

Ethics for IT Workers and IT Users

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. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections



Relationships That Must Be Managed

Relationships between IT Workers and Employers

IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. 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**. Many other aspects of this relationship may be addressed in a company's policy and procedures manual or in the company's code of conduct, if one exists. These issues may include protection of **company secrets**; **vacation policy**; **time off for a funeral** or an illness in the family; **tuition reimbursement**; and **use of company resources**, including computers and networks. Other aspects of this relationship develop over time as the need arises (for example, whether the employee can leave early one day if the time is made up another day). Some aspects are addressed by law—for example, an employee cannot be required to do anything illegal, such as falsify the results of a quality assurance test. Some aspects are specific to the **role of the IT worker and are established based on the nature of the work or project**—for example, the **programming language** to be used, the type and **amount of documentation** to be produced, and the **extent of testing** to be conducted.

As the stewards of an organization's IT resources, IT workers must set an example and enforce policies regarding the ethical use of IT. 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—either they allow it to happen or they actively engage in it, often to reduce IT-related spending.

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 is funded both through dues based on member companies' software revenues and through settlements from companies that commit piracy. BSA membership includes two dozen or so members such as Adobe, Apple, Intel, McAfee, Microsoft, Symantec, and The Math Works. More than 100 BSA lawyers and investigators prosecute thousands of cases of software piracy each year. BSA investigations are usually triggered by calls to the BSA hotline (1-888-NO-PIRACY), reports sent to the BSA Web site (www.nopiracy.org), and referrals from member companies. Many of these cases are reported by discontented employees or former employees. For 2011, the commercial value of software piracy in the United States was estimated to be nearly \$10 billion with 31 percent of computer users participating in this illegal activity. When BSA finds cases of software piracy, it assesses heavy monetary penalties. Failure to cooperate with the BSA can be extremely expensive. The cost of criminal or civil penalties to a corporation and the people involved can easily be many times more expensive than the cost of "getting legal" by acquiring the correct number of software licenses. Software manufacturers can file a civil suit against software pirates with penalties of up to \$150,000 per copyrighted work. Furthermore, the government can criminally prosecute violators and fine them up to \$250,000, incarcerate them for up to five years, or both. 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. BSA was alerted to this situation by a report sent to its Web site.

Trade secrecy is another area that can present challenges for IT workers and their employers. 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. Examples include the Colonel's secret recipe of 11 herbs and spices used to make the original KFC chicken, the formula for Coke, and Intel's manufacturing process for the i7 quad core processing chip. Employers worry that employees may reveal these secrets to competitors, especially if they leave the company. As a result, companies often require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets.

Zynga is a provider of online social games such as ChefVille, CityVille, FarmVille, FrontierVille, and Zynga Poker that boast over 300 million active monthly users. After just over a year with Zynga, the firm's general manager of CityVille left to become a vice president at Kixeye, a competitor. Zynga claimed that the employee stole files with data critical to the business—including financial projections, marketing plans, and game designs. Zynga filed a request for a temporary restraining order barring its former employee from sharing or copying the information or from engaging in any actions using the information to develop online games employing these trade secrets.

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. The H-1B visa is a work visa that allows foreigners to come to the United States and work full-time in specialty occupations that require at least a four-year bachelor's degree in a specific field. A U.S. consultant for India-based outsourcing firm Infosys filed a whistle-blower lawsuit against the firm for abusing H-1B program rules. The lawsuit alleged that at a management meeting in Bangalore, Infosys officials discussed the need to "creatively" circumvent the H-1B visa restrictions. The lawsuit further alleged that Infosys brought workers to the United States on B-1 visas (which are intended for workers coming to the United States for short-term work assignments only), but that these workers were assigned full-time jobs. It also claimed that Infosys was not paying the B-1 workers the prevailing wage and was not withholding federal and state income taxes. The whistle-blower filed a separate lawsuit in which he claimed that Infosys retaliated

against him for the filing of the visa-related lawsuit by lowering his bonuses, harassing him, and giving him no meaningful work to do.