Chapter 3. Legal, Ethical, and Professional Issues in Information Security

⊙ Introduction

- To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new issues as they emerge.
- By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, security professionals can help keep an organization focused on its primary objectives.

⊙ Organizational Liability

- Even if there is no breach of criminal law, there can still be "liability" - legal responsibility. Liability includes the legal obligation to make restitution for wrongs comitted.
- "Due care" means measures that an organization takes to ensure every employee knows what is acceptable (i.e. legal and ethical) and what is not.

  (Note) If due care ↓ then liability ↑
- "Due diligence" requires that organization make a valid effort to continually maintain this level of effort.

⊙ Policy v.s. Law

- Within an organization, information security professionals help maintain security via the establishment and enforcement of policies.

  describe acceptable and unacceptable employee behaviors in the workplace.

- Policies function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance.
- The difference between a policy and a law is that ignorance of a policy is an acceptable defense.
- For a policy to become enforceable, it must meet the following criteria:

The organization must be able to demonstrate that

① Dissemination (distribution) – the relevant policy has been made readily available for review by the employee.
(tech.) hard copy, electronic distribution

② Review (reading) – the organization disseminated the document in an intelligible form.
(tech.) recordings of policy in English and alternate languages

③ Comprehension (understanding) – the employee understood the requirements and content of the policy.
(tech.) quizzes and other assignments

④ Compliance (agreement) – the employee agrees to comply with the policy, through act or affirmation.
(tech.) logon banners or a signed document

⑤ Uniform enforcement – the policy has been uniformly enforced, regardless of employee status or assignment.

⑥ Law and Ethics

- "Laws" are rules that mandate or prohibit certain behavior in society.
- It is impossible or impractical to develop laws to describe and enforce all forms of behavior acceptable to society.
- Instead, society relies on "ethics" or "morals" to prescribe generally accepted standards of proper behavior.
- "Ethics" are objectively defined standards of right and wrong.
- "Laws" are drawn from "ethics".

- "Laws" carry the sanctions of a governing authority and "ethics" do not.
- Law vs Ethics

Law	Ethics
◦ Described by formal, written documents	◦ Described by unwritten principles
◦ Interpreted by courts	◦ Interpreted by individual
◦ Established by legislatures representing all people	◦ Presented by philosophers, religions, and professional groups
◦ Applicable to everyone	◦ Personal choice
◦ Priority determined by courts if two laws conflict	◦ Priority determined by an individual if two principles conflict
◦ Court is final arbiter of "right"	◦ No external arbiter
◦ Enforceable by police and courts	◦ Limited enforcement

⊙ Codes of Ethics and Professional Organizations

- A number of professional organizations have established "codes of conduct" or "codes of ethics" that members are expected to follow.
- It is the responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.
- It is likewise the organization's responsibility to develop, disseminate, and enforce its policies.

IEEE

IEEE CODE OF ETHICS

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.

Approved by the IEEE Board of Directors | February 2006

Code of Ethics

I acknowledge

That I have an obligation to management, therefore, I shall promote the understanding of information processing methods and procedures to management using every resource at my command.

That I have an obligation to my fellow members, therefore, I shall uphold the high ideals of AITP as outlined in its Association Bylaws. Further, I shall cooperate with my fellow members and shall treat them with honesty and respect at all times.

That I have an obligation to society and will participate to the best of my ability in the dissemination of knowledge pertaining to the general development and understanding of information processing. Further, I shall not use knowledge of a confidential nature to further my personal interest, nor shall I violate the privacy and confidentiality of information entrusted to my or to which I may gain access.

That I have an obligation to my employer whose trust I hold, therefore, I shall endeavor to discharge this obligation to the best of my ability, to guard my employer's interests, and to advise him or her wisely and honestly.

That I have an obligation to my college or university, therefore, I shall uphold its ethical and moral principles.

That I have an obligation to my country, therefore, in my personal, business, and social contacts, I shall uphold my nation and shall honor the chosen way of life of my fellow citizens.

I accept these obligations as a personal responsibility and as a member of this Association, I shall actively discharge these obligations and I dedicate myself to that end.

Standards of Conduct

These standards expand on the Code of Ethics by providing specific statements of behavior in support of each element of the code. They are not objectives to be strived for, they are rules that no true professional will violate. It is first of all expected that an information processing professional will abide by the appropriate laws of their country and community. The following standards address tenets that apply to the profession.

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 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 acknowledgment 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 to 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 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.

See the following site for ACM Code of Ethics
http://www.acm.org/about/code-of-ethics

aitp Association of Information Technology Professionals