

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. There is currently no single, formal organization of IT workers that takes responsibility for establishing and maintaining standards that protect the public. However, as discussed in the following sections, there are a number of professional organizations that provide useful professional codes of ethics to guide actions that support the ethical behavior of IT workers.

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. Practitioners in many professions subscribe to a code of ethics that governs their behavior. For example, doctors adhere to varying versions of the 2,000-year-old Hippocratic oath, which medical schools offer as an affirmation to their graduating classes. 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. Many codes also include a commitment to continuing education for those who practice the profession.

Laws do not provide a complete guide to ethical behavior. Just because an activity is not defined as illegal does not mean it is ethical. Nor can a professional code of ethics be expected to provide an answer to every ethical dilemma—no code can be a definitive collection of behavioral standards. However, following a professional code of ethics can produce many benefits for the individual, the profession, and society as a whole:

- *Ethical decision making*—Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs as a guideline for ethical decision making.
- *High standards of practice and ethical behavior*—Adherence to a code of ethics reminds professionals of the responsibilities and duties that they may be tempted to compromise to meet the pressures of day-to-day business. The code also defines acceptable and unacceptable behaviors to guide professionals in their interactions with others. Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice. Such codes are the exception, however, and few exist in the IT arena.
- *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.

Professional Organizations

No one IT professional organization has emerged as preeminent, so there is no universal code of ethics for IT workers. However, the existence of such organizations is useful in a field that is rapidly growing and changing. In order to stay on top of the many new developments in their field, IT workers need to network with others, seek out new ideas, and continually build on their personal skills and expertise. Whether you are a freelance programmer or the CIO of a *Fortune* 500 company, membership in an organization of IT workers enables you to associate with others of similar work experience, develop working relationships, and exchange ideas. These organizations disseminate information through email, periodicals, Web sites, meetings, and conferences. Furthermore, in recognition of the need for professional standards of competency and conduct, many of these organizations have developed codes of ethics. Four of the most prominent IT-related professional organizations are highlighted in the following sections.

Association for Computing Machinery (ACM)

The Association for Computing Machinery (ACM) is a computing society founded in 1947 with over 97,000 student and professional members in more than 100 countries. It is international in scope—with an ACM Europe, ACM India, and ACM China organization. ACM currently publishes over 50 journals and magazines and 30 newsletters—including *Communications of the ACM* (ACM's primary publication), *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). The organization also offers a substantial digital library of bibliographic information, citations, articles, and journals. The ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.³⁰

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

The Institute of Electrical and Electronics Engineers (IEEE) covers the broad fields of electrical, electronic, and information technologies and sciences. The IEEE-CS is one of the oldest and largest IT professional associations, with about 85,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The IEEE-CS helps meet the information and career development needs of computing researchers and practitioners with technical journals, magazines, books, conferences, conference publications, and online courses. It also offers a Certified Software Development Professional (CSDP) program for experienced professionals and a Certified Software Development Associate (CSDA) credential for recent college graduates. The society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.³¹

In 1993, the ACM and IEEE-CS formed a Joint Steering Committee for the Establishment of Software Engineering as a Profession. The initial recommendations of the committee were to define ethical standards, to define the required body of knowledge and recommended practices in software engineering, and to define appropriate curricula to acquire knowledge. The "Software Engineering Code of Ethics and Professional Practice"

documents the ethical and professional responsibilities and obligations of software engineers. After a thorough review process, version 5.2 of the Software Engineering Code of Ethics was adopted by both the ACM and IEEE-CS in 1999.³²

✓ Association of Information Technology Professionals (AITP)

The Association of Information Technology Professionals (AITP) started in Chicago in 1951, when a group of machine accountants got together and decided that the future was bright for the IBM punched-card tabulating machines they were operating—a precursor of the modern electronic computer. They were members of a local group called the Machine Accountants Association (MAA), which first evolved into the Data Processing Management Association in 1962 and finally the AITP in 1996.³³

The AITP provides IT-related seminars and conferences, information on IT issues, and forums for networking with other IT workers. Its mission is to provide superior leadership and education in information technology, and one of its goals is to help members make themselves more marketable within their industry. The AITP also has a code of ethics and standards of conduct. The standards of conduct are considered to be rules that no true IT professional should violate.

✓ SysAdmin, Audit, Network, Security (SANS) Institute

The SysAdmin, Audit, Network, Security (SANS) Institute provides information security training and certification for a wide range of individuals, such as auditors, network administrators, and security managers. Each year, its programs train some 12,000 people, and a total of more than 165,000 security professionals around the world have taken one or more of its courses. SANS publishes a semiweekly news digest (NewsBites), a weekly security vulnerability digest (@Risk), and flash security alerts.³⁴

At no cost, SANS makes available a collection of some 1,200 research documents about various topics of information security. SANS also operates Internet Storm Center—a program that monitors malicious Internet activity and provides a free early warning service to Internet users—and works with Internet service providers to thwart malicious attackers.

Table 2-3 provides the URL for the codes of ethics for the above IT professional organizations.

TABLE 2-3 Code of ethics for popular IT professional organizations

Organization	URL for code of ethics
Association for Computing Machinery	www.acm.org/about/code-of-ethics
Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)	http://seeri.etsu.edu/Codes/TheSECode.htm
Association of Information Technology Professionals (AITP)	www.aitm.org/?page=Ethics
SysAdmin, Audit, Network, Security (SANS) Institute	www.sans.org/security-resources/ethics.php

Source Line: Course Technology/Cengage Learning.

Certification

Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Unlike licensing, which applies only to people and is required by law, certification can also apply to products (e.g., the Wi-Fi CERTIFIED logo assures that the product has met rigorous interoperability testing to ensure that it will work with other Wi-Fi-certified products) and is generally voluntary. IT-related certifications may or may not include a requirement to adhere to a code of ethics, whereas such a requirement is standard with licensing.

57

Numerous companies and professional organizations offer certifications, and opinions are divided on their value. Many employers view them as a benchmark that indicates mastery of a defined set of basic knowledge. On the other hand, because certification is no substitute for experience and doesn't guarantee that a person will perform well on the job, some hiring managers are rather cynical about the value of certifications. Most IT employees are motivated to learn new skills, and certification provides a structured way of doing so. For such people, completing a certification provides clear recognition and correlates with a plan to help them continue to grow and advance in their careers. Others view certification as just another means for product vendors to generate additional revenue with little merit attached.

Deciding on the best IT certification—and even whether to seek a certification—depends on the individual's career aspirations, existing skill level, and accessibility to training. Is certification relevant to your current job or the one to which you aspire? Does the company offering the certification have a good reputation? What is the current and potential future demand for skills in this area of certification?

Vendor Certifications

Many IT vendors—such as Cisco, IBM, Microsoft, SAP, and Oracle—offer certification programs for those who use their products. Workers who successfully complete a program can represent themselves as certified users of a manufacturer's product. Depending on the job market and the demand for skilled workers, some certifications might substantially improve an IT worker's salary and career prospects. Certifications that are tied to a vendor's product are relevant for job roles with very specific requirements or certain aspects of broader roles. Sometimes, however, vendor certifications are too narrowly focused on the technical details of the vendor's technology and do not address more general concepts.

To become certified, one must pass a written exam. Because of legal concerns about whether other types of exams can be graded objectively, most exams are presented in a multiple-choice format. A few certifications, such as the Cisco Certified Internetwork Expert (CCIE) certification, also require a hands-on lab exam that demonstrates skills and knowledge. It can take years to obtain the necessary experience required for some certifications. Courses and training material are available to help speed up the preparation process, but such support can be expensive. Depending on the certification, study materials can cost \$1,000 or more, and in-class formal training courses often cost more than \$10,000.

Ethics for IT Workers and IT Users

✓ Industry Association Certifications

There are many available industry certifications in a variety of IT-related subject areas. Their value varies greatly depending on where people are in their career path, what other certifications they possess, and the nature of the IT job market. Table 2-4 lists several of the certifications most in demand by employers.

TABLE 2-4 Certifications in high demand

Certification	Subject matter
Microsoft Certified Technology Specialist	Designing and optimizing solutions based on Microsoft products and technologies
Cisco Certified Internetwork Expert	Managing and troubleshooting large networks
Cisco Certified Network Professional Security	Configuring and designing firewalls and the security settings on routers and switches
CompTIA A+	Performing computer and network maintenance, troubleshooting, and installation—including addressing security issues
Project Management Institute's Project Management Professional (PMP)	Leading and directing projects

Source Line: Course Technology/Cengage Learning.

Certification requirements generally oblige an individual to have the prerequisite education and experience, and to sit for and pass an exam. In order to remain certified, the individual must typically pay an annual certification fee, earn continuing education credits, and—in some cases—pass a periodic renewal test.

Certifications from industry associations generally require a higher level of experience and a broader perspective than vendor certifications; however, industry associations often lag in developing tests that cover new technologies. The trend in IT certification is to move from purely technical content to a broader mix of technical, business, and behavioral competencies, which are required in today's demanding IT roles. This trend is evident in industry association certifications that address broader roles, such as project management and network security.

✓ Government Licensing

In the United States, a government license is government-issued permission to engage in an activity or to operate a business. It is generally administered at the state level and often requires that the recipient pass a test of some kind. Some professionals must be licensed, including certified public accountants (CPAs), lawyers, doctors, various types of medical and daycare providers, and some engineers.

States have enacted legislation to establish licensing requirements and protect public safety in a variety of fields. For example, Texas passed the Engineering Registration Act after a tragic school explosion at New London, Texas, in 1937. Under the act and

subsequent revisions, only duly licensed people may legally perform engineering services for the public, and public works must be designed and constructed under the direct supervision of a licensed professional engineer. People cannot call themselves engineers or professional engineers unless they are licensed, and violators are subject to legal penalties. Most states have similar laws.

The Case for Licensing IT Workers

The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on one another. Highly integrated enterprise resource planning (ERP) systems help multibillion-dollar companies control all of their business functions, including forecasting, production planning, purchasing, inventory control, manufacturing, and distribution. Complex computers and information systems manage and control the nuclear reactors of power plants that generate electricity. Medical information systems monitor the vital statistics of hospital patients on critical life support. Every year, local, state, and federal government information systems are entrusted with generating and distributing millions of checks worth billions of dollars to the public.

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. Licensing would also allow for violators to be punished. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice.

Issues Associated with Government Licensing of IT Workers

Australia, Great Britain, and the Canadian provinces of Ontario and British Columbia have adopted licensing for software engineers. In the United States, the National Council of Examiners for Engineering and Surveying (NCEES) has developed a professional exam for electrical engineers and computer engineers. However, there are many reasons why there are few international or national licensing programs for IT workers in the United States:

- *There is no universally accepted core body of knowledge.* The core body of knowledge for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. At present, however, there are no universally accepted standards for licensing programmers, software engineers, and other IT workers. Instead, various professional societies, state agencies, and federal governments have developed their own standards.
- *It is unclear who should manage the content and administration of licensing exams.* How would licensing exams be constructed, and who would be responsible for designing and administering them? Would someone who passes a license exam in one state or country be accepted in another state or country? In a field as rapidly changing as IT, workers must commit to ongoing, continuous education. If an IT worker's license were to expire every few years (like a driver's license), how often would practitioners be required to prove competence in new practices in order to renew their license? Such

Ethics for IT Workers and IT Users

- questions would normally be answered by the state agency that licenses other professionals.
- *There is no administrative body to accredit professional education programs.* Unlike the American Medical Association for medical schools or the American Bar Association for law schools, no single body accredits professional education programs for IT. Furthermore, there is no well-defined, step-by-step process to train IT workers, even for specific jobs such as programming. There is not even broad agreement on what skills a good programmer must possess; it is highly situational, depending on the computing environment.
 - *There is no administrative body to assess and ensure competence of individual workers.* Lawyers, doctors, and other licensed professionals are held accountable to high ethical standards and can lose their license for failing to meet those standards or for demonstrating incompetence. The AITP standards of conduct state that professionals should “take appropriate action in regard to any illegal or unethical practices that come to [their] attention. However, [they should] bring charges against any person only when [they] have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.” The AITP code addresses the censure issue much more forcefully than other IT codes of ethics, although it has seldom, if ever, been used to censure practicing IT workers.

* * * 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. Likewise, defendants who have particular expertise or competence are measured against a **reasonable professional standard**. For example, in a medical malpractice suit based on improper treatment of a broken bone, the standard of measure would be higher if the defendant were an orthopedic surgeon rather than a general practitioner. In the IT arena, consider a hypothetical negligence case in which an employee inadvertently destroyed millions of customer records in an Oracle database. The standard of measure would be higher if the defendant were a licensed, Oracle-certified database administrator (DBA) with 10 years of experience rather than an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle software.

If a court finds that a defendant actually owed a duty of care, it must then determine whether the duty was breached. A breach of the **duty of care** is the failure to act as a reasonable person would act. A breach of duty might consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when

there is a duty to do so—for example, a police officer not protecting a citizen from an attacker.

Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as **professional malpractice**. For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client's books is liable for accounting malpractice. Professionals who breach this duty are liable to their patients or clients, and possibly to some third parties.

Courts have consistently rejected attempts to sue individual parties for computer-related malpractice. Professional negligence can only occur when people fail to perform within the standards of their profession, and software engineering is not a uniformly licensed profession in the United States. Because there are no uniform standards against which to compare a software engineer's professional behavior, he or she cannot be subject to malpractice lawsuits.

IT USERS

Chapter 1 outlined the general topic of how corporations are addressing the increasing risks of unethical behavior. This section focuses on encouraging employees' ethical use of IT, which is an area of growing concern as more companies provide employees with PCs, tablets, cellphones, and other devices to access to corporate information systems, data, and the Internet.

Common Ethical Issues for IT Users

This section discusses a few common ethical issues for IT users. Additional ethical issues will be discussed in future chapters.

Software Piracy

As mentioned earlier in this chapter, 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. For example, the software piracy rate in China exceeds 80 percent, so it is clear that the business managers and IT professionals in that country do not take a strong stand against the practice.

Sometimes IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home. When confronted, the IT user's argument might be: "I bought a home computer partly so I could take work home and be more productive; therefore, I need the same software on my home computer as I have at work." However, if no one has paid for an additional license to use the software on the home computer, this is still piracy.

DRF

The increasing popularity of the Android smartphone operating system has created a serious software piracy problem. Some IT end users have figured out how to download applications from the Android Market Web site without paying for them, and then use the software or sell it to others. One legitimate Android application developer complained that his first application was pirated within a month and that the number of downloads from the pirate's site were greater than his own. Professional developers become discouraged as they watch their sales sink while pirates' sales rocket.³⁵

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at worker productivity and waste time. Furthermore, activities such as viewing sexually explicit material, sharing lewd jokes, and sending hate email could lead to lawsuits and allegations that a company allowed a work environment conducive to racial or sexual harassment. A survey by the Fawcett Society found that one in five men admit to viewing porn at work, while a separate study found that 30 percent of mobile workers are viewing porn on their Web-enabled phones.^{36,37} Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders.

Recently, the executive director of the Pentagon's Missile Defense Agency issued a memo to its 8,000 employees warning them to stop using their work computers to access Internet porn sites. One concern of government officials is that many pornography sites are infected with computer viruses and other malware; criminals and foreign intelligence agencies often use such sites as a means to gain access to government and corporate computer networks. For example, a foreign agent can embed malware capable of stealing data or opening computer communications ports whenever certain photos or videos are downloaded to a computer.³⁸

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describes individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also includes information about customers—credit card information, telephone number, home address, and so on. Confidential information describes a company and its operations, including sales and promotion plans, staffing projections, manufacturing processes, product formulas, tactical and strategic plans, and research and development. An IT user who shares this information with an unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors. For example, if an employee accessed a coworker's payroll records via a human resources computer system and then discussed them with a friend, it would be a clear violation of the coworker's privacy.

In late 2010, hundreds of thousands of leaked State Department documents were posted on the WikiLeaks Web site. As of this writing, it appears that the source of the leaks was a low-level IT user (an Army private) with access to confidential documents. The documents revealed details of behind-the-scenes international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea.³⁹ The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will lead to less sharing of sensitive information with the United States because of concerns over further disclosures.

Supporting the Ethical Practices of IT Users

The growing use of IT has increased the potential for new ethical issues and problems; thus, many organizations have recognized the need to develop policies that protect against abuses. Although no policy can stop wrongdoers, it can set forth the general rights and responsibilities of all IT users, establish boundaries of acceptable and unacceptable behavior, and enable management to punish violators. Adherence to a policy can improve services to users, increase productivity, and reduce costs. Companies can take several of the following actions when creating an IT usage policy.

Establishing Guidelines for Use of Company Software

Company IT managers must provide clear rules that govern the use of home computers and associated software. Some companies negotiate contracts with software manufacturers and provide PCs and software so that IT users can work at home. Other companies help employees buy hardware and software at corporate discount rates. The goal should be to ensure that employees have legal copies of all the software they need to be effective, regardless of whether they work in an office, on the road, or at home.

Defining the Appropriate Use of IT Resources

Companies must develop, communicate, and enforce written guidelines that encourage employees to respect corporate IT resources and use them to enhance their job performance. Effective guidelines allow some level of personal use while prohibiting employees from visiting objectionable Internet sites or using company email to send offensive or harassing messages.

Structuring Information Systems to Protect Data and Information

Organizations must implement systems and procedures that limit data access to just those employees who need it. For example, sales managers may have total access to sales and promotion databases through a company network, but their access should be limited to products for which they are responsible. Furthermore, they should be prohibited from accessing data about research and development results, product formulas, and staffing projections if they don't need it to do their jobs.

Installing and Maintaining a Corporate Firewall

A **firewall** is hardware or software that serves as a barrier between an organization's network and the Internet; a firewall also limits access to the company's network based on the organization's Internet-usage policy. A firewall can be configured to serve as an effective deterrent to unauthorized Web surfing by blocking access to specific objectionable Web sites. (Unfortunately, the number of such sites is continually growing, so it is difficult to block them all.) A firewall can also serve as an effective barrier to incoming email from certain Web sites, companies, or users. It can even be programmed to block email with certain kinds of attachments (for example, Microsoft Word documents), which reduces the risk of harmful computer viruses.

Table 2-5 provides a manager's checklist for establishing an IT usage policy. The preferred answer to each question is yes.

Ethics for IT Workers and IT Users