Professional Codes of Ethics

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group. Most codes of ethics created by professional organizations have two main parts: The first outlines what the organization aspires to become, and the second typically lists rules and principles by which members of the organization are expected to abide.

While laws do not fully define ethical behavior, a code of ethics benefits individuals, professions, and society by promoting:

- **Ethical Decision Making**: Practitioners use a common set of core values and beliefs as a guideline for consistent ethical choices.
- **High Standards of practice and ethical behaviour**: Adherence to a code of ethics helps professionals remain aware of their responsibilities and duties, even when faced with the pressures of daily business. The code sets clear standards for acceptable and unacceptable behavior, guiding interactions with others. Strong codes may include disciplinary measures for serious violations, potentially resulting in the loss of the right to practice. However, such comprehensive codes are rare, particularly in the IT field.
- **Trust and respect from the general public**: —Public trust is built on the expectation that a professional will behave ethically. People must often depend on the integrity and good judgment of a professional to tell the truth, abstain from giving self-serving advice, and offer warnings about the potential negative side effects of their actions. Thus, adherence to a code of ethics enhances trust and respect for professionals and their profession.
- **Evaluation Benchmark**:A code of ethics provides an evaluation benchmark that a professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

IT PROFESSIONALS

A profession is a calling that requires specialized knowledge and often long and intensive academic preparation.

employee. The United States Code of federal regulations defines a "professional employee" as one who is engaged in the performance of work:

> "(i) requiring knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study in an institution of higher learning or a hospital (as distinguished from knowledge acquired by a general academic education, or from an apprenticeship, or from training in the performance of routine mental, manual, mechanical, or physical activities);
> (ii) requiring the consistent exercise of discretion and judgment in its performance;
> (iii) which is predominantly intellectual and varied in character (as distinguished from routine mental, manual, mechanical, or physical work); and
> (iv) which is of such character that the output produced or the result accomplished by such work cannot be standardized in relation to a given period of time."[11]

In other words, professionals such as doctors, lawyers, and accountants require advanced training and experience; they must exercise discretion and judgment in the course of their work; and their work cannot be standardized. Many people would also expect professionals to contribute to society, to participate in a lifelong training program (both formal and informal), to keep abreast of developments in their field, and to assist other professionals in their development. In addition, many professional roles carry special rights and responsibilities. Doctors, for example, prescribe drugs, perform surgery, and request confidential patient information while maintaining doctor–patient confidentiality.

U.S. regulations further specify that a professional's work must demand advanced knowledge, involve discretion and judgment, be predominantly intellectual, and resist standardization within fixed time frames. Examples include doctors, lawyers, and accountants.

These professionals not only require specialized training and experience but are also expected to contribute to society, pursue lifelong learning, and support the growth of others in their field.

Are IT Workers Professionals?

Many business workers have duties, backgrounds, and training that qualify them to be classified as professionals, including marketing analysts, financial consultants, and IT specialists such as mobile application developers, software engineers, systems analysts, and network administrators. One could argue, however, that not every IT role requires "knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study," to quote again from the United States Code. From a *legal* perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government. This distinction is important, for example, in malpractice lawsuits, as many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.

Professional Relationships That Must Be Managed

IT workers typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large—as illustrated in Figure 2-1. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections.

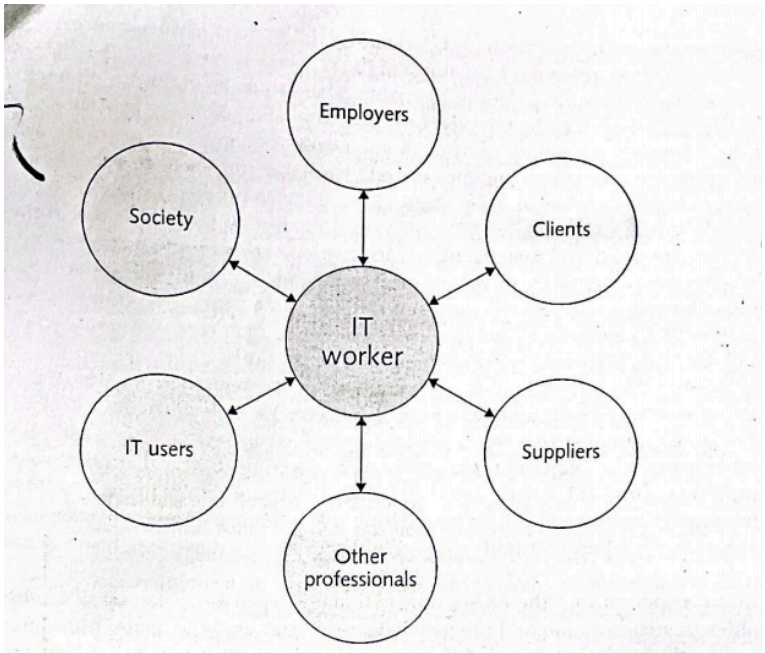


FIGURE 2-1 Professional relationships IT workers must manage
Credit: Course Technology/Cengage Learning.

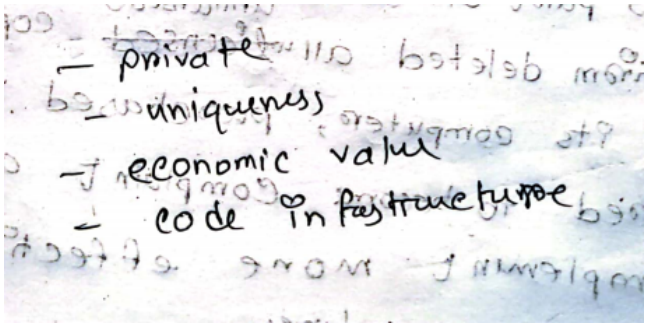
Relationship between IT workers and Employers

An IT worker and an employer typically agree on fundamental aspects of this relationship before the worker accepts an employment offer. These issues may include job title, general performance expectations, specific work responsibilities, drug-testing requirements, dress code, location of employment, salary, work hours, and company benefits. . IT workers often have the skills and knowledge to abuse systems and data or to enable others to do so. Software piracy is an area in which IT workers may be tempted to violate laws and policies. Although end users often get the blame when it comes to using illegal copies of commercial software, software piracy in a corporate setting is sometimes directly traceable to IT staff members.

The Business Software Alliance (BSA) is a trade group that represents the world's largest software and hardware manufacturers. Its mission is to stop the unauthorized copying of software produced by its members. BSA investigations are usually triggered by calls to the BSA hotline.

In 2012, the Alexander Automotive Group paid $325,000 to settle claims that it was using unlicensed Microsoft software on its computers. As part of the settlement agreement with BSA, the firm deleted all unlicensed copies of software from its computers, purchased the licenses required to become compliant, and agreed to implement more effective software management procedures.

A **trade secret** is information, generally unknown to the public, that a company has taken strong measures to keep confidential. It represents something of economic value that has required effort or cost to develop and that has some degree of uniqueness or novelty. Trade secrets can include the design of new software code, hardware designs, business plans, the design of a user interface to a computer program, and manufacturing processes.



Another issue that can create friction between employers and IT workers is **whistleblowing.** Whistle-blowing is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. Whistle-blowers often have special information based on their expertise or position within the offending organization. For example, an employee of a chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public. A conscientious employee would call the problem to management's attention and try to correct it by working with appropriate resources within the company. But what if the employee's attempt to correct the problem through internal channels was thwarted or ignored? The employee might then consider becoming a whistleblower and reporting the problem to people outside the company, including state or federal agencies that have jurisdiction. Obviously, such actions could have negative consequences on the employee's job, perhaps resulting in retaliation and firing.

Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same organization as the IT worker. In other cases, the client is part of a different organization. In relationships between IT workers and clients, each party agrees to provide something of value to the other. Generally speaking, the IT worker provides hardware, software, or services at a certain cost and within a given time frame.

This relationship is usually documented in contractual terms— who does what, when

the work begins, how long it will take, how much the client pays, and so on.

a conflict of interest—a conflict between the IT worker's (or the IT firm's) self interest and the interests of the client. For example, an IT consulting firm might be hired to assess a firm's IT strategic plan. After a few weeks of analysis, the consulting firm might provide a poor rating for the existing strategy and insist that its proprietary products and services are required to develop a new strategic plan. Such findings would raise questions about the vendor's objectivity and whether its recommendations can be trusted.

Fraud is the crime of obtaining goods, services, or property through deception or trickery. Fraudulent misrepresentation occurs when a person consciously decides to induce another person to rely and act on a misrepresentation. To prove fraud in a court of law, prosecutors must demonstrate the following elements:

• The wrongdoer made a false representation of material fact.

• The wrongdoer intended to deceive the innocent party.

• The innocent party justifiably relied on the misrepresentation.

• The innocent party was injured.

Misrepresentation is the misstatement or incomplete statement of a material fact. If the misrepresentation causes the other party to enter into a contract, that party may have the legal right to cancel the contract or seek reimbursement for damages.

Breach of contract occurs when one party fails to meet the terms of a contract. Further, a material breach of contract occurs when a party fails to perform certain express or implied obligations, which impairs or destroys the essence of the contract.

Relationships Between IT Workers and Suppliers

IT workers deal with many different hardware, software, and service providers. Most IT workers understand that building a good working relationship with suppliers encourages the flow of useful communication as well as the sharing of ideas. Such information can lead to innovative and cost-effective ways of using the supplier's products and services that the IT worker may never have considered.

Suppliers strive to maintain positive relationships with their customers in order to make and increase sales. To achieve this goal, they may sometimes engage in unethical actions—for example, offering an IT worker a gift that is actually intended as a bribe.Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.

Relationships Between IT Workers and Other Professionals

Professionals often feel a degree of loyalty to the other members of their profession. As a result, they are often quick to help each other obtain new positions but slow to criticize each other in public. Professionals also have an interest in their profession as a whole, because how it is perceived affects how individual members are viewed and treated. (For example, politicians are not generally thought to be very trustworthy, but teachers are.) Hence, professionals owe each other an adherence to the profession's code of conduct. Experienced professionals can also serve as mentors and help develop new members of the profession. A number of ethical problems can arise among members of the IT profession. One of the most common is résumé inflation, which involves lying on a résumé by, for example, claiming competence in an IT skill that is in high demand.

Relationships Between IT Workers and IT Users

The term IT user refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity. IT workers have a duty to understand a user's needs and capabilities and to deliver products and services that best meet those needs—subject, of course, to

budget and time constraints. **IT workers also have a key responsibility to establish an environment that supports ethical behavior by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information**.

Relationships Between IT Workers and Society

Regulatory laws establish safety standards for products and services to protect the public. However, these laws are less than perfect, and they cannot safeguard against all negative side effects of a product or process. Often, professionals can clearly see the effect their work will have and can take action to eliminate potential public risks. Thus, society expects members of a profession to provide significant benefits and to not cause harm through their actions. One approach to meeting this expectation is to establish and maintain professional standards that protect the public.

Clearly, the actions of an IT worker can affect society. For example, a systems analyst may design a computer-based control system to monitor a chemical manufacturing process. A failure or an error in the system may put workers or residents near the plant at risk. As a result, IT workers have a relationship with members of society who may be affected by their actions.

Professional Organizations

The text outlines key IT professional organizations and their contributions to the field. These organizations promote networking, skill development, and ethical standards for IT professionals. Here's a summary of the organizations discussed:

1. **Association for Computing Machinery (ACM)**

    - Founded in 1947, with over 97,000 members globally.
    - Publishes journals, newsletters (e.g., *Communications of the ACM , ACM Tech News (coverage of timely topics for IT professionals), XRDS (for both*

graduate and undergraduate students considering computing careers), RISKS Forum (a moderated dialogue on risks to the public from computers and related systems), and eLearn (an online magazine about online education and training)), and hosts special-interest groups (SIGs) representing major areas of computing.

- Offers a vast digital library of bibliographic information, citations, articles, and journals and facilitates workshops, conferences, and discussions on risks and trends.

2. **Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)**

    - Covers the broad fields of electrical, electronic, and information technologies and sciences.
    - Founded in 1946, with 85,000 members, it is the largest IEEE society.
    - Provides technical journals, conferences, online courses, and certifications like **CSDP** (Certified Software Development Professional) and **CSDA**(Certificate Software Development Associate) to help meet the information and career development needs of computing researchers and practitioners.
    - Collaborated with ACM to establish the *Software Engineering Code of Ethics* in 1999.

3. **Association of Information Technology Professionals (AITP)**

    - Originated in 1951, evolving to its current form in 1996.
    - Focuses on leadership, education, and marketability in IT.
    - Hosts seminars, conferences, and networking opportunities, and maintains a code of ethics and standards.

4. **SysAdmin, Audit, Network, Security (SANS) Institute**

    - Provides cybersecurity training and certifications to a global audience.

- Publishes security news, research documents, and operates the Internet Storm Center for monitoring threats.

These organizations support professional growth, provide resources, and set ethical standards for IT workers worldwide.

Common Ethical Issues for IT Users

Software Piracy: Software piracy in a corporate setting can sometimes be directly traceable to IT professionals—they might allow it to happen, or they might actively engage in it. Corporate IT usage policies and management should encourage users to report instances of piracy and to challenge its practice. Employees may engage in piracy, such as copying work software for home use or downloading pirated Android apps. Such practices discourage legitimate developers and harm businesses.

Inappropriate Use of Computing Resources: Workers may misuse IT resources by browsing irrelevant websites, playing games, or viewing pornography, which reduces productivity and can lead to legal issues. Accessing porn sites also poses cybersecurity risks due to potential malware. Furthermore, activities such as viewing sexually explicit material, sharing offensive jokes, and sending hate emails could lead to lawsuits and allegations. Studies show a significant percentage of workers admit to viewing pornography at work, even on mobile devices.

Inappropriate Sharing of Information: Organizations store vast amounts of private (employee and customer data) and confidential (company operational data) information. IT users who share this information with unauthorized parties, even unintentionally, violate privacy and risk giving sensitive information to competitors. Sharing payroll information with a friend is a clear privacy violation.

Organizations must enforce strict policies to promote ethical IT use and safeguard sensitive data.

Supporting the Ethical Practices of IT Users

Organizations must establish IT usage policies to address ethical concerns and prevent misuse of IT resources. These policies outline user rights, responsibilities, and acceptable behaviors, helping improve productivity, reduce costs, and enhance IT services. Key actions include:

1. **Establishing Guidelines for Use of Company Software**: Companies should provide employees with clear rules for legal software use, especially for home work setups, and may offer software or discounts for work-related needs.
2. **Defining the Appropriate Use of IT Resources**: Companies need written guidelines that encourage responsible use of IT resources for job enhancement. These guidelines should allow some personal use while prohibiting activities like visiting objectionable websites or sending offensive messages via company email. Clear communication and enforcement of these guidelines are essential.
3. **Structuring Information Systems to Protect Data and Information**: Organizations should implement access controls, ensuring employees can only view the data relevant to their roles, protecting sensitive information like R&D results and staffing projections.
4. **Installing and Maintaining a Corporate Firewall**: Firewalls act as barriers to unauthorized internet activity, blocking objectionable websites and risky email attachments, and reducing the threat of malware and viruses.

By following these measures, organizations can foster ethical IT practices and safeguard corporate resources.

Government Licensing in General:

A government license is official permission to engage in a specific activity or operate a business. It's typically managed at the state level and often requires passing a test.

Many professions require licenses, including CPAs, lawyers, doctors, and some engineers. States enforce licensing laws to protect public safety.

The Case for Licensing IT Workers:

Modern information systems are complex, interconnected, and crucially dependent on each other. They manage everything from large-scale business functions (Enterprise Resource Planning)(ERPs) to critical infrastructure like nuclear power plants and medical life support systems. Government systems also rely heavily on IT. As a result of the increasing importance of IT in our everyday lives, the development of reliable, effective information systems has become an area of mounting public concern. This concern has led to a debate about whether the licensing of IT workers would improve information systems. Proponents argue that licensing would strongly encourage IT workers to follow the highest standards of the profession and practice a code of ethics

Issues with Licensing IT Workers:

While some countries and regions have licensing for software engineers, IT worker licensing in the U.S. faces several challenges:

- **No Universal Body of Knowledge:** There's no universally agreed-upon set of skills and abilities that all IT professionals must possess. Various organizations have their own standards, but there's no single, accepted standard.
- **Unclear Management of Licensing Exams:** Questions arise about how exams would be created, administered, and managed. Reciprocity between states and countries is also an issue. The rapid pace of technological change necessitates continuous education, raising questions about license renewal requirements and demonstrating competency in new practices.
- **No Accrediting Body for IT Education:** Unlike other professions, there's no single body accrediting IT education programs. There's also no standard training process or agreement on the essential skills for IT workers, even for specific roles like programming.

- **No Body to Assess Competence:** There's no established body to assess and ensure the competence of individual IT workers. While some professional organizations like AITP have codes of ethics, enforcement and censure are rare. Accountability mechanisms like those in other licensed professions are lacking.

IT Professional Malpractice

Negligence has been defined as not doing something that a reasonable person would do, or doing something that a reasonable person would not do. Duty of care refers to the obligation to protect people against any unreasonable harm or risk. For example, people have a duty to keep their pets from attacking others and to operate their cars safely. Similarly, businesses must keep dangerous pollutants out of the air and water, make safe products, and maintain safe operating conditions for employees.

The courts decide whether parties owe a duty of care by **applying a reasonable person standard** to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances.

Breach of Duty and Malpractice:

A breach of duty is a failure to act as a reasonable person would act. This can be an action (e.g., throwing a lit cigarette in a fireworks factory) or inaction (e.g., a police officer failing to protect someone). Professionals who breach their duty of care are liable for resulting injuries. This is called professional malpractice. For example, a CPA who fails to use reasonable care when auditing books is liable for accounting malpractice. Professionals are liable to their clients/patients and sometimes to third parties.

IT Professional Malpractice:

Courts have generally rejected attempts to sue individuals for IT-related malpractice. Professional negligence requires established professional standards. Because software engineering is not uniformly licensed in the U.S., there are no consistent standards to compare a software engineer's actions against. Therefore, they cannot be readily subjected to malpractice lawsuits in the same way as licensed professionals.

What is Certification?

Certification confirms that a professional possesses specific skills, knowledge, or abilities, as judged by the certifying organization. Unlike licensing, it's generally voluntary and can apply to products as well as people. IT certifications may or may not include adherence to a code of ethics, unlike licensing which almost always does.

Value of Certifications:

Opinions on the value of certifications vary. Many employers see them as a benchmark of basic knowledge, but some hiring managers are skeptical, as certification doesn't replace experience or guarantee on-the-job performance. For IT professionals, certifications can be a structured way to learn new skills, gain recognition, and advance their careers. Others view certifications as a revenue source for vendors with limited actual value.

Choosing a Certification:

Deciding on the right certification depends on career goals, existing skills, and training availability. Consider relevance to current/desired jobs, the certifying organization's reputation, and current/future demand for those skills.

Vendor Certifications:

IT vendors (Cisco, IBM, Microsoft, etc.) offer certifications for their products. These can improve salary and career prospects, particularly for roles with specific technical requirements. However, vendor certifications can be too narrowly focused on the vendor's technology and may lack broader conceptual coverage. Certification typically involves passing a written, usually multiple-choice, exam. Some, like the Cisco CCIE, require hands-on lab exams. Gaining the necessary experience for some certifications can take years, and training materials/courses can be expensive.

Industry Association Certifications:

Many industry associations offer certifications in various IT areas. Their value varies based on career stage, other certifications held, and the job market. Certification typically requires prerequisites (education and experience), passing an exam, paying annual fees, earning continuing education credits, and sometimes passing periodic renewal tests. Industry association certifications generally require more experience and a broader perspective than vendor certifications. However, they may lag in developing tests for new technologies. The trend

is to incorporate not just technical skills, but also business and behavioral competencies into IT certifications.