get advice on how to proceed

Codes of Conduct

- Ethics are not precise laws or sets of facts
- Many areas may present ethical ambiguity
- Many professional societies have adopted ethical codes of conduct which can:



The ACM (Association for Computing Machinery) Code of Ethics and Professional Conduct

1. GENERAL MORAL IMPERATIVES.

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
2.2 Acquire and maintain professional competence.
2.3 Know and respect existing laws pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
2.6 Honor contracts, agreements, and assigned responsibilities.
2.7 Improve public understanding of computing and its consequences.
2.8 Access computing and communication resources only when authorized to do so.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

4. COMPLIANCE WITH THE CODE.

4.1 Uphold and promote the principles of this Code.
4.2 Treat violations of this code as inconsistent with membership in the ACM.

Figure 19.6 ACM Code of Ethics and Professional Conduct

ACM Code of Ethics and Professional Conduct (2018)

1. General Ethical Principles.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

1.2 Avoid harm.

1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

1.7 Honor confidentiality.

ACM Code of Ethics and Professional Conduct (2018)

2. Professional Responsibilities.

2.1 Strive to achieve high quality in both the processes and products of professional work.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.3 Know and respect existing rules pertaining to professional work.

2.4 Accept and provide appropriate professional review.

ACM Code of Ethics and Professional Conduct (2018)

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

2.6 Perform work only in areas of competence.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

2.9 Design and implement systems that are robustly and usably secure.

ACM Code of Ethics and Professional Conduct (2018)

3. Professional Leadership Principles.

3.1 Ensure that the public good is the central concern during all professional computing work.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

3.3 Manage personnel and resources to enhance the quality of working life.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

ACM Code of Ethics and Professional Conduct (2018)

3.5 Create opportunities for members of the organization or group to grow as professionals.

3.6 Use care when modifying or retiring systems.

3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

4. Compliance With The Code.

4.1 Uphold, promote, and respect the principles of the Code.

4.2 Treat violations of the Code as

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics

Figure 19.7 IEEE Code of Ethics

In recognition of my obligation to management I shall:

- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:

- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:

- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:

- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest, and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Figure 19.8 AITP Standard of Conduct

Class exercise

1. What are the common themes in these ethical code of conduct?
   - ACM
   - IEEE
   - AITP

Comparison of Codes of Conduct

- All three codes place their emphasis on the responsibility of professionals to other people
- Do not fully reflect the unique ethical problems related to the development and use of computer and IT technology
- Common themes:
  - Dignity and worth of other people
  - Personal integrity and honesty
  - Responsibility for work
  - Confidentiality of information
  - Public safety, health, and welfare
  - Participation in professional societies to improve standards of the profession
  - The notion that public knowledge and access to technology is equivalent to social power

The Rules

- Collaborative effort to develop a short list of guidelines on the ethics of computer systems
- Ad Hoc Committee on Responsible Computing
  - Anyone can join this committee and suggest changes to the guidelines
  - Moral Responsibility for Computing Artifacts
    - Generally referred to as The Rules
    - The Rules apply to software that is commercial, free, open source, recreational, an academic exercise or a research tool
  - Computing artifact
    - Any artifact that includes an executing computer program

As the book was writing, the rules were as follows:

1. The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system.
2. The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying, or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.
3. People who knowingly use a particular computing artifact are morally responsible for that use.
4. People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.
5. People who design, develop, deploy, promote, or evaluate a computing artifact should not explicitly or implicitly deceive users about the artifact or its foreseeable effects, or about the sociotechnical systems in which the artifact is embedded.

Version 27

Importance of Ethics to Security

- Information Security professionals are entrusted with the crown jewels of an organization.
- Ethical behavior, both on and off-the-job, is the assurance that we are worthy of that trust.
- IS Security sets and upholds a standard
  - Corporate Ethics programs originating from the CSO
  - Promote uniform adherence to policy through example

Ethical Challenges in InfoSec

- Misrepresentation of certifications, skills
- Abuse of privileges
- Inappropriate monitoring
- Withholding information
- Divulging information inappropriately
- Overstating issues
- Conflicts of interest
- Management / employee / client issues

Ethical Challenges – Snake Oil

- “Consultants" who profess to offer information security consulting, but offer profoundly bad advice
- "Educators", both individuals and companies, that offer to teach information security, but provide misinformation (generally through ignorance, not intent)
- "Security Vendors", who oversell the security of their products
- "Analysts", who oversimplify security challenges, and try to upsell additional services to naïve clients
- "Legislators", who push through "from-the-hip" regulations, without thoughtful consideration of their long-term impact

Ten Commandments of Ethics in Information Security

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

Courtesy of the Computer Ethics Institute, A project of the Brookings Institution

Definition of data ethics

DATAETHICS

- Data ethics is about responsible and sustainable use of data. It is about doing the right thing for people and society. Data processes should be designed as sustainable solutions benefitting first and foremost humans.
- Data ethics refer and adhere to the principles and values on which human rights and personal data protection laws are based. It's about honest and genuine transparency in data management. To actively develop privacy-by-design and privacy-enhancing products and infrastructures. To treat someone else's personal information as you wish your own, or your children's, treated.
- Data ethics is the step further than mere compliance with personal data protection laws: All data processing therefore respects as a minimum the requirements set out in the EU's General Data Protection Regulation (GDPR), the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

DATAETHICS

- The human being at the centre
- Individual data control
- Transparency
- Accountability
- Equality

https://dataethics.eu/data-ethics-principles/

Class exercise

1. Which element should an ethical code of conduct for informatics students at RUC address wrt IT Security?
   - Basic elements
   - Dilemmas
2. Which one do you consider most important?
   - Rank them
3. Give two examples on how to spell out the code of conduct for an important issue

Summary

- Ethical issues
  - Ethics and the IT professions
  - Ethical issues related to computers and information systems
  - Codes of conduct
  - The rules
- Data Ethics

Learning outcome

Be able to answer:

- What is an ethical code of conduct for IT professionals?
- What are the important elements of such code of conduct?
- What are data ethics?

Exam themes/questions:

- Describe important, current data ethical dilemmas and how an ethical code of conduct can address them?