CONTENT ANALYSIS OF COMPUTER ETHICS HANDBOOKS IN TEXAS STATE AGENCIES

BY

MARIA EVELIA MORENO

AN APPLIED RESEARCH PROJECT (POLITICAL SCIENCE 5397)
SUBMITTED TO
THE DEPARTMENT OF POLITICAL SCIENCE
SOUTHWEST TEXAS STATE UNIVERSITY
IN PARTIAL FULFILLMENT
FOR THE REQUIREMENTS FOR THE DEGREE
OF

MASTER OF PUBLIC ADMINISTRATION

(FALL 1998)

FACULTY APPROVAL

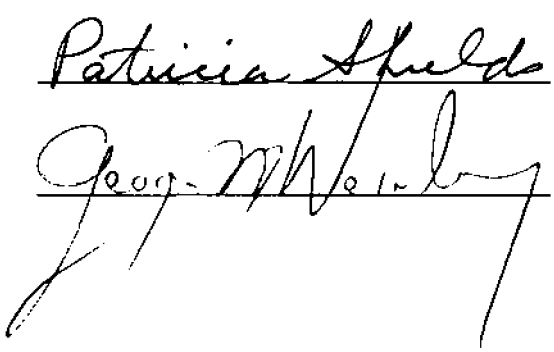

TABLE OF CONTENTS

APPENDICES

CHAPTER I

INTRODUCTION

In order for the employees to be aware of computer ethics, some type of written communication should take place. The methods used to educate employees about computer ethics are crucial to guarantee that those employees are aware of their responsibilities toward the use of computers and the information obtained from computers. The use of computer technology in the private and public sector has created new dilemmas and issues that both management and the employee need to face. These dilemmas are comprised of legal and ethical issues such as:

- Confidentiality of sensitive data and invasion of privacy (Parker 1984, 83).
- Personal morality and organizational loyalty (Parker 1984, 99).
- Ownership and disputed rights of computer software (Johnson and Nissenbaum 1995, 148.
- Responsibility for computer applications with controversial consequences (Parker 1984, 121).
- Responsibility for dissemination of complete and accurate information to decision makers or the public (Parker 1984, 139).

The following scenario illustrates the ethical issue in "confidentiality of sensitive matter."

A computer file maintenance clerk worked in a police department computer center. He had access to local and national arrest records. No laws or rules existed governing his handling of the information. A friend was in charge of security in a large organization and was responsible for performing background investigation of new employees. The new employees signed release statement authorizing their employer to investigate their background, including arrest records.

The security person frequently asked for and received copies of all arrest records for new employees from the friend in the police department, who supplied the records

> *as a favor. Both assumed this was acceptable practice, since arrest records are individually available from police arrest blotter, which are in the public domain. Complete arrest records were more conveniently obtained through the computer system. The police employee did not inform his superior or request permission to do this, since it was routinely done for courts, prosecutors, attorneys, other police agencies, and banks.* (Parker 1984, 85).

In this case it was decided that clerk should not have given out the information and that it was an irresponsible act. It was considered to be misappropriation of computer resources and also unethical. However, it was also pointed out that the clerk's superiors should have instructed him on the handling of confidential information. In summary, it was determined that it was poor management not to give specific instructions or ethical training which resulted in ethical violations.

The adoption of computer technology by private companies and government agencies has drastically changed the way business is conducted and affected the customer, client and administrator. Computers have changed the way people work, communicate with one another, the way they are educated and how they entertain themselves. However computer technology is a phenomenon that is still considered "new" and has resulted in unexpected effects. The benefits of computer technology are tremendous and exciting. It has created new ways of doing business that are different from past methods.

Information systems have evolved into sophisticated and vital networks all over the nation. These networks make it possible to conduct business, educate, administer health care, and conduct other activities all over the world in a rapid and expedient manner. "Computers have changed the environment in which they are used and in so doing give rise to questions of right and wrong, good and bad." (Johnson an Nissenbaum 1995, 1). Many of these changes raise social and moral questions which lead to ethical analysis and ethical decision making.

Some of the most frequent questions dealing with computer ethics involve issues such as invasion of privacy, computer professional responsibility, ownership of artificial intelligence, and the actual reliability of computers. A changing work environment has

occurred in both the private and public sectors. As per one computer ethics expert, references are being made to "the insidious threats of government control reminiscent of Orwell's Big Brother in 1984. (Edgar 1997, 2). The issue of privacy is one of the most prevalent among the computer ethics issues. Who actually owns the information found on computers and web sites? Can an individual stop private information from being put on a computer system? Does the Privacy Act of 1974 apply to information found on computers? Do the private and public sector maintain a code of ethics with regard to computer technology? If so, what steps are taken to instill these ethics in their employees? What methods have the private and public sector set up to ensure that computer ethics are followed?

The issues that arise in computer ethics fall into four categories: (Edgar 1990, 3.)

1. Computer technology may ***aggravate*** traditional ethical problems such as creating a new way to instigate invasion of privacy
2. Computer technology may ***transform*** familiar ethical problems and ambiguities such as changing the criteria for ownership; such as a literary work
3. Computer technology may ***create*** new problems unique to the computer world, such as relying on computers to make decisions about war strategies
4. Computer technology may ***relieve*** existing moral problems because the computer may be utilized to project consequences in different areas such as environment and one will be able to make more informed moral decisions.

The use of computers in the public sector has many different implications. Public employees have access to all types of information. For example, social service agencies may have access to Internal Revenue System (IRS), Social Security benefits, state and federal employment agencies, and health and life insurance benefits. These public entities often maintain computer databases that contained detailed information such as:

- the size of the household
- the head of the household

- who makes the most money
- how much they make
- address information
- driver's license numbers
- other household data.

But it is not only social service agencies that have access to private information. Private sector entities can also access this type of data from various computer networks, credit reports, and store records through the use of sophisticated computer technology.

The private sector has access to confidential information through the use of its customer files. It is able to obtain information from their customers and to buy data from other private entities. The Internet and other web sites have made it possible for computer experts to extract personal data about customers.

Tools utilized by state agencies to expose new and tenured employees to state agency policy and procedures are found in written communication form such as Human Resource Handbooks, employee guides, and other types of written formats. This written communication may cover employee personnel policy, benefits, work rules, leave guidelines and at times ethics guidelines. However, one question that arises is whether a written communication form exists which explicitly covers computer ethics.

The majority of the computer ethics literature reviewed, such as textbooks, articles, and the Internet, focuses on the nature of computer ethics in the workplace and that it should be emphasized in the private and public sector. An overriding theme within the literature also focuses on the need for managers in the public sector to emphasize computer ethics. The literature does not include an ideal computer ethics handbook. However, the information reviewed can be used to inform state agencies as to the topics that should be incorporated into some type of written communication guide that focuses on computer ethics in the work area. The focus of the communication should be to enable

the employee to make timely, sound yet ethical decisions in the execution of his or her duties.

Purpose of the Research Project

The purpose of this research is threefold. The first purpose is to describe the ideal written characteristics of effective computer ethics. The second purpose is assess the formal forms of communication contained in public sector handbooks and compare written computer ethics communications used by Texas state agencies with the practical ideal type. The final purpose is to make recommendations to improve computer ethics written communication found in Texas state agencies. By describing a "practical guide" and making recommendations, it is hoped that Texas state agencies will incorporate this research information and consolidate written communications into a uniform handbook or guide which will become a "practical working tool" for computer ethics presentations to public sector employees.

Chapter Descriptions and Organizations

Chapter Two provides an in-depth narrative of the literature reviewed that has relevance to computer ethics. The conceptual framework was based and developed through concepts found in the literature review. The need of the public administrators to emphasize computer ethics is discussed. Chapter Three provides background information--the research setting--for this Applied Research Paper. As previously documented, the main focus of this research project is on computer ethics written communications used by public administrators in the state of Texas. The legal components of computer ethics are introduced. These components are identified and developed through descriptive categories developed by the literature review. Chapter Four deals with methodology and a discussion of the operationalization of the data. It provides a detailed narrative of the method used to gather and analyze the research data for this study. This chapter also explains why the methodology chosen, content analysis, is the best choice for the research

topic. Chapter Five provides the results and analysis of the content analysis of the state handbooks and other documents. Percent distribution and raw data are used to depict the results of the data gathering. Chapter Six concludes the research study. It includes a summary of the major findings and conclusions. A recommendation for improvements for public sector employee computer ethics written communication such as handbooks is presented.

CHAPTER 2

REVIEW OF THE LITERATURE

Introduction

The purpose of this chapter is to discuss scholarly literature about computer ethics and how the information is disseminated to the public employee by the public administrator. Through the literature review computer ethics components and elements will be developed.

There are many state and federal agencies who have equipped their employees with personal computers at the job site. According to various publications and textbooks reviewed, there are concerns about the type of training given to employees. How does one effectively use the computers without infringing on ethical principles? Are classes held about computer ethics? Are there handbooks or employee guides that address the question of computer use? Are its implications such as ethical dilemmas and legal issues being reviewed with the public sector computer user?. "As advances in technology shape the work place of the future, ethical standards will need to guide employees as they encounter new situations and new moral dilemmas." (Jones 1995, 64).

One of the issues in the study and analysis of ethics training is that it is difficult to reduce to "numerical data". Due to this characteristic, ethics training advocates have problems in providing clear analytical data and results of ethical training. (Jones 1995, 64) Yet ethics training may still be the first step in incorporating stronger ethics concerns in computer technology use.

One objective of the ARP is to gather information to examine if the public sector employees receives computer ethics training and review the tools used to deliver the training. The premise is that there is computer ethics training and that the method utilized is a practical type. An assumption was also made that this training was documented in

some form. such as a handbook, employee guide or training curriculum Another intent of the review is to develop a conceptual tool by which computer ethics training may be delivered to public employees. To achieve the purposes stated this chapter reviews different aspects of computer ethics as presented by the articles reviewed in preparation for this proposed Applied Research Project. In the final segment of this chapter the conceptual framework used to assess the computer ethics communication tools is described and explained.

Need of Public Administrators to Emphasize Computer Ethics

The adoption of computer technology[1] by private companies and government agencies has drastically changed the way business is conducted and affected both the customer, client and the administrator. Many of these changes raise social and moral questions about how people are using the computer. The lack of what constitutes computer ethics may at times lead to ethical analysis and the need for ethical decision making. "Computers are special technology and raise some special ethical issues." (Johnson and Nissenbaum 1995, 1). It is the absence of a clear concept of computer ethics that raises so many questions about computer usage creating moral dilemmas and issues.

What is computer ethics? Moor(1985, 7) defines computer ethics as " the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology." Computers provide a new way of doing business which in turn gives new choices for action. Moor goes on to explain that a central task of computer ethics is to determine what should be done in such situations.

Ethics has been described as the "field of study that is concerned with questions of value, that is, judgments about what human behavior is "good" or "bad." (Barger 1995, 1).

---

[1] The terminology "computer technology" is used broadly and includes computers, software, hardware, information systems, and computer networks. The Internet and world wide web is also included in this terminology.

Computers raise problems in privacy, theft, ownership and responsibility. The literature reviewed indicates that ethical judgments vary in the workplace. It all depends on the individual's world view. Moor states that much of the work of computer ethics is a matter of *"proposing conceptual frameworks for understanding ethical problems involving computer technology."*

Ethical issues often arise as administrators decide how to create and/or implement a computer system. If ethical issues are not resolved, there may be negative consequences for the individual who misuses the computer. In addition, organizations may face legal problems associated with computer use.

General Background on Computer Technology

With the coming of computer technology and all its innovations, significant changes have occurred in the United States and in the rest of the world. Many of these changes are positive and have created opportunities for organizations--both in the private and the public sectors. The individual also has benefited from the new technology encountered in his/her professional world as well as in his/her personal life.

The impact of technological change may be described as multilevel, complex, and perplexing. The "modern American way of life was created with the existence of the automobile and interstate highways." (Burke 1998, 13). The automobile made it possible for citizens to move often and gave more opportunities to an individual to choose something different. The innovation of the automobile led to superhighways. The highways led to the creation of suburbs and a new way of life. The suburban ethic led to the ghettoization of some citizens who could not leave the center of the city sometimes leading to social disruptions. (Burke 1998, 13).

Computer technology is similar to the innovation of the automobile. It appears to be a phenomenon that will improve communication between individuals, cities, and countries. This technology may reap the benefits sought like cheaper energy, grater mobility, better health care, but it also gets unforeseen effects. (Johnson and Nissenbaum 1995, 1). It is

true that technology may make life easier for all because work will be easier, faster, more accurate, and more productive. But, at what price? "Dramatic evolution in the use of computers and electronic communication has presented problems and new challenges insofar as ethical conduct is concerned." (Koocher 1996, 9). Some of the problems encountered may be in the area of electronic communication etiquette, electronic psychotherapy, radiation problems associated with computer usage, the lack of Internet access by low income citizens, and the impact of information technology on our social systems.

Expert Systems and Computer Ethics

What is meant by an expert system? An expert system may be described as an information system technology (IST). IST sets the computer and computer applications to efficiently produce information needed by an organization and its management. The expert system is considered a type of artificial intelligence which emulates the thinking and decision-making process of human beings (Belohav and Drehmer 1997, 1). This system is constructed by defining the perception and opinions of experts and deriving decision rules based on those opinions. Thus, this computer based experts system is believed to have the capability to replace the current organizations' decision making process. IST has had a direct effect on organizations by creating significant changes in standard operation procedures (SOP). The effect on the business environment has caused drastic changes on the way business is conducted.

In this modern age of technology ethical dilemmas are not confined to the computer programmers or hardware technicians. Ethical dilemmas are also prevalent among the personal computer user. A movement is growing among computer professionals and entrepreneurs to "curb the lawless side of the Internet and bring awareness and acceptance

of computer ethics."[2] There are many issues in information systems for which there are no laws. Where does an individual turn for ethical guidelines?

The Computer Ethics Institute (CEI) is working to move computer ethics out of the philosophical debates and into the real world of computers and users. CEI stresses that for centuries there has been, in the real world, definite standards of behavior. Therefore it is time to transpose such values and ethical standards to the computer world. The National Computer Ethics and Responsibilities Campaign (NCERC) believes that an important part of the answer to computer ethics' problems lies in education. Ethics of different fields are taught in schools but computer ethics is not.[3] Much of the unethical behavior that occurs in organizations is a product of ignorance of computer ethics. NCERC advocates that computer ethics becomes part of standard school curriculum. NCERC also hopes that all who are concerned understand that there is vested interest in regulating themselves both in the private and the public sectors. In order to give ethical considerations priority, one has to understand the relationship that is created between the developer and the user of the expert system.

ROLE OF THE COMMON RATIONALE OF COMPUTER ETHICS

A useful "myth" is that someday there might be a common rationale for computer ethics. (Barger 1994, 1). Some experts believe that achieving a common rationale may be mythical because this is probably not achievable. Robert Barger states that there are four basic philosophies in computer ethics: idealism, realism, pragmatism, and existentialism. Idealism, he states, is a belief that reality is *ideas* and ethics involves conforming to *ideals.* He describes realism as a "belief that reality is nature and ethics involves acting according

---

2 This information was found on the Internet: "Introducing Ethics into the Computer World." Bringing Cyperspace to the Classroom, October 4, 1997, 1. The information was chosen due to its relevance to teaching of computer ethics in a classroom setting.

3 Ibid., 1

to what is natural." Barger explains that idealism (ideas) and realism (nature) may be considered **ABSOLUTIST** world views because they are based on something that is fixed. Pragmatism (based on society), Barger explains, is a "belief" that reality is not fixed but in process: thus ethics is practical." Existentialism (based on the individual) is a belief that reality is self-defined but ethics is individual. He then explains that pragmatism and existentialism can be considered **RELATIVIST** worldviews because they are based on something rational. (Barger 1995, 1). Barger concludes that the search for a common rationale for ethics decision making needs to be based on an absolutist framework which is derived from idealism and realism philosophies. In the long run, he further explains, and individual or social ethical policy must be based on principle which is founded on the absolutist framework. (Barger 1994, 1).

In his argument for a common rationale for computer ethics, Barger goes on to explain that individual and social ethical policy must be based on principle. He states that ethical methodology such as pragmatism cannot serve as the basis for ethical decision - making. There are two dilemmas in computer ethics: what to prohibit and how to enforce such prohibition. A suggestion for a common rationale for computer ethics consists of an agreement on principles such as honesty, justice, truthfulness. Secondly, an application of these principles in prohibition of unethical behavior. Third, enforcement of these prohibitions by punishment and/or by positive incentives for compliance. (Barger 1994. 2). Barger also agrees with Professor Alicia Juarrerro who states that there is a technical revolution and no one knows how it will turn out. Older technology has been passed by current technology. Basic ethical standards are not obsolete and moral standards need to be applied to the current technological revolution. (Barger 1994, 2).

COMPUTER CODE OF ETHICS

Many companies develop their own Code of Ethics for their computer users. A code of ethics is a collection of principles intended as a guide for members of a company or an

association. One of the oldest Code of Ethics is the Ten Commandments. (Turban, McLean, and Wetherbe 1996, 738). Through the Ten Commandments clear guidelines are given as to what one should or should not do.

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.*

Another code of ethics was adopted by the Association for Computing Machinery (ACM); the ACM Code of Professional Conduct. (Parker 1984, 159). The preamble states that in order to be given professional status by the public there needs to be "adherence to a professional code of ethics." The code is divided into general principles, canons; professional ideals, ethical considerations; and mandatory rules, Disciplinary Rules. (APPENDIX A).

A revised Code of Ethics was adopted by the ACM on October 16, 1992. (APPENDIX B). It contains several issues that many professionals might encounter but it is not all inclusive. It is supplemented by a code of guidelines. Computing is not specifically mentioned in the moral imperative section. The code is concerned with how

these imperatives are followed or applied by computing professionals. (Edgar 1997, 422). The general moral imperatives are listed as follows:

1.1 Contribute to society and human well-being

1.2 Avoid harm to others

1.3. Be honest and trust worthy

1.4 Be fair and take action not to discriminate

1.5. Honor property rights including copyrights and patents

1.6 Give proper credit for intellectual property

1.7 Respect the privacy of others

1.8 Honor confidentiality

Section 2 of this code deals with more professional responsibilities. In addition to being professionally competent, the code states, a professional must know, respect, and obey existing local, state, national and international laws except when there is an ethical basis not to do this. Computer professionals must evaluate the impact of a computer system and accept responsibility for the product. Others rely on them to be trustworthy. The reliability of the system as well as relevant conflicts of interest must be identified. No one should enter another computing system, software, or data files without authorization. Trespassing includes accessing communication networks and computer system , accounts, or any files associated with those systems. (Edgar 1997, 427).

One of the main obstacles to a consistent code of ethics is that there are different philosophies regarding ethics. This has been a problem for many years where philosophers have proposed many different types of ethical theories and propositions. What is unethical is not necessarily illegal. Most ethical people are not trying to decide whether to break the law or not. The question is to distinguish between right or wrong. Some companies believe that it is not their responsibility to instill ethics, rather ethical behavior should be instilled by the family and schools.

ROLE OF PRIVACY RIGHTS IN COMPUTER ETHICS

One of the ethical issues created by the increased used of computer technology deals with information privacy. Privacy is defined as the collection, storage, and dissemination of information about individuals. A definition of information privacy is the "claim of individual, groups or institutions to determine for themselves when, and to what extent, information about them as communicated to others." (Turban, McLean and Wetherbe 1996, 719).

There is an increasing demand for information that can be found in government records. One New York article writer states "for Government, selling data can provide extra revenue in time of tight budgets." (Edgar 1997, 299). Government records found in computers containing confidential information critical to an individual's privacy are: the motor vehicle records, police computers, health care providers, and various computer matches such as the Texas wage and unemployment computerized reports. (Texas Workforce Commission). The American Bar Association has identified seven areas in which computer matching programs affect privacy. (Edgar 1997, 299).

1. *The Fourth Amendment*
2. *The Privacy Act of 1974*
3. *Fair Information Practice Principle*
4. *Due Process*
5. *Data Process*
6. *Data Security*
7. *Data Merging*
7. *Fundamental Privacy Rights*

Now that government agencies have vast information on individuals, several privacy issues have risen. Some privacy advocates believe that there should be a policy agency that monitors the dissemination of information. Others argue for public access to computer information such as data related to Social Security. (Hammit 1997, 11).

According to Hammit, the individual's information should be accessible unless the government has proof that disclosure would cause "a foreseeable harm." He goes on to stress that there is no difference between one's ability to access third party information through the Internet (high tech) or intercepting a letter or a telephone call (low tech). In either case entry may be done fraudulently. Hammit adds that "regardless of the possibility of fraud, the agency should at least consider the question of how private or confidential the account information is as a practical matter". He concludes that government electronic dissemination schemes are occurring more frequently but it should not be turned into a matter of mass hysteria.

Sale of Public Information

The sale of public information by government agencies is another critical aspect of the automated system utilized by government entities. According to one authority, Blake Harris, the general public in Europe and other countries appear to be more concerned about personal privacy than most Americans. However, since more Americans are using the Internet there may be increased concern with privacy issues. This in turn may lead to restrictions on the sale of public information. The second issue Harris considers lies with the public's right to know and the Freedom of Information Act. (Harris 1997, 32). Access advocates feel that the information has been collected by using tax payer's money. Subsequently, they, this "private" information has become "public" information and there should only be minimal charges to cover production costs. Generally when public agencies agree to disclose client information, they include charges that will cover the cost of electronic databases and computers.

The Privacy Act of 1974

The Privacy Act of 1974 sets clear guidelines for the proper collection/dissemination of information. The act guarantees one's rights to see one's individual records and it gives the right to amend records (within guidelines/exemptions). In addition, this act gives the

right to sue the government in cases of law violation. According to a study released by the OMB WATCH, a non-profit organization concerned about federal government's response to public need, 31 out of 70 federal agencies collect information from networks. The study further stated that less than 20% collect information that qualifies as records as stated in the Privacy Act of 1974. (Kavanaugh-Brown 1997, 14).

This act also established general records management guideline for supplying information by federal agencies. It includes a requirement that the agencies must publish notices describing all system of record, including personal data record policies, practices and unique system. The Kavanaugh-Brown article also pointed out that the OMB-WATCH study found that only four agencies have consistent notices. These are:
1) Commodity Futures Trading Commission 2) Federal Deposit Insurance Corp;
3) U.S. Postal Service and 4) Social Security Administration. Three federal agencies have placed "cookies"[4] which will automatically retrieve personal data from a user's hard drive. The user is unaware that this is happening. These three agencies are: 1) the Department of Veterans Affairs; 2) the Federal Emergency Management Agency; and 3) the National Science Foundation. Kavanaugh-Brown further stated that the study found only 17 of the 70 Web sites provided adequate Privacy Act statements. All of the sites studied were linked to the White House Web site. The author pointed out the discrepancy in that the White House staff have been pressuring private web sites to ensure their customers individual privacy is protected.

---

[4] A "cookie" is a small piece of information which a web server can store temporarily with a user's web browser. The browser can rember some specific information which the web server can later retieve. "Cookies: what they are and how they work", Support Tech Support, Netscape.com/kblcl.ent/970226-2html.

THE ROLE OF THE INTERNET

Any ethics policy would have to take into account and review the Internet. This section develops the unique challenges to organizations and individual ethics associated with the Internet's use and abuse. It is unlikely that anyone would dispute that the Internet is a valuable resource. The Internet's predecessor was ARPANET which was managed by the Department of Defense. (Foster, Ratkowski, and Goodman 1997, 15). The United States government has been responsible for much of the Internet research. The Internet requires coordination of thousands of Internet service providers (ISP). The ISPs must coordinate and meet with network groups. Foster et al. states that "understanding the governance of the Internet requires that standard making processes be considered and that relationships between ISPs and broader Internet business community be understood".

The Internet is governed by a complex interaction between business researchers and governments all over the world. Foster also suggests that what is missing is a global consensus on proper value of market mechanisms, government regulation, and international accord (p. 20). Regardless of who governs the Internet or who really has control over the networks, the Internet is a valuable resource that can be used widely and wisely. Sometime the Internet is not used wisely depending on the user.

One computer ethics expert states that personal responsibility and respect for others is the cornerstone of a successful Internet policy. (Willard 1997, 1) "Treat others as you would like to be treated" is a rule one should adhere to. Willard also advocates one should be professional and polite about what one says on the Internet. One should be clear and logical with Internet correspondence. All quotes and references should be cited. Above all, the privacy of others should be respected. Personal information may be gathered, stored and dispersed easily due to the technology available that privacy is constantly threatened.

There are norms/guidelines which organizations should stress in order to protect privacy. (Willard, 1997, 12-13).

1. Keep information and personal details confidential.
2. Treat what people say with respect.
3. Don't read other people's E-mail.
4. Don't invade other people's storage space.

In short, "Don't go where you don't belong." Violation of these guidelines is often equivalent to privacy violations and /or violation of unauthorized access laws.

Both private companies and public agencies have certain responsibilities regarding the Internet and/or E-mail. Management has the right to access employees mail but employees do not have the right to look in other employees E-mail files. (Willard 1997, 14. Employees need to be extremely careful with information gathered through E-mail. Many company and agency trade secrets are found in E-mail and this information should not be shared with outsiders. Not only is this unethical and unprofessional, but an employee can get fired for this type of disclosure. Things to remember not to do on the Internet are:

1. Don't get mad on the Internet.
2. Be careful not to reach to someone else's E-mail.
3. Encryption is not always reliable.
4. Don't send chain letters.
5. Don't engage in spamming and cause network congestion.

Most states have laws that address the issue of unauthorized access to a computer site or system. But it is the user's responsibility to acquire secured passwords and accounts. As per several computer ethics experts, (such as Edgar, Johnson, Turban, and Willard) another user responsibility deals with knowing and taking precautions not to introduce viruses into the network.

CONCEPTUAL FRAMEWORK

The purpose of this section of the literature review chapter is to provide background information on computer ethics. The research purpose is threefold. The first purpose is to describe the ideal written characteristics of effective computer ethics. The second purpose is to assess the formal forms of communication contained in public sector handbooks and compare written computer ethics communications used by Texas state agencies with the practical ideal type. The final purpose is to make recommendations to improve computer ethics written communications found in Texas state agencies.

PRACTICAL IDEAL TYPE

The conceptual framework has a dual purpose. First, the literature reviewed contained many references to computer ethics and what different author's believe should be classified as computer ethics. But the literature reviewed lacks studies that identify and describe the typical characteristics of what should be included in a public sector's computer ethics handbook. In short, it appeared that there are very few computer ethics employee handbooks in the public sector. Texas state agency handbooks are generally the documents used to provide training and guidance to the public sector employee. Secondly, an analysis of these handbooks can establish the existence or non-existence of specific computer ethics training and/or guidelines for the Texas state employee.

Using insights from the literature review, topics and items are identified as ideal or recommended to be included as components of computer ethics written communications. These components are noted as recommended elements of employee computer handbooks and they are classified into six categories. **(FIGURE 2.1)** Basic characteristics have been identified which will be used as ideal standards for computer ethics written communications. The elements are not rigid in scope as the rationale behind a successful computer ethics handbook is a vision for the future. The vision is that public sector administrators embrace the necessity of a computer ethics handbook and take into account the ideal elements developed in this chapter.

FIGURE 2.1

COMPUTER ETHICS HANDBOOK COMPONENTS

SETTING OF ETHICAL GUIDELINES FOR EMPLOYEES
DEFINITION OF ETHICS
ETHICAL THEORY
MORALITY AND VALUES
OWNERSHIP OF COMPUTER ETHICS RESPONSIBILITY
NEED OF ETHICS TRAINING

PRIVACY AND CONFIDENTIALITY
CONFIDENTIALITY OF SENSITIVE DATA
PRIVACY ACT OF 1974
PROTECTION OF CLIENT'S INFORMATION
RIGHT TO PRIVACY

COMPUTERS AND USER RESPONSIBILITY
SECURITY AND SECURITY AGREEMENTS
ACCOUNT SECURITY/PASSWORDS
ACCESS AND COPYING OF COMPUTER SOFTWARE
USER RESPONSIBILITY

LAW, LEGAL ASPECTS AND CONSEQUENCES
CRIMINAL ASPECTS, COMPUTER FRAUD AND ABUSE
COMPUTER HACKERS
COMPUTER STATUTES
COPYRIGHT INFRINGEMENTS
CONSEQUENCES OF COMPUTER USE VIOLATIONS

CODE OF ETHICS
ETHICAL QUESTIONS AND DILEMMAS
CODE OF ETHICS, CONDUCT AND GOOD PRACTICE
RESPONSIBILITY FOR DISSEMINATING ACCURATE INFORMATION
ASSOCIATION FOR COMPUTING MACHINERY CODE OF PROFESSIONAL
CONDUCT

ETHICS AND THE INTERNET
INTRODUCTION/DEFINITION OF THE INTERNET
PRIVATE AND PUBLIC USAGE/CONCERNS OF THE INTERNET
DOWNTIME DUE TO WORMS/VIRUSES

The following section provides a detailed discussion of the six categories. Secondly, the recommended physical feature for the computer ethics handbook or guide for Texas state employees is presented.

SETTING OF ETHICAL GUIDELINES FOR EMPLOYEES

Ethics in the public sector is a continuing issue. Most people consider themselves ethical. But at the same time ethical considerations are not always apparent to the individual. (Babbie 1995, 447). This factor may lead to ethical as well as legal consequences due to ignorance of the ethical issues involved. Some of the issues are new but in "other instances computers have merely created new version of old moral issues such as right and wrong, honesty, loyalty, responsibility, confidentiality and fairness." (Forester and Morrison 1990, 4).

In order to remedy this dilemma the public employee needs to be made aware of these ethical and legal issues. First, **ethics needs to be defined**. *Webster's New World Dictionary* defines ethics as "conforming to the standards of conduct of a given profession or group." (Babbie 1995, 448). Traditionally, ethics is defined as a set of principles of judgment and action which imposes itself upon individual conscience and collective consensus as defined by the boundaries of "the good". (Berleur and Brunnstein 1996, 4). Ethics refers to an action to be achieved and the goodness of that action. Ethics also includes ethical theory, an idea of values which differ socially and culturally. (Berleur and Brunnstein 1996, 4). The conclusion that Berleur and Brunnstein arrived at regarding ethics is that an international agreement and code on ethics is not achievable. But they n also asserts that a discussion on ethical issues in software engineering is overdue. The technicians argue that engineers must build safe techniques and users are responsible to use them safely. (Berleur and Brunnstein 1996, 52). But Berleur and Brunnstein advocate that the engineer must build products that can be used safely. Incidents such as the sinking of the Titanic and Three Mile Island are mentioned by Brunnstein as examples of

professional behavior and professional consciousness which were overruled by political and industry interest groups.

"The existence of computers-and their ability to malfunction or to be abused-has created a whole new range of social problems or issues with which we need urgently to grapple." (Forester and Morrison, 4). These social problems are listed as:

--- the unauthorized use of hardware

--- the theft of software

--- disputed rights to products

---the use of computers to commit fraud

---the phenomenon of hacking and data theft

---sabotage in the form of viruses

---responsibility for the reliability of output

---making false claims for computers

---the degradation of work

The above discussion deals with ethics definition and examples of how ethics relates to the subject of computer ethics training. In summary, the following items deal with the setting of ethical guidelines for public employees and should be included in computer ethics training in some form such as an employee handbook, employee guide, or a computer ethics training manual. (Reference Table 2.2).

TABLE 2.2 SETTING OF ETHICAL GUIDELINES
Definition of Ethics
Ethical Theory
Morality and Values
Ownership of Computer Ethics Responsibility
Need of Ethics Training

The next component is also identified by experts as necessary for computer ethics training.

PRIVACY AND CONFIDENTIALITY

Computing issues also include privacy. Privacy may be described as an important moral value. It provides the *rational context* for other concepts such as love, trust and friendship as well as respect and self-respect." (Ermann, Williams and Gutierrez 1990, 51). Privacy is also the control that individuals have over information about themselves.

The ***Privacy Act of 1974*** states that personal information collected for one purpose cannot be used for a different purpose without notice to the subject and the subject's consent. (Edgar 1997, 238). Most countries have come to a decision that private information needs to be treated as "property". This concept is supported by the different worlwide patents and copyright protection laws in existence. Due to the expanding organization which have access to personal information, this type of legal protection has been extended to private information. (Forester and Morrison 1990, 96).

Protection of the individual privacy is important. This includes protection of the client by the ***Privacy Act of 1974***. This act does include one clause--"routine use"-- that is used to expand the use and dissemination of information gathered by government sources. There currently exists a world of ***sensitive data***. Data have become a commodity because they can be bought and sold for profit. One example is the sale of an individual's address and telephone number by different private entities. There is also an increasing demand for information found in government sources. One New York article states that "for government, selling data can provide extra revenue in times of tight budgets." (Edgar 1997, 227).

In the United States there exists several professional codes which address information privacy. One of these, is the code of the Computer Professionals for Social Responsibility (CPSR). (Berleur and Brunnstein 1996, 199).[5] This code consists of the following criteria:

---

5 The essence of the code of ethics composed by CPSR was taken from the original Code of Fair Information Practices, published in the 1973 Report of the Department of

- Stop Data Misuse
- Encourage Data Minimization
- Promote Data Integrity
- Allow Data Inspection
- Establish Privacy Policies

The Code of Fair Information Practices states that to promote information privacy data misuse must be avoided by ensuring that personal information that is obtained for a specific reason should not then be used for another reason unless permission is obtained to do so. Only relevant information should be gathered and all identifiable and irrelevant information should be disposed of. To promote data integrity there must be accuracy, reliability, and completeness of information. Secret systems should not be created and must be open for amendment and correction to the individual. An information privacy policy is an essential element to be established. Privacy is valuable and as per an analogy, "It is not computers that invade privacy--people invade privacy." (Forester and Morrison 1990, 224).

In summary, the following topics deal with privacy and confidentiality and should be included in computer ethics training in some form of delivery such as employee handbooks, employee guides, or computer ethics handbook or training. (Reference Table 2.3).

TABLE 2.3 PRIVACY AND CONFIDENTIALITY

Confidentiality of Sensitive Data
Privacy Act of 1974
Protection of Clients' Information
Right to Privacy

Health, Education and Welfare. This is entitled "Computers, Records & the Rights of Citizens." The code was modified an adapted by CPSR and Privacy International. (Berleur and Brunnstein 1996, 199).

The next component identified by experts as necessary inclusion to computer ethics is computers and user responsibility.

COMPUTERS AND USER RESPONSIBILITY

Most organizations appear aware of the security risks associated with the usage of expert systems In order to safeguard customer and client information security guidelines may be set up. Private companies and state agencies have employees sign computer **security agreements**. These agreements may address the boundaries of the use of the personal computer, the confidentiality of the information available, and the responsibilities of the computer user (the employee). **Security agreements** discuss who is responsible for computer damage both software and hardware as well as penalties imposed for damage to the computers. **Security agreements** may contain a statement that the individual's **account security password** will not be shared with any other person.

While doing routine work an employee may accidentally finds a problem with security. The appropriate system manager must be notified immediately. This information is not to be shared with others. Computer users should not go looking for security problems by going where they don't belong as this could be seen as an "illegal attempt to access a computer system." (Willard 1997, 34).

To enter the computer system one needs a user code and a **password**. User codes may be the person's name, initials or some type of identification. These user codes may be easily identifiable and easy to guess. (Edgar 1997, 186). The user needs to ensure the integrity of the system by choosing a password that includes both letters and numbers. Also by choosing a different password for sites on the Internet and a user is never to share an access code or password with anyone. (Willard 1997, 31). The releasing of a password gives a non-valid user access to confidential information which is supposed to be available only to certain employees. It also gives the illegal user an opportunity to copy

files or even modify the information without restraints. This may harm or benefit other individuals or companies. (Edgar 1997, 186).

If an employee's computer is on a network, the employee must be very careful not to introduce a virus into the network.[6] The employee may avoid this by not importing programs from unknown sources, checking for viruses on new programs/files, or checking with the system administrator if the communication is questionable. (Willard 1997, 34).

"User Responsibility" implies that the user is a responsible person and has free will or the ability to make choices. Free will is an essential characteristic of an ethical system and a necessary condition for attributing **responsibility**. (Edgar 1997, 328). Those who create, use, and maintain computer systems must be responsible professionals and can be held responsible or even liable for their activities. Computer experts and users must be accountable in order to protect those with which they make agreements such as private customers or the public agency client. If the computer professionals want to be given the status, of other professions such as law and medicine, their social awareness and ethical values must be upgraded substantially. (Forester and Morrison 1990, 169).

In summary, the following items address computers and user responsibility and should be included in computer ethics written communications form such as an employee Human Resource Handbook, employee guide, or computer ethics training manual. **(Reference Table 2.4)**

TABLE 2.4 COMPUTERS AND USER RESPONSIBILITY

Security Agreements
Account Security Passwords
Access and Copying of Computer Software
User Responsibility

6 A computer virus is a program that can destroy other programs or data.

Several of the textbooks from the literature reviewed identified law, legal aspects and consequences as critical areas of computer ethics. The following section is a detailed discussion of this component.

LAW, LEGAL ASPECTS AND CONSEQUENCES

Several computer experts address the **legal aspects** of computer ethics because of its influence on how the employee should utilize the information obtained through the company's or government agency's information system.[7] A report published by the National Institute of Justice defines computer crime as "any illegal act for which knowledge of computer technology is used to commit the offense." (Edgar 1990, 150). Computer crimes are classified into different categories by different computer experts. Most of them include the following categories: internal computer crimes involving viruses, telecommunication crimes such as E-mail and illegal bulletin boards, and manipulation of computer information.

Computer crimes resemble conventional crimes. For example manipulating or falsifying information on the computer sometimes results in fraud and/or embezzlement. Other types of computer crimes are: destruction or alteration of software or data, unauthorized access to software or data, unauthorized use of computers and computer services. (Turban, McLean, and Wetherbe 1996 707).

There are computer crimes which are committed by agency outsiders, called ***computer hackers***, who are able to penetrate a computer system. The term *hacker* means different things to different people. One definition of *hacker* is "people who illegally or unethically access a computer system." (Turban, McLean, and Wetherbe 1996, 708). This definition indicates that there is a controversy among individuals regarding computer hackers. Some people believe that there is a difference between those who try to break

---

[7] Edgar 1997, 149-171; Johnson and Nissenbaum 1995, 57-147; Ermann 1990, 319-352; and Turban, McLean and Whetherbe 1996, pp. 702-712;

into computer system to create harm. Others believe that some hackers just want to break in to see if they can do it (Willard 1997, 86). Some computer ethics experts state that information is not universally free and should be considered private property because of privacy concerns. Claiming that computer information is free is looking at the situation in an unrealistic view of the world. To use this view to justify computer break-ins is clearly unethical. (Johnson and Helen Nissenbaum 1995, 128).[8]

Ethical issues and guidelines are helpful but do not deter computer crime. Subsequently **laws** have been implemented to curtail computer crimes. Deborah Johnson discusses the problem of deciding when a software developer ought to be legally liable. Current **tort law** is not applicable to new computer technology. Espionage occurs within private companies. Government agencies are susceptible to hackers and viruses. In short, it appears that there are insufficient laws to cover computer crimes which places computer systems in a vulnerable position. (Ermann 1990, 318). The following are just some of the **federal statutes** that deal with computer crime:

- Counterfeit Access Device and Computer Fraud Act (1984).
- Computer Fraud and Abuse Act (1986).
- Computer Security Act of 1987.
- Electronic Communications Act of 1986.
- Electronic Funds Transfer Act of 1980.

(Turban, McLean, and Wetherbe 1996, 707).

Another managerial issue deals with the proper use of licensed software by the employee. Companies want to get the most benefit for their money by utilizing the software wherever possible. The vendors want to make as much profit as possible by controlling and limiting the copying of a particular software. This situation creates legal

---

[8] This reference is taken from the article "Are computer Hacker Break-Ins Ethical" by Eugene H. Spafford, 1990.

questions in the area of copyrights. Laws used to be out-dated, confusing and it was not clear whether copyright, patents or trade secrets laws applied to new software technology. (Forrester and Morrison 1990 31). Currently the software is automatically covered by a federal copyright law, the Copyright Act, Title 17 of the U.S. Code. The unauthorized duplication of software is a federal crime if done "willfully and for purposes of commercial advantage or private financial gain. (Title 18 Section 231(b)." Fines may be imposed up to $250,000 along with jail terms of up to 5 years. Companies need to be careful and ensure that unauthorized copying of licensed software does not take place. (Turban, McLean, and Wetherbe 1996, 220).

The consequences of computer use violations, computer fraud and abuse, copyright infringements, or criminal aspects have consequences. Illegal duplication may entail fines and jail terms. Deliberate attempts to cause disruptions or corruption of computer system by spreading a computer virus is considered criminal activity under state and federal laws. (Willard 1997, 34).

In summary, computer ethics experts address the following items as critical to law, legal aspects and consequences and should be included in computer ethics training in a written communications form such as an employee Human Resource Handbook, employee guide, or computer ethics training manual. (Reference Table 2.5)

TABLE 2.5 LAW, LEGAL ASPECTS, AND CONSEQUENCES

Criminal Aspects, Computer Fraud and Abuse
Computer Hackers
Computer Statutes
Copyright Infringements
Consequences of Computer Use Violations

A code of ethics is another area identified by experts as necessary to computer ethics.

CODE OF ETHICS

There are several **ethical questions** and issues that computer users and computer professionals encounter. One question is whether information on individuals which is stored in a computer is an invasion of privacy. Another deals with potential computer crimes like copying software or hacking. Is copying software or hacking a computer really a form of stealing and burglary? Viruses and Internet worms which disrupt or damage computer systems are considered as crimes by some but not by others. Making false claims about computer software is also considered to be a crime by those who feel misrepresenting computer capabilities is not ethical. The main question is whether computer professionals should be bound by a **Code of Conduct**. What should this **Code of Conduct** or **Ethics** include?

Several computer ethics experts such as Forrester, Morrison, Johnson, Nissenbaum and Edgar make references to a code of conduct and a computer ethics code. The Code of Conduct presented by the **Association for Computing Machinery (ACM)** is one. (Reference APPENDIX B). Other organizations mentioned who have codes of conduct or ethics are The Institute of Electrical and Electronic Engineers (IEEE) and the Data Processing Management Association (DPMA) both have a code of ethics. (Reference Appendix E). The International Federation for Information Processing (IFIP) also developed a code of Ethics. The computer guidelines developed to guide the computer user called The Ten Commandments is a very clear and to the point guide. It clearly states what a computer user should not do. (Reference APPENDIX F.)

Deborah Johnson compares the status of computer experts to the status of engineers. Computer experts usually work in teams and on small segments of large projects. Like engineers, Johnson states, computer experts have four obligations: to society; to their employers; to their clients; and to co-professionals and even professional organizations.

The following table summarizes ethical topics to be included in computer ethics written communications is some form of handbook or guide such as the Human Resource Handbook, employee guide, or computer ethics training manual. **(Reference Table 2.6)**

TABLE 2.6 CODE OF ETHICS

Ethical Questions and Dilemmas
Code of Ethics Conduct and Good Practice
Responsibility for Disseminating Accurate Information
Association for Computing Machinery Code of Professional Conduct

Another important section which has a continuously growing user population is the Internet. Ethics and the Internet is identified by experts in this area as relevant to computer ethics.

ETHICS AND THE INTERNET

The literature reviewed addressed ethics as applicable to the realm of the Internet. The Internet is one of the biggest most widely used wide-area networks in the world. It is not owned or regulated by a private commercial carrier. Because it is used by millions, the Internet is referred to as "the superhighway" of worldwide information. (Turban, McLean, and Wetherbe, 1996, 311). The Internet is defined as "the global network of networks that all speak the same language known as TCP/IP. (Willard 1997, 87)[9] The Internet is a self-regulated network of computer networks connecting over 25,000 networks with over 2.5 million computers and 25 million users in 1994. (Turban, McLean, and Wetherbe 1996, 518).

---

[9] Willard also defines TCP (Transmission Control Protocol as the protocol that ensures data transmission is complet, error-free, and in the proper sequence. IP (Internet Protocol) is the protocol or rules that control how data is routed between hosts on the Internet.

The Internet has several time saving and expedient communication uses. It may be used in E-mail functions, news groups-electronic bulletin boards, mailing lists, and access to remote computers. It may also be used in business activities such as making reservations, remote log in with interactive sessions, and accessing databases and browsing. (Turban, McLean, and Wetherbe 1996, 518).

By providing access to the Internet management may create ethical decision- making situations for the employee. Ethical and privacy issues may surface when utilizing E-mail. One issue is the matter of invasion of privacy of the user who may be monitored. The other issue is the use of E-mail for personal usage which may mean wasting company time. The right of free speech may allow inappropriate material to be communicated to others. The security of communication is questionable because data being transmitted is placed in jeopardy. In both private and public organizations the integrity and privacy of the information may not be protected. (Turban, McClean, and Wetherbe)

A "worm is a computer program that infests a network environment and copies itself repeatedly." (Willard 1997, 96). When an individual is on a network, there exists a responsibility to make sure that a computer worm or virus is not introduced into the network. An example of a worm program is the Internet Worm which was released on the ARPANET on November 2, 1988. The worm reached 2,500 to 3,000 computers. and created thousands of copies of itself. These copies clogged the systems they invaded and they became nonfunctional causing a loss of about $1 million due to computer down time. The Computer Professional for Social Responsibility issued a statement which condemned the action. Furthermore, they encouraged the teaching of ethics in the computer community. A point was made that when this type of "worm" occurs it clearly shows "our increasing dependence on computer networks.". (Edgar 1997, 195).

Below is a summary of elements that computer experts identify as essential to computer ethics and should be included in the employee Human Resource Handbook, employee guide, or a computer ethics training manual. **(Reference Table 2.7)**.

TABLE 2.7 ETHICS AND THE INTERNET

Introduction/Definition of the Internet
Private And Public Usage/Concerns of the Internet
Downtime due to Worms/Viruses

For a presentation or training on computer ethics to be successful the trainer and the content must be organized. One of the tools that can be utilized by the trainer may be the Human Resource Handbook, the employee guide, or the computer ethics handbook. Whatever training tool is chosen it must be organized and have relevant content.. The following is a summary of the handbook model presented by Rebecca Short in her 1997 Applied Research Paper, Content Analysis of State Agency Employee Handbooks.

PHYSICAL ATTRIBUTES

In her Applied Research Project, Short addresses the following attributes as important to an organized, useful and effective employee handbook. These attributes would also apply to computer ethics.

Format and Design

Handbooks must be kept current and therefore a loose-leaf ring book is recommended. The second option is a spiral binder because the spiral may be removed to update the handbook. Organizations are more likely to revise these type of handbooks. Adding or deleting individual pages is easier and less costly. The design of the computer ethics handbook is important. Short notes that subheadings, bullets, and plenty of white space assist in making the handbook readable and interesting.

Dated Pages

Annual updates on computer ethics handbooks or guides is recommended. These updates will reflect the current year and ensure that current employee guidelines are included.

Removable Acknowledgment Statement

An acknowledgment statement needs to be included in the handbook, guide, or training manual. The signed statement may then be filed in the employee's personnel folder.

Writing Style

The handbooks have important information and it is difficult to maintain the interest of the employee. Through her readings in the literature review, Short derived the following writing style factors to be utilized in the handbooks.

- Language should be kept clear and simple
- Legal jargon should be avoided whenever possible
- Policy statements should be direct using everyday terms
- Paragraphs and sentences should be kept short

The recommended physical attribute standards of Human Resource Handbooks, employee guides, and computer ethics training manuals are listed below. **(Reference Table 2.8).**

TABLE 2.8 PHYSICAL ATTRIBUTES STANDARDS

Format and Design
Dated Pages
Acknowledgment Statement
Writing Style

The literature reviewed, the conceptual framework for this Applied Research Paper, and the recommended components of computer ethics documentation/handbooks have been presented in this chapter. The methodology involved in analyzing Texas state agency employee computer ethics written communications will be discussed in Chapter 3.

CHAPTER 3

RESEARCH SETTING AND BACKGROUND

Introduction

As mentioned earlier in this study, Computer Information Systems are an important part of the present and the future. There all types of personal computers being used in the public sector and this usage continues to grow. Statistics recorded in 1997 indicate that there are 1,915 national level government agencies worlwide with Web sites. The United States is leading all countries with 205 agencies on line. (Menzel 1998, 445) In the United States more than 2,500 governments agencies have Web sites. The justification for expanding web sites and making them available to state employees is routinely stated as: improvement of client services, faster dissemination of information, and cost effective use of time and resources.

Setting

Providing access to the Internet has created many ethical and management challenges. It has also raised questions regarding the consequences of establishing web sites for the government employees. For instance, in Texas questions have been raised about the possible misuse of the state government and the possible legal consequences not only for the employee but also for the agency. State employees have had access for some years to driver licenses and automobile registrations in Texas. But recently a private firm in Dallas placed information in an accessible data base on the Internet. An individual who has a driver's license, a computer, and an Internet server has the capability of researching Texas license plates and other Texans. The site will be expanded in the future and information about arrests and convictions, marriage records and voter registrations may be readily available. (Menzel 1998, 450).

As a result, there are questions about Internet access for state employees. Is access to such information ethical? Is it legal? Another concern is the selling of information gathered from government data bases. In brief, is it ethical to create data bases that can be searched and information gathered regarding one's private information and property? Most important what type of training is being conducted for Texas state employees in the area of computer ethics?

Since there are so many unanswered questions and new issues regarding computer ethics, there is not a really consistent way of communication information to state employees. Most agencies do not typically have a standardized way of presenting computer ethics guidelines to their staff. The agencies may have information in different types of written communications such as human resource handbooks, employee guides and other informal forms of written communication.

Background

In the Spring of 1995 Sheri Jones, in order to complete her Master's degree program, conducted a study on ethical awareness related to the use of computers. A review of the student body in the Master's of Public Administration program at Southwest Texas state University was completed. In 1995 David Trevino, another MPA student conducted a study of the Department of Public Works for the City of Austin. Then in 1996, Gary Coe, also and MPA student did a study on ethical awareness of the members of the Texas Association of State Systems for Computing and Communication, Inc. All three studies arrived at the conclusion that computer ethics training needs to be a major part of a state employee's training. They concluded that overall the higher the education of an individual the higher the ethical awareness the individual possesses. (Coe 1996, 31.) It is this aspect that can lead to the conclusion that computer ethics education is also very important. There are different methods that may be used in educating the state employee in computer ethics. Computer ethics may be presented through training sessions. Another method is through written communications on computer ethics such as handbooks, personnel guides,

or computer ethics manuals. This second method of disseminating information to state employees is being explored in this research.

APPROACHES AND METHODS TO DISPERSING INFORMATION INTEGRITY

In order for employees to understand the basis for computer ethics guidelines, they must first have an understanding of ethical expectations for state employee. Consequently, administrators of state agencies should create a computer ethics plan for disseminating computer ethics. They may first need to look at their own agency's ethics handbooks. If such handbooks do not exist, they could refer to the Texas State Ethics Commission and review the ethical outline documented and proscribed by the Texas lawmakers and other related ethical materials.

The Texas Ethics Commission is an oversight agency that ensures state employees follow requirements. The commission has the authority to issue advisory opinions, subpoena records and witnesses at formal and informal hearings. It also has the authority to fine state employees for disclosing confidential information regarding commission activities. Commission ruling may be appealed in court. However, these rulings cannot be used as evidence during the court appeal process.

The Texas Ethics Commission was created and signed into law on June 7, 1991. Article 6252 of Human Resource Code is a guide to ethics laws for state offices and employees. It specifies standards of conduct of state offices and employees. Article 6353-9d, Vernon's Texas Civil Statutes requires the Texas Ethics Commission to provide ethics training for all state employees--a time frame is not specified. The Ethics Commission has only one full time ethics trainer. (Bryan Jones 1995, 5). The Texas Ethics Commission's training seminar consists of the following parts (Jones 1995, 27).

- Respect for State Property
- Why Ethics in Government
- Appearance

- Consequences
- Conception of Ethics
- Definition of Ethics
- State Property; the law, key words, self guiding steps
- Gifts, the principles; the NO NOs
- Public Trust

In his applied Research Project, Bryan Jones gave a description of how ethics training should be conducted and gave an overview of the contents of that training. Bryan stated that the following conditions need to be present for an effective ethics training:

1. Designer of ethics programs need to be aware of how such an initiative will be perceived by others.
2. The goals are made very clear to those involved.
3. Commitment to ethics training by top management is essential
4. The training is different fro technical and management training

For computer systems to have safe and accurate information, it is essential that programming, hardware security, software security, and all encryption are created with integrity factors in mind. The end user also has responsibility for keeping information and data integrity. It is difficult to audit individual users to see how they protecting the security and integrity of spreadsheets and other data. Making employees aware of information integrity issues from the beginning ensures that good systems will be built from the outset in future computer innovations. A fundamental part of this approach would be the way system developments is taught to students. Students are taken through the complete system development cycle. It is very important that employees are aware of all the implications of the technical skills they are learning. For example, one University's approach provided and integrated system to teaching methods of technical skills. (Clipsham 1997, 1). The focus is in three areas:

1. Accuracy of data and information encompassing issues of fidelity and accuracy

2. Security and computer misuse issues

3. Ensuring social values are properly addressed

In addition this university developed ethical and human factor guidelines which are made available to all undergraduate students who take information systems and computing courses. The training curriculum includes issue of security, the law and social impact of information system and technology. This provides an ethical framework for the development of the students or the "end user " of information systems.

Disseminating Computer Ethics to State Employees

A review of Bryan Jones guidelines for ethics training and the computer ethics training agendas indicate that computer ethics curriculum needs to be well organized and documented. One form of communicating this information would be through written communication documents which may include Human Resource Handbooks, employee guides, or computer ethics handbooks. It is through documentation of computer ethics guidelines that state employees may be trained efficiently and effectively.

ETHICAL ISSUES AND THE TEXAS DEPARTMENT OF HUMAN SERVICES

This chapter discusses The Texas Department of Human Services (DHS) in order to give a specific example of how computer ethics is an important aspect of current state business. DHS is a state agencies that deals with thousands of clients who receive all types of public services--ranging from food stamps to some type of medical assistance. Consequently, DHS employees have access to individual's personal and economic information. This agency has a technology information computer system that encompasses programs such as Food Stamps, Temporary Assistance Program (TANF), Long Term Care, Medicaid Eligibility and others. In order to ensure the integrity of the programs, DHS has employee sections that review or investigate the quality of the client's casework. The computer is the instrument used to review referrals by gathering

information from other agencies. Computer matching is done extensively and all types of confidential information may be gathered through the use of the client's Social Security number.

New DHS employees must go through an orientation conducted by the Human Resources Department (HRS). HRS conducts the orientation on the employees first day of employment. One item on the agenda deals with computer usage and security guidelines. The new employee reads, signs and dates the Computer Security Agreement. By signing this document the new employee is agreeing to follow all confidentially rules and guidelines. A copy of the agreement is given to the employee and the original is kept by the HRS officer. All employees are made aware of the Privacy Act of 1974. This is the one law that an employee has to know and understand. It is also made clear to them that client confidentiality has to be maintained and if one deviates from this there are severe penalties for divulging information incorrectly. The penalties may range from oral reprimands to suspension, up to and including dismissal.

Ethics guidelines are found in the Human Resource Handbook. (TDHS Human Resources Handbook 1992, Section 7100). These guidelines provide a framework to be followed by employees as well as a guide when dealing with ethical dilemmas in the workplace. Some of the guidelines are:

1. Perform all duties with competency and remain open to new ideas and training
2. Avoid the appearance of favoritism, prejudice/undue influence/ or impropriety
3. No acceptance or soliciting of gifts, favors, service, etc. from anyone in exchange for performance and/or information
4. Maintain appropriated confidentiality--with DHS information or other dealings
5. Avoid situations where conflict of interest may occur
6. Protect and do not destroy, remove, conceal, or misuse state information or property (i.e. computers).

All employees have the responsibility of helping their fellow DHS empties and the public understand the department's ethics guidelines. They need to seek advice if uncomfortable with some issue or have questions about issues related to work and computer ethics. The training given to DHS employees usually contains one specific point. *"When in doubt--don't do it!"* (DHS Ethics Training 1994).

The HRS Handbook also has laws that govern ethics and standard of conduct including an Ethics Code, TEX. GOVT. CODE ANN. 572.051, Section 7131. According to this code and employee cannot accept employment, do business, or conduct an activity that requires the employee to disclose confidential information. This, of course, applies To all client information regardless of the source paper case records or computer records. The Penal Code provides penalties for certain offenses involving public administrators. TEX. PEN. CODE ANN. 3.08-36.10.(TDHS HRS, Ethics Code, Section 7131, 1996) defines a benefit as "anything reasonable regarded as pecuniary gain or advantage, including benefit to any other person in whose welfare the beneficiary has a direct and substantial interest." A DHS employee is considered to have committed a class A misdemeanor if he/she commits such offenses. On the other side, a private citizen is also held liable for tying to influence or bribe the public official and is committing a class A misdemeanor when she/he/she offers, confers, or agrees to confer any benefit on public servant they know it is illegal.

Overall there is good written documentation on "ethics" and training is provided sporadically. But, any further presentations regarding computer ethics must be done by the employees direct supervisor. There are no written guidelines that address issues and problems concerning computer ethics. There are some computer security forms that an employee must sign before obtaining computer permissions to specific computer information but these are not forms found in one standard handbook.

All DHS employees at all levels are periodically reminded through computer broadcasts (E-Mail), in memorandums, and unit meeting agendas that information found

on the computer is not to be divulged to anyone without a valid work reason and only for work purposes. Computer ethics guidelines are not documented in any standardized form of documentation. A handbook or some type of written communication with computer ethics guidelines is needed in DHS.

CHAPTER 4

METHODOLOGY

The first step of this project was to evaluate the pertinent literature addressing computer ethics. The review included textbooks, journals, periodicals, and Internet sources relevant to computer ethics. Recommended characteristics of computer ethics were identified through the literature review.

Content Analysis

The technique chosen to address the purpose of this research is content analysis of agency documents. To fulfill the purpose of this research, a document content analysis was conducted on state agency policies and procedures dealing with computer ethics. Earl Babbie (1995, 306) refers to content analysis as unobtrusive methodology that uses direct observation of documents. The research purpose was performed using content analysis of current Texas state agency employee handbooks and other formal written communications. The handbooks reviewed consisted of the Human Resource Handbook, Ethics Handbooks, and Automation Handbooks. All other written communication documents provided by the agencies were also reviewed. These documents were used because the contents are routinely used to conduct presentations and training for new and tenured staff regarding personnel matters including legal and ethical aspects.

Through content analysis information was gathered on the characteristics found in public sector computer ethics including training programs of Texas government agencies. This method of information gathering furnishes information to ***describe*** the characteristics found in public sector computer ethics training's. According to Babbie (1995, 305) a content analysis is a social research method appropriate for studying human communications process and other aspects of social behavior. Content analysis allows

researchers to examine a class of social artifacts, typically written documents. (Babbie 1995, 306). The usual units of analysis in content analysis are units of communication such as words, paragraphs and books (Babbie 1995, 335). Weber (1985) identifies content analysis as a "research methodology that utilizes a set of procedures to make valid references from text" (1985, 9). Therefore content analysis may be used to examine computer ethics policies and procedures as well as training documentation modules and forms.

Strengths and Weaknesses of Content Analysis

Content analysis has strengths and weaknesses. It has advantages and disadvantages in terms of validity and reliability. One advantage of content analysis is the fact that research staff is kept minimal and no special equipment is needed. Thus, making this type of research economical. Regarding research repetition, safety is another advantage. If an error is made in content analysis research, it may be readily remedied by repeating the portion in question of the study. Another advantage is that it permits historical studies and comparisons. Content analysis is unobtrusive and seldom has any effect on the subject being studied. (Babbie 1995, 306-307).

One potential disadvantage of content analysis is that it relies implicitly on one single researcher to construct the appropriate categories for which there is empirical data. Another disadvantage is that content analysis is limited in the analysis of recorded communications such as written, graphic and oral. (Babbie 1995, 320). There may also be potential problems with the validity of the content analysis. Therefore, in order to enhance the validity and reliability of the results, manifest and latent content analysis was used.

Population

The State of Texas leads the nation with 134 agencies on line. (Menzel 1998, 445). The setting for this research focuses on Texas state agencies and how computer ethics

training is presented and utilized. In this research study 35 state agencies were contacted by written correspondence and 32 responded. Refer to **Appendix D** for a list of the population included in the sampling frame. The State of Texas has a total of 155 agencies. (http://www.state.tx.us/agency/agencies.html September 1998.).

Specifics of the Methodology--Statistical Analysis

The unit of analysis is the written information such as handbooks, employee guides or other formal documents. Upon receipt of the information requested a coding scheme sheet was developed to track the frequency of each of the categories pertaining to each component. The information obtained on each code sheet provided information gathered through numerical data. This data is summarized and explained in the following chapters through the use of charts, tables and narrative summaries. The statistics are descriptive.

A document coding scheme was used to rank the various computer ethics documents. The coding procedure used "include" (yes or no) to assess if the ideal characteristics are included in the documented policies and procedures for computer ethics training. A coding sheet was prepared for each agency's policies and procedures. **Appendix C** depicts the coding scheme developed from the research conducted. **Appendix G** represents the results derived from the document content analysis. The *"degree"* to which the characteristics were addressed were assessed. Degree represents the number of lines dedicated to each item. The information gathered was calculated in order to determine the average number of lines on each of the characteristics. An effective written communication tool could then be determined. **Reference Figure 4.1.**

A full discussion of the sample analysis follows. The frequency of each answer determined whether or not a consistent method of documentation was used by state agencies in the dissemination of computer ethics information, policy and procedures.

FIGURE 4.1 - RESULT TOTALS

CODING PROCEDURES FOR CONTENT ANALYSIS OF COMPUTER ETHICS DOCUMENTS

State Agencies _____

State Agency Responses _____ % _____

ELEMENTS	INCLUDED		
	#Yes	#No	Line Average
SETTING OF ETHICAL GUIDELINES			
1. Definition of Ethics			
2. Ethical Theory			
3. Morality and Values			
4. Ownership of Computer Ethics Responsibility			
5. Need of Ethics Training			
COMPUTER PRIVACY AND CONFIDENTIALITY			
1. Confidentiality of Sensitive Data			
2. Privacy Act of 1974			
3. Protection of Clients Information			
4. Right to Privacy			
COMPUTERS AND USER RESPONSIBILITY			
1. Security and Security Agreements			
2. Account Security Passwords			
3. Access and Copying of Computer Software			
4. User Responsibility			
LAW, LEGAL ASPECTS AND CONSEQUENCES			
1. Criminal Aspects, Computer Fraud and Abuse			
2. Computer Hackers			
3. Computer Statutes			
4. Copyright Infringements			
5. Consequences of Computer Use Violations			
CODE OF ETHICS			
1. Ethical Questions and Dilemmas			
2. Code of Ethics, Conduct and Good Practice			
3. Responsibility for Disseminating Accurate Information			
4. Association for Computing Machinery Code of Professional Conduct			
ETHICS AND THE INTERNET			
1. Introduction/Definition of the Internet			
2. Private and Public Usage /Concerns of the Internet			
3. Downtime and Damage Due to Worms/Viruses			
PHYSICAL ATTRIBUTES STANDARDS			
1. Format and Design			
2. Dated Pages			
3. Acknowledgment Statements			
4. Writing Style			

CHAPTER 5

RESULTS AND ANALYSIS

Introduction

This chapter presents the organized results obtained from the document analysis. A narrative description of the findings is being used to describe the computer ethics written communication documents available to Texas state employees. In addition, data gathered during the content analysis are organized in this chapter. Through the use of tables and narrative summaries the research results are revealed. These coding results were utilized to assess manifest content. The results present a picture of 32 Texas state agencies' computer ethics handbooks and other written information and their relationship to the proposed ideal type.

Data Results and Analysis

SETTING OF ETHICAL GUIDELINES

The Human Resource Handbooks, automation handbooks/guides and/or computer ethics information exhibit a lack of emphasis on computer ethics. Only two agencies define specific criteria to be followed by employees to maintain ethical computer usage. Other agencies with references to computer issues do not address ethics or if addressed did not define it. The state agency handbooks, guides, and automation manuals do not adequately address or define computer ethics. Ethical theory, morality and values are also not defined or reviewed. The need for computer ethics training was not addressed in any of the handbooks, guides and manuals reviewed. Overall the 32 agency's handbooks reviewed in this content analysis fail to address the elements recommended for the ideal type.

TABLE 5.1 SETTING OF ETHICAL GUIDELINES

Categories	Yes	No	Average Lines
Definition of Ethics	2	30	2
Ethical Theory	0	32	0
Morality and Values	1	31	1
Ownership of Computer Ethics Responsibility	0	32	0
Need of Ethics Training	0	32	0

COMPUTER PRIVACY AND CONFIDENTIALITY

The Privacy Act of 1974 was enacted to protect individuals personal information. The 32 agencies reviewed through this study did not specify this federal law in their personnel handbooks, employee guides or other written forms of communication. Only a few agencies did address the confidentiality of state data and how this cannot be given out without the written consent of the proper agency staff person. A minimal number stressed the protection of client information. These agencies made clear that without the client's consent individual client information could not be given to anyone.

Overall these agencies covered an individual's right to privacy by setting rules on the protection of the agency and client information data. But the Privacy Act of 1974 was not reviewed or documented. According to the literature reviewed this Act is very important to the question of privacy and computer confidentiality. The Privacy Act is a federal law and important to the individual privacy rights. According to the ideal type of computer ethics information training this should be a primary resource for all state agencies and their employees when faced with information dissemination.

TABLE 5.2 COMPUTER PRIVACY AND CONFIDENTIALITY

Categories	Yes	No	Average Lines
Confidentiality of Sensitive Data	8	24	5
Privacy Act of 1974	0	32	0
Protection of Clients Information	5	27	2
Right to Privacy	0	32	0

COMPUTERS AND USER RESPONSIBILITY

One of the most basic needs of the public employee is to be informed about the agency they are working for. By knowing the rules and regulations of the agency specifically in the area of computer use, the employee will be a low risk productive staff person. About a fourth of the state agencies have rules and guidelines regarding computer security and security agreements. It is through these security agreements that the agencies present work rules to the employees regarding the usage of the computer for business purposes. The computer user is subject to the statements found in the security agreement . None of the state handbooks, guides or computer manual reviewed addressed the question of copying computer software.

User responsibility was not stressed. Topics like making sure that the information obtained does not harm others or ensuring that the information obtained was not infringing on someone's right as an individual was not discussed. Copying computer software and given or selling it to a third party was not reviewed. The agencies did include the security agreements which contain language and phrases to make the user aware that they must use the computer and the information gathered in a proper and confidential manner. A fourth of the agencies dwelled on the importance of not sharing computer passwords with anyone else.

TABLE 5.3 COMPUTERS AND USER RESPONSIBILITY

Categories	Yes	No	Average Lines
Security and Security Agreements	7	25	10
Account Security Passwords	6	26	7
Access and Copying of Computer Software	0	32	0
User Responsibility	3	29	3

LAW, LEGAL ASPECTS AND CONSEQUENCES

Of the 32 agencies reviewed, none of them addressed copyright infringements or laws. There were only a minimal number of agencies that specifically addressed the consequences of computer use. One agency discussed the consequences and listed them under the subheading "Violations". This section specifically addressed that violation of computer use could result in some type of reprimand, loss of computer usage, transfer to another section, or termination from the agency. In this same section the agency also stressed that certain violations could possibly be subject to personal civil or criminal liability.

Unauthorized disclosure and breach of Computer Security was thoroughly reviewed by this group of agencies. Training in this area was briefly mentioned. However the training was incorporated in the employee handbook and was to be read by the employee. Some of the other agency's guides also reviewed the consequences of computer user violations and related them to breach of confidentiality. A warning was found in one guide stating that unauthorized disclosure of confidentiality was punishable under state and federal law and could result in dismissal from the agency.

In summary, the handbooks, guides and training material reviewed did not contain any references to computer hackers, fraud, and other criminal aspects relevant to computer technology. The laws pertaining to computer abuse and fraud were not listed or explained.

Surprisingly, copyright infringements were not covered in any of the materials reviewed. The laws dealing with copyrights of software were not mentioned. Even though, the mechanics of Security guidelines are explained, such as not sharing passwords, the actual statutes are not listed. The one brief discussion on training regarding law and consequences indicated that there is no formal consistent training in the are of law, legal aspects and consequences. The written documents were not consistent in their presentation and format.

TABLE 5.4 LAW, LEGAL ASPECTS, AND CONSEQUENCES

Categories	Yes	No	Average Lines
Criminal Aspects, Computer Fraud and Abuse	0	32	0
Computer Hackers	0	32	0
Computer Statutes	0	32	0
Copyright Infringements	0	32	0
Consequences of Computer Use Violations	5	27	6

CODE OF ETHICS

None of the agencies reviewed referenced a code of ethics for their agency's computer users. The appropriateness of using computer information correctly and with ethical practices were not addressed. The 10 Commandments of computer usage were not mentioned or alluded to in any form. The Code of Ethics for the Association for Computing Machinery Code of Professional Conduct was not found in the agency handbooks, guides and other written materials reviewed.

As per Rebecca Short's ARP "it is evident that state agencies are taking a positive step to address the public's concern regarding ethical issues in public sector employment." However, upon completion of this content analysis, it is evident that a computer code of ethics is not a part of the computer materials that are used in informing and training of Texas state employees. Since a code of ethics is an essential component of the ideal type the lack of one indicates a weakness in the effectiveness of the computer ethics training conducted by the state agencies.

Overall the Texas state agencies do not appear to have a Code of Ethics for computer users or computer programmers This lack of a Code of Ethics, or at a minimum references to existing codes, minimizes the validity of the computer ethics training conducted by the state agencies.

TABLE 5.5 CODE OF ETHICS

Categories	Yes	No	Average Lines
Ethical Questions and Dilemmas	0	32	0
Code of Ethics, Conduct and Good Practice	0	32	0
Responsibility for Disseminating Accurate Information	0	32	0
Association for Computing Machinery Code of Professional Conduct	0	32	0

ETHICS AND THE INTERNET

The fact that the Internet is a growing phenomenon of business and personal communication makes it a priority form of communication for the state administrator. Yet the information reviewed for the state agencies do not have substantial information on the Internet. One agency does have one complete manual on usage of the Internet which included an introduction, a definition of the Internet, and defined the guidelines for the employee who utilizes the Internet. It also included material explaining damage due to viruses.

In another agency the use of the Internet or any public network is discouraged until the security of the networks is more reliable. It explains that until sophisticated hardware and encryption software is in place Security staff cannot ensure non-access by a third party to confidential and mission-critical information.

It is difficult to comprehend why the materials submitted for the content analysis do not include many references to the Internet. Less than a fourth of the agencies reviewed addressed the Internet. The agencies who did address the Internet are very thorough and have detailed instructions and guidelines. Overall the documents reviewed indicated there is a lack of information sharing or training regarding the Interment and the related concerns.

TABLE 5.6 ETHICS AND THE INTERNET

Categories	Yes	No	Average Lines
Introduction/definition of the Internet	6	26	7
Private and public usage/Concern of the Internet	6	26	7
Downtime and Damage Due to Worms/Viruses	4	28	8

Conclusion

The content analysis of 32 Texas state agency's written form of communication such as Human Resource Handbooks, employee guides, automation manuals and other computer ethics material illustrated failure to appropriately and consistently disseminate computer ethics information to the state employee. The data indicate that computer ethics training for state employees is narrow in scope and limited to only a few agencies. In summary, results of the content analysis is dependent on the type of documents provided by the state agencies. Based on the questions received from agency information specialists and legal departments, there seems to be a reluctance on the part of several agencies to share computer ethics information or to admit to the lack of such information. Future researchers may need to contact more Texas state agencies and focus even more on the actual computer ethics presentations or classroom training.

CHAPTER 6
SUMMARY AND CONCLUSION

This chapter presents a summary of the research results. It also identifies whether the ideal components derived from the literature are found in the state employee handbooks and other documents used to disseminate computer ethics information to state employees. In this chapter policy and procedure recommendations for computer ethics handbooks are made and an ideal type of training handbook is proposed. Also in this chapter will be found research limitations and weaknesses.

Purpose of the Research

This research project was conducted for three purposes: 1) to describe the ideal characteristics of effective computer ethics written communications gathered through a literature review 2) to assess the information contained in the public sector handbooks and compare the computer ethics communication documents used by Texas state agencies with the ideal type described 3) to make recommendations to improve computer ethics written communications found in Texas state agencies.

Research Weakness

This study includes a content analysis of 32 state agencies' employee handbooks, employee guides, and computer ethics manuals. The review of the documents clearly indicate the lack of emphasis on computer ethics and information dissemination or training of state employees. Since this analysis is based on the information provided by the state agencies in a variety of employee handbooks and guides, it may prove beneficial to continue gathering additional information of other state agencies with a more narrow focus on computer ethics written materials used by administrators, personnel officers or

trainers to educate employees in the area of computer ethics. In addition to content analysis, a more detailed research on written forms of computer ethics will be achieved by adding surveys and interviews of state agency administrators and training staff.

OVERALL SUMMARY AND RECOMMENDATIONS

Component: **Setting of Ethical Guidelines**

The research clearly indicates that there is insufficient information or training in the setting of ethical guidelines. The categories suggested in **Table 5.1** were not included in the majority of the state agencies documents. More emphasis is needed in this area. Public sector employees should develop computer ethics guidelines, and ensure these are documented and verbally presented to state employees preferably in a training setting.

Component: **Computer Privacy and Confidentiality**

This component does exist in some of the state agency handbooks and guides reviewed. However, the practical ideal type standard as represented in **Table 5.2** is not met. More emphasis needs to be made on this component. The characteristics in this component needs to be documented and made a part of an employee's computer ethics handbook as well as the training material.

Component: **Computers and User Responsibility**

This component contained more information than any other component. Security rules and Security Agreements are found documented and explained. The four categories found in **Table 5.3** appear to be important to public administrators since they specifically address these characteristics in the handbooks reviewed These categories include security guidelines, security agreement forms, rules on confidentiality of passwords, and computer user responsibility. One exclusion noted is access and copying of computer software which is a very important characteristic of computer ethics. In summary, more

emphasis is needed on computer user responsibility with extensive explanation on why this aspect is critical to the employee's job status. Documenting this in one uniform computer ethics handbook would avoid future problems in this area.

Component: **Law, Legal Aspects and Consequences**

More emphasis should be placed on the issue of law, legal aspects and consequences of not following laws and guidelines. The few state agencies that address this area are limited in their discussion of the component. The characteristics found in **Table 5.4** should be addressed and thoroughly discussed in a computer ethics handbook. State employees could be exposed to an intensive review of the law and legal aspects in a classroom setting. It is recommended that the tool used to present this type of training should be a statewide standard computer ethics manual. Emphasis for this component should be on probable consequences due to violations of computer laws. These consequences could involve an oral reprimand up to and including dismissal from the agency. In addition, employees need to be aware that certain violations could lead to imprisonment.

Component: **Code of Ethics**

This is another component that does not meet the standard for the ideal type. As per **Table 5.5**, a computer code of ethics is an essential part of the ideal computer ethics handbook. This code of ethics should include computer ethics guidelines for ethical practices and ethical conduct when employing computer technology systems. None of the agencies reviewed emphasized a code of ethics for computer user. Emphasis should be placed on reviewing established codes of ethics or in creating an agency's computer code of ethics. In summary, the established code of ethics should be placed in a uniform computer ethics state employee handbook. It is also recommended that the code used by several computer ethics advocates, the Association for Computing Machinery Code of Professional Conduct, also be included in the computer ethics handbook.

Component: **Ethics and the Internet**

The number of agencies that covered this component were minimal. Overall the standard illustrated in **Table 5.6** for the ideal type was not met. Internet ethics should include a description and definition of the Internet and how the private and public use the Internet. Next the concerns surrounding the use and attributes of the Internet need to be addressed.. The consequences and damage caused by viruses and Worms should be explained and documented in the statewide uniform computer ethics handbook.

CONCLUSION

The literature reviewed, the content analysis and the results indicate that there is no one consistent method of disseminating computer ethics information to state employees. The results of the analysis indicate that computer ethics information is also not found in one standard written communication tool. Out of all the agencies written communications reviewed only about three agencies had some type of effective written communication. Most of the agencies written communication was fair to poor in quality of the document used..

A uniform computer ethics handbook for state employees could be used as the main resource by the training division of each state agency. This would ensure that all state employees are given uniform acceptable information and guidelines regarding computer ethics. This type of handbook would be cost effective for the public administrators. By educating the public sector employee on these components in computer ethics, public sector management may prevent or reduce the liabilities incurred due to computer user violations. In the end the state employee, the state agency, and the clients serviced by the agency will benefit from an effective computer ethics written communication tool.

BIBLIOGRAPHY

Babbie, Earl. The Practice of Social Research, Belmont, California: Wadsworth Publishing Company, 1995.

Barger, Robert N. "Computer-Ethics," Philosophical Bases of Computer Ethics, October 25, 1995, 1.

Barger, Robert N. "In Search of a Common Rationale for Computer Ethics," April 28, 1994, 1.

Belohlav, Jim, and David Drehmer. "Ethical Issues of Expert Systems," The Online Journal of Ethics, October 1997, 1.

Berleur, Jacques, an Klaus Brunnstein."Ethics of Computing", Chapman and Hall, Bardary Row, London, 1990, 1-19.

Burke, James. "The Process of Change," Government Technology. February 1998, Vol 11, 13.

Clipsham, Phil. "Teaching Information Integrity-an ethical approach", Center for Computing Social Responsibility, p.s.clipsham@greenwich.ac.uk 1

Coe, Gary A. "Computer Ethics: An Ethical Awareness Study of the Members of the Texas Association of State Systems for Computing and Communications, Inc.," Applied Research Project, Summer 1996, SWTSU.

"Computer Ethics", Available RTPnet Home Page www.Rtpnet.or/newuser/ethics.html. September 1997, 1.

Computer Fraud and Abuse Act of 1986.

Computer Security Act of 1987.

"Cookies: what they are and how they work", Support Tech Support, Netscape Communications Corporation, 1998, http:help.netscape.com/kb/client/970226-2html

Counterfeit Access Device and Computer Fraud Act of 1984.

Duncan, George. "Is My Research Ethical?," Communications of the ACM, December 1996. Vol. 39, No. 12, 67-68.

Edgar, Stacy L. "Computers and Privacy," Technology and Values, Lowman and Littlefield Publishers, Maryland, 1997, 295-310.

Electronic Communications Act of 1986.

Electronic Funds Transfer Act of 1980.

Ethics Code, TEX. GOVT. CODE ANN. 572.051, SECTION 7131, 1996.

Forester, Tom and Perry Morrison. Computer Ethics: Critical Tales and Ethical Dilemmas in Computing. Mit Press, Cambridge, Mass. 1990, 1-7.

Foster, Will A., Seymour E. Goodman and Anthony M. Rutkowski. "Who Governs the Internet," Communications of the ACM, August 1997, Vol. 40, No. 8, 15-20.

Ghaemian, Kaveh. "First Internet Security, Then Internet Commerce," Government Technology, October 1997, Vol. 10, No 11, 66.

Goodman, Seymour E. "Who Governs the Internet," Communications of the ACM, August, 1997. Vol. 40, No. 8.

Hale, Jerri. "Client Issues Presentation," Internal Audit Department, Available: Lycos.com.hale,j.@wizard.colorado.edu. 1

Hammit, Harry. "What Price, Privacy?" Government Technology, October 1997, Vol.. 10, No. 11, 22.

Harris, Blake. "How to Finance Service to the Citizen," Government Technology and Government Executive Supplement, October 1997, 32

Human Resource Handbook, Texas Department of Human Services, Section 7100, 1992 & 7131, 1996.

Johnson, Deborah G., and Helen Nissenbaum. Computers, Ethics & Social Values. Englewood Cliffs, N.J.: Prentice-Hall, 1995.

Jones, Bryan. "A Descriptive Study of Ethics Training Programs in Texas State Government," Applied Research Project, Spring 1995, SWTSU, 5, 64.

Jones, Sheri A. "Computer User Ethics In Public Administration," Applied Research Project, Spring 1993, SWTSU, 25, 40.

Kavanaugh-Brown. "Government Sites Set Cookies, Violate Privacy," Government Technology, October 1997, Vol. 10, No. 11, 14.

Kesar, Shalini and Simon Rogerson. "Computer use and abuse within organizations: Understanding ethics of a workplace," ETHCOMP98, CCSR, March 31, 1998, 1, www.ethcomps98

Koocher, Gerald P. "Ethics in Cyberspace," Ethics & Behavior, Lawrence Erlbaum Associates, New Jersey, November 2, 1996, Vol. 6, 9.

Meeks, Brock. "Privacy Lost, Anytime , Anywhere;" Communications of the ACM. August, 1997, Vol. 40, No. 8, 11-12.

Menzel, Donald C. "WWW.ethics.gov: Issue and Challenges Facing Public Managers." Public Administration Review. September/October 1998, Vol. 58 No. 5, 445-451.

Moor, James H. " What is Computer Ethics." Metaphilosophy16, Blackwell Publishers, 1985, 266-75.

O'Leary, Dianne Prost. "Use of Computer Facilities." Professional Ethics, Available www.oleary@ cs.umd.edu, 7/1/97, 1.

Parker, Donna B. "Ethical Conflicts in Computer Science and Technology." Afips Press, California, 1984, iii-vi.

Pojman, Lewis P. "What is Moral Philosophy," Technology and Values,1997, 11-22.

Schrader-Frechette, Kristin. "Technology and Ethical Issues, " Technology and Values, Roman and Littlefield Publishers Inc., Laham, Maryland, 1997, 25.

Schrader-Frechette, Kristin and Laura Westra. "Overview: Ethical Studies about Technology," Technology and Values, Roman and Littlefield Publishers. Inc., Laham, Maryland, 1997, 3-6.

Schulman, Charles Eric and Daniel Edward Shapiro. "Ethical and Legal Issues in E-Mail Therapy," Ethics and Behavior, 1996, 109-123.

Short, Rebecca, "Content Analysis of State Agency Employee Handbooks," Applied Research Project, Fall 1998, SWTSU.

"Social, Legal, and Ethical Issues in Computing," Issues in the News, SDSU.edu/course/CS440/hot issues.html.

Texas Ethics Commission, Article 6252 Human Resource Code, June 7, 1991.

"The Ten Commandments of Computer Ethics", Computer Ethics Institute, Available: www.Computing and Network Services,ksu.edu., March 24, 1996, 1.

Trevino, David S. "Computer User Ethics: A Study of the Ethical Awareness of the Public Works and Transportation Department Employees of the City of Austin," Applied Research Project, Summer 1995, SWTSU.

Turban, Efrain and McLean, Efrain and Wetherbe, James. Information Technology, John Wiley & Sons Inc., New York, 1996, G-5, 702-712.

Willard, Nancy E. The Cyber Ethics Reader, McGraw-Hill, New York, 1997, 1-53.

Williams, Bernard. "Ethics and the Limits of Philosophy." October 1997, 1.

APPENDIX A—ASSOCIATION FOR COMPUTING MACHINERY CODE OF PROFESSIONAL CONDUCT

ACM CODE OF PROFESSIONAL CONDUCT

PREAMBLE

Recognition of professional status by the public depends not only on skill and dedication but also on adherence to a recognized code of Professional Conduct. The following Code sets forth the general principles (Canons), professional ideals (Ethical Considerations), and mandatory rules (Disciplinary Rules) applicable to each ACM Member.

The verbs "shall" (imperative) and "should" (encouragement) are used purposefully in the Code. The Canons and Ethical Considerations are not, however, binding rules. Each Disciplinary Rule is binding on each individual Member of ACM. Failure to observe the Disciplinary Rules subjects the Member to admonition, suspension, or expulsion from the Association as provided by the Constitution and Bylaws. The term "member(s)" is used in the Code. The Disciplinary Rules of the Code apply, however, only to the classes of membership specified in Article 3, Section 4, of the Constitution of the ACM.

CANON 1

An ACM member shall act at all times with integrity.

Ethical Considerations

EC1.1. An ACM member shall properly qualify himself when expressing an opinion outside his areas of competence. A member is encouraged to express his opinion on subjects within his areas of competence.

EC1.2. An ACM member shall preface any partisan statements about information processing by indicating clearly on whose behalf they are made.
EC1.3. An ACM member shall act faithfully on behalf of his employers or clients.

Disciplinary Rules

DR1.1.1. An ACM member shall not intentionally misrepresent his qualifications or credentials to present or prospective employers or clients.
DR1.1.2. An ACM member shall not make deliberately false or deceptive statements as to the present or expected state of affairs in any aspect of the capability, delivery, or use of information processing systems.
DR1.2.1. An ACM member shall not intentionally conceal or misrepresent on whose behalf any partisan statements are made.
DR1.3.1. An ACM member acting or employed as a consultant shall, prior to accepting information from a prospective client, inform the client of all factors of which the member is aware which may affect the proper performance of the task.
DR1.3.2. An ACM member shall disclose any interest of which he is aware which does or may conflict with his duty to a present or prospective employer or client.
DR1.3.3. An ACM member shall not use any confidential information from any employer or client, past or present, without prior permission.

CANON 2

An ACM member should strive to increase his competence and the competence and prestige of the profession.

Ethical Considerations

EC2.1. An ACM member is encouraged to extend public knowledge, understanding, and appreciation of information processing, and to oppose any false or deceptive statements relating to information processing of which he is aware.
EC2.2. An ACM member shall not use his professional credentials to misrepresent his competence.
EC2.3. An ACM member shall undertake only those professional assignments and commitments for which he is qualified.
EC2.4. An ACM member shall strive to design and develop systems that adequately perform the intended functions and that satisfy his employer's or client's operational needs.
EC2.5. An ACM member should maintain and increase his competence through a program of continuing education encompassing the techniques, technical standards, and practices in his fields of professional activity.

EC2.6. An ACM member should provide opportunity and encouragement for professional development and advancement of both professionals and those aspiring to become professionals.

Disciplinary Rules

DR2.2.1. An ACM member shall not use his professional credentials to misrepresent his competence.
DR2.3.1. An ACM member shall not undertake professional assignments without adequate preparation in the circumstances.
DR2.3.2. An ACM member shall not undertake professional assignments for which he knows or should know he is not competent or cannot become adequately competent without acquiring the assistance of a professional who is competent to perform the assignment.
DR2.4.1. An ACM member shall not represent that a product of his work will perform its function adequately and will meet the receiver's operational needs when he knows or should know that the product is deficient.

CANON 3

An ACM member shall accept responsibility for his work.

Ethical Considerations

EC3.1. An ACM member shall accept only those assignments for which there is reasonable expectancy of meeting requirements or specifications, and shall perform his assignments in a professional manner.

Disciplinary Rules

DR3.1.1. An ACM member shall not neglect any professional assignment which has been accepted.
DR3.1.2. An ACM member shall keep his employer or client properly informed on the progress of his assignments.
DR3.1.3. An ACM member shall not attempt to exonerate himself from, or to limit his liability to clients for his personal malpractice.
DR3.1.4. An ACM member shall indicate to his employer or client the consequences to be expected if his professional judgment is overruled.

CANON 4

An ACM member shall act with professional responsibility.

Ethical Considerations

EC4.1. An ACM member shall not use his membership in ACM improperly for professional advantage or to misrepresent the authority of his statements.

EC4.2. An ACM member shall conduct professional activities on a high plane.
EC4.3. An ACM member is encouraged to uphold and improve the professional standards of the Association through participation in their formulation, establishment, and enforcement.

Disciplinary Rules

DR4.1.1. An ACM member shall not speak on behalf of the Association or any of its subgroups without proper authority.
DR4.1.2. An ACM member shall not knowingly misrepresent the policies and views of the Association or any of its subgroups.
DR4.1.3. An ACM member shall preface partisan statements about information processing by indicating clearly on whose behalf they are made.
DR4.2.1. An ACM member shall not maliciously injure the professional reputation of any other person.
DR4.2.2. An ACM member shall not use the services of or his membership in the Association to gain unfair advantage.
DR4.2.3. An ACM member shall take care that credit for work is given to whom credit is properly due.

CANON 5

An ACM member should use his special knowledge and skills for the advancement of human welfare.

Ethical Considerations

EC5.1. An ACM member should consider the health, privacy, and general welfare of the public in the performance of his work.
EC5.2. An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of the individual's privacy and seek the following:

—To minimize the data collected.
—To limit authorized access to the data.
—To provide proper security for the data.
—To determine the required retention period of the data.
—To ensure proper disposal of the data.

Disciplinary Rules

DR5.2.1. An ACM member shall express his professional opinion to his employers or clients regarding any adverse consequences to the public which might result from work proposed to him.

Appendix B

ACM Code of Ethics and Professional Conduct

On October 16, 1992, ACM's Executive Council voted to adopt a revised Code of Ethics. The following imperatives and explanatory guidelines were proposed to supplement the Code as contained in the new ACM Bylaw 17.

Commitment to ethical professional conduct is expected of every voting, associate, and student member of ACM. This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment.

It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity, for example with organizations such as ACM. Principles involving compliance with this Code are given in Section 4.

The Code is supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained

---

This code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct: Ronald E. Anderson, chair, Gerald Engel, Donald Gotterbarn, Grace C. Herlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtke, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund.

Source: Communications of the ACM 32, no. 2 (February 1993), 100–105.

in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the moral imperatives section, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. General Moral Imperatives.

As an ACM member I will . . .

1.1 Contribute to society and human well-being

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

1.2 Avoid harm to others

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public,

employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of computer viruses.

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. (See principle 2.5 regarding thorough evaluations.)

1.3 Be honest and trustworthy

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

1.5 Honor property rights including copyrights and patents

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

1.6 Give proper credit for intellectual property

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected, for example by copyright or patent.

1.7 Respect the privacy of others

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the

permission of users or *bona fide* authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

1.8 Honor confidentiality
The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

2. More Specific Professional Responsibilities.

As an ACM computing professional I will . . .

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work
Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence
Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work
ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recogni-

tion that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged.

Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

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

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Honor contracts, agreements, and assigned responsibilities

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences. However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

2.7 Improve public understanding of computing and its consequences
Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so
Theft or destruction of tangible and electronic property is prohibited by imperative 1.2—"Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4).

No one should enter or use another's computing system, software, or data files without permission. One must always have appropriate approval before using system resources, including .rm7 communication ports, file space, other system peripherals, and computer time.

3. Organizational Leadership Imperatives.

As an ACM member and an organizational leader, I will . . .

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities
Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social

responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communications resources

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

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.

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision-making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including

courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4. Compliance with the Code.

As an ACM member I will . . .

4.1 Uphold and promote the principles of this code
The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

4.2 Treat violations of this code as inconsistent with membership in the ACM
Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

APPENDIX C

CODING PROCEDURES FOR CONTENT ANALYSIS OF COMPUTER ETHICS DOCUMENTS

State Agency_____
Employee Handbook___ Employee Guide___ Training Manual___
Title:_____ Number of Lines_____

SETTING OF ETHICAL GUIDELINES	INCLUDED	DEGREE
1. Definition of Ethics		
2. Ethical Theory		
3. Morality and Values		
4. Ownership of Computer Ethics Responsibility		
5. Need of Ethics Training		
COMPUTER PRIVACY AND CONFIDENTIALITY		
1. Confidentiality of Sensitive Data		
2. Privacy Act of 1974		
3. Protection of Clients Information		
4. Right to Privacy		
COMPUTERS AND USER RESPONSIBILITY		
1. Security and Security Agreements		
2. Account Security Passwords		
3. Access and Copying of Computer Software		
4. User Responsibility		
LAW, LEGAL ASPECTS AND CONSEQUENCES		
1. Criminal Aspects, Computer Fraud and Abuse		
2. Computer Hackers		
3. Computer Statutes		
4. Copyright Infringements		
5. Consequences of Computer Use Violations		
CODE OF ETHICS		
1. Ethical Questions and Dilemmas		
2. Code of Ethics, Conduct and Good Practice		
3. Responsibility for Disseminating Accurate Information		
4. Association for Computing Machinery Code of Professional Conduct		
ETHICS AND THE INTERNET		
1. Introduction/Definition of the Internet		
2. Private and Public Usage /Concerns of the Internet		
3. Downtime and Damage Due to Worms/Viruses		

PHYSICAL ATTRIBUTES STANDARDS
1. Format and Design
2. Dated Pages
3. Acknowledgment Statements
4. Writing Style

APPENDIX D

POPULATION SAMPLE OF TEXAS STATE AGENCIES

1. ATTORNEY GENERAL
2. DEPARTMENT OF BANKING
3. DEPARTMENT OF INFORMATION RESOURCES
4. ETHICS COMMISSION
5. GENERAL SERVICES COMMISSION
6. RAILROAD COMMISSION OF TEXAS
7. SECRETARY OF STATE
8. STATE OFFICE OF ADMINISTRATIVE HEARINGS
9. STATE OFFICE OF RISK MANAGEMENT
10. STATE AUDITOR
11. STATE DEPARTMENT OF ECONOMIC DEVELOPMENT
12. TEACHER'S RETIREMENT SYSTEM
13. TELECOMMUNICATIONS INFRASTRUCTURE FUND
14. TEXAS ALCOHOLIC BEVERAGE COMMISSION
15. TEXAS ANIMAL HEALTH COMMISSION
16. TEXAS COMMISSION ON FIRE PROTECTION
17. TEXAS COMPTROLLER OF PUBLIC ACCOUNTS
18. TEXAS DEPARTMENT OF CRIMINAL JUSTICE
19. TEXAS DEPARTMENT OF ECONOMIC DEVELOPMENT
20. TEXAS DEPARTMENT OF HOUSING AND COMMUNITY AFFAIRS
21. TEXAS DEPARTMENT OF HUMAN SERVICES
22. TEXAS DEPARTMENT OF INSURANCE
23. TEXAS DEPARTMENT OF LICENSING AND REGULATIONS
24. TEXAS DEPARTMENT OF TRANSPORTATION
25. TEXAS EDUCATION AGENCY
26. TEXAS GENERAL LAND OFFICE
27. TEXAS HIGHER EDUCATION COORDINATING BOARD
28. TEXAS LOTTERY
29. TEXAS NATURAL RESOURCE CONSERVATION COMMISSION
30. TEXAS PARKS AND WILDLIFE
31. TEXAS REHABILITATION COMMISSION
32. TEXAS STATE LIBRARY AND ARCHIVES COMMISSION
33. TEXAS VETERAN'S COMMISSION
34. TEXAS WATER DEVELOPMENT BOARD
35. TEXAS WORKFORCE COMMISSION

APPENDIX E

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 engineering 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 hones 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

APPENDIX F

TEN COMMANDMENTS FOR COMPUTER ETHICS

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 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 use or copy software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you write.
10. Thou shalt use a computer in ways that show consideration and respect.

APPENDIX G
RESULTS TOTALS: TALLY SHEET
CODING PROCEDURES FOR CONTENT ANALYSIS OF COMPUTER ETHICS DOCUMENTS

State Agencies _____

State Agency Responses _____ %_____

ELEMENTS	INCLUDED		
	# Yes	#No	Line Average
SETTING OF ETHICAL GUIDELINES			
1. Definition of Ethics			
2. Ethical Theory			
3. Morality and Values			
4. Ownership of Computer Ethics Responsibility			
5. Need of Ethics Training			
COMPUTER PRIVACY AND CONFIDENTIALITY			
1. Confidentiality of Sensitive Data			
2. Privacy Act of 1974			
3. Protection of Clients Information			
3. Right to Privacy			
COMPUTERS AND USER RESPONSIBILITY			
1. Security and Security Agreements			
2. Account Security Passwords			
3. Access and Copying of Computer Software			
4. User Responsibility			
LAW, LEGAL ASPECTS AND CONSEQUENCES			
1. Criminal Aspects, Computer Fraud and Abuse			
2. Computer Hackers			
3. Computer Statutes			
4. Copyright Infringements			
5. Consequences of Computer Use Violations			
CODE OF ETHICS			
1. Ethical Questions and Dilemmas			
2. Code of Ethics, Conduct and Good Practice			
3. Responsibility for Disseminating Accurate Information			
4. Association for Computing Machinery Code of Professional Conduct			
ETHICS AND THE INTERNET			
1. Introduction/Definition of the Internet			
2. Private and Public Usage /Concerns of the Internet			
3. Downtime and Damage Due to Worms/Viruses			

PHYSICAL ATTRIBUTES STANDARDS
1. Format and Design
2. Dated Pages
3. Acknowledgment Statements
4. Writing Style

Texas Alcoholic Beverage Commission

Information Resources Security Guidelines

June 1995

OVERVIEW

Background

The Department of Information Resources (DIR) published rules in the Texas Administrative Code establishing state policy regarding security, TAC201.13b. The Texas Alcoholic Beverage Commission (TABC) assigned responsibility for information resources to the Information Resources Department (IRD).

TABC, hereinafter called the Commission, relies heavily on automation resources for efficient and effective operations management. Increased use of automation and continued technical advances in automation processing increase the Commission's dependence on information resources. The value of data and software, in terms of restoration costs or losses due to unauthorized disclosure, modification or destruction, far exceeds the value of associated hardware. For that reason, information processed by computers is a critical asset and must be protected accordingly.

Purpose

To provide security guidelines and standards intended to:

- establish responsibilities, minimum standards, and requirements for the protection of Commission information assets as they relate to data, image, text and voice within internal automated systems
- minimize exposure which could threaten the Commission's ability to perform critical functions
- ensure proper use of Commission information resources for state purposes only
- prevent misuse and loss of information assets
- establish the basis for audits and self assessments
- preserve management options and legal remedies in the event of asset loss or misuse
- provide a compilation of information security material in support of Commission security awareness and training programs.

DIR Rules Published in the Texas Administrative Code

It is the policy of the State of Texas that:

- Automated information and information resources residing in the various agencies of state government are strategic and vital assets belonging to the people of Texas. These assets require a degree of protection commensurate with their value. Measures shall be taken to protect these assets against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity and availability of information.
- The protection of assets is a management responsibility.
- Access to state information resources must be strictly controlled. State law requires that state owned information resources be used only for official state purposes.

MANAGEMENT AND STAFF RESPONSIBILITIES

Overall Roles And Responsibilities

Roles and responsibilities are required to provide adequate segregation of duties and responsibilities. There should exist an acceptable level of segregation of responsibility and duties to effectuate a successful information security program. Internal control principles applicable to other areas of the organization should also guide segregation of duties considerations in the security management program.

Fulfillment of information resource security responsibilities is required in order to have effective security for all information resources.

Responsibility for information assets will be assigned to the lowest reasonable level possible in the Commission.

All employees will read and sign a TABC Confidential Information Non-disclosure Agreement and those who refuse to sign the form will be denied access to the information resources.

Division/Department Director/Manager/Supervisor Responsibilities

Agency managers have ownership responsibility for the information assets utilized in carrying out the program(s) under their direction.

Managers have the following ownership responsibilities:

- participate in the risk analysis process by identifying assets and assessing their value to the Commission
- define quality assurance procedures to minimize the risk of errors and omissions and to ensure the integrity of the data for which they are responsible
- knowing assets and services they are responsible for and applicable control requirements
- authorizing users to utilize information assets and ensuring all equipment is used for department management approved purposes only
- assigning OPR authority and responsibility for appropriate information assets
- ensuring employee security education and awareness
- responding in a timely, effective way to loss or misuse of information assets and to identified business control and information asset security exposures

responsibility enables management to define security requirements based on business objectives. Since the OPR is usually within an organizational unit, protection of this information is a management decision.

Although it is the responsibility of the OPR to determine protection requirements for the information assets, the protection requirements themselves are implemented and maintained by IRD Security team.

The OPR has the following authority and responsibilities:

- determine the asset's value and importance to the Commission
- classify the assets and review control and classification recommendations
- ensure that information asset security and application system controls are in place
- define access requirements that are implemented by IRD Security team
- provide IRD Security team with resource definition information
- communicate control and protection requirements to suppliers of services and users
- review and verify/approve existing access rules at least annually and request revisions where appropriate
- participate in risk assessment and risk acceptance process, make risk management decisions
- bring security exposures, misuse, or noncompliance situations to the attention of their own management and to the IRD Security team
- participate in contingency planning

OPR Security Administrators (Division/Department Director or Designee)

Duties of division/department security administrators may include:

- establishing, monitoring, updating and enforcing division/department security measures, policies and procedures, as appropriate to amplify departmental policy, standards, guidelines, and procedures. Make recommendations for updating policies, standards, guidelines, procedures, and forms as necessary
- User Support:
  - serve as liaison between IRD Security team and users on security matters
  - provide user support with sign-on/password problems
  - provide all automation users with any information pertaining to the users' security

Software License Agreements

Guidelines

- Software license agreements must be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one personal computer except as expressly provided for in the manufacturer's license agreement.

Standards

- Personnel should be advised of the necessity to adhere to software license agreements and consequences of failure to do so. Training and awareness is management responsibility.

Documentation

Guidelines

- A minimum set of standard documentation should be maintained by the individual or organization responsible for a personal computer or word processor. Standard documentation can be categorized into four basic areas and includes the following:

  Hardware. All manuals supplying documentation relating to the installation, maintenance, or care of the equipment should be located in an area adjacent to the equipment.

  Proprietary Software. All manuals supplying documentation relating to the installation and use of proprietary software should be located in an area adjacent to the equipment or in a central library, as appropriate.

  User-Programmed Applications. Custom in-house development of systems requires a level of documentation commensurate with the importance of the application to the agency. Documentation for applications developed in-house should consist of no less than the following elements:
  - an approved justification for user-generated application system development;
  - user manual/instructions containing the scope and purpose of the system, data entry instructions, and processing instructions;
  - program/procedure source data;
  - file descriptions including data dictionaries; and,
  - sample report/screen formats.

  Applications Using Proprietary Software Packages. For those applications which make use of proprietary software packages (including data base systems, spreadsheets, or software that maintains data files), the agency should establish procedural documentation sufficient to allow for its productive use in the absence of the primary user. This documentation will normally consist of the following:

Guidelines

- Strict adherence to the procedures and guidelines outlined in preceding sections will minimize this risk.

- Educate users about malicious software in general, the risks that it poses, virus symptoms and warning signs, how to use control measures, policies and procedures to protect themselves and the organization.

- Establish software management policies and procedures that address public-domain software. Never download software from public access bulletin boards.

- Establish and educate users about careful change management procedures and the use of programs to aid in virus detection.

- Initiate control procedures to regularly run virus detection programs on personal computers and word processors used to store confidential or sensitive information or to run critical applications.

- Monitor user and software activity to detect signs of attacks, to detect policy violations, and to monitor the overall effectiveness of policies, procedures and controls.

Standards

- Employees will be made aware of Commission policies and procedures outlined in The TABC Employee Handbook.

- IRD has established and maintains formal change management procedures.

- Virus detection programs will be run on personal computers and word processors used to store confidential or sensitive information or to run critical applications.