

99A016 I

Project Number: LAB-99MP -51

MAJORING IN PIRACY

An Interactive Qualifying Project Report

submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the

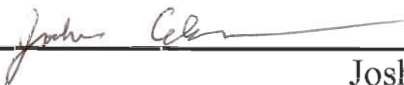
Degree of Bachelor of Science

by



---

Ian Parmenter



---

Joshua Colson

Date: October 15, 1999

Approved:



---

Professor Lee A. Becker, Project Advisor

## **Abstract**

A look at the state of piracy on college campuses finds that the policies used to inform students just what is acceptable are sorely lacking. These policies are reviewed and analyzed, and a generic policy is put forward as being an ideal choice to base college policies off of. A thorough review of literature on campus piracy is given, along with results of surveys on the matter.

# Table of Contents

1. Introduction	4
2. Background	5
2.1 Organization	5
2.2 Defining Software Piracy	5
2.3 Defining Copyright Piracy	6
2.4 Extent of Campus Software Piracy	6
2.5 Methods of Software Piracy	8
2.6 Methods to Combat Software Piracy	10
2.7 Methods to Combat Copyright Piracy	14
2.8 Arguments over Software Piracy	15
2.9 Conclusion	16
3. Methodology	17
3.1 Literature Search	17
3.2 Student Survey	17
3.3 System Administrator Survey	19
3.4 College Software Policy Analysis	23
3.5 Methodology of the Generic Policy	23
4. Results	24
4.1 Student Survey	24
4.2 College Software Policy Analysis	29
4.3 Ideal Generic Policy	33
5. Conclusion	36
6. Bibliography	37

# Introduction

The goals of this project are: to provide a review of college policies regarding piracy; to show that the average college policy is lacking in what needs to be included to help stem piracy; to put forward a generic policy that can be used by colleges and universities to help educate students and prevent the spread of piracy.

We accomplished these goals by gathering and reviewing policies from colleges and universities across the country, by analyzing these policies along with surveys of students, and by taking the results of the analysis and interpolating what needed to be more strongly emphasized in our generic policy.

What follows is the result of this project. It includes a comprehensive review of literature regarding piracy on college campuses, as well as the methodology and analysis of our surveys of students and research into campus policies.

## **2. Background**

### **2.1 Organization**

The information obtained by the literature review will be presented in the following order :

The first two sections will define software and copyright piracy as it applies to universities such as WPI. This is followed by a section which shows evidence that these activities take place to large extent. Methods of software and copyright piracy will be described, and then methods to combat them. The next section deals with the differing opinions on piracy. It is followed by the conclusion.

### **2.2 Defining Software Piracy**

Software piracy is the use of software without first purchasing the appropriate license, or breaking the licensing agreement. Many users on campuses such as WPI steal software, and many different types of piracy exist. Low end pirates are those who trade software with fellow students or colleagues. High end pirates trade software not only with those they know, but also over the Internet. They use a variety of methods, such as Internet Relay Chat (IRC) and 'warez,' terms which will be defined below. Couriers are high end pirates who also happen to be insiders at companies that manufacture software. Couriers create so called 'zero day warez,' software that is available for illegal download before it is released to the general public. These couriers are outside the scope of this report since there are few, if any, such people here at WPI.

Piracy can also be divided by where it takes place. Corporate piracy takes place when businesses make multiple copies of software from only one license, usually spreading the illegal copies over a local area network (LAN). An analogous situation at a university would be if a professor were to distribute software to students for an assignment, without purchasing enough additional copies. Reseller piracy is the sale of computers bundled with unlicensed software. Finally, home piracy is the kind which takes place on individual students' computers, both low end and high end.

There are two terms which should also be defined in this section. Shareware is software, usually less functional than the full version, that may

be used freely for a period specified by an agreement between the end user and the creator. It is for evaluation purposes, and in most cases the user is required to either buy the full version or delete the shareware copy after the evaluation period ends. Shareware can not be resold by the user for profit. Freeware is software that need not be paid for, however like shareware it is illegal for the user to sell the software for profit.

## **2.3 Defining Copyright Piracy**

In recent years, the problem of software piracy has been compounded by the addition of two new types of electronic piracy. Music piracy, in the form of downloading MP3 (standing for MPEG-1 Layer-III Compression), has been popular since early 1996, when the first MP3 compression and playback programs became available on the internet. Movie piracy, originally in the form of VIVO movie files and evolving into simple MPEG files, became more popular in late 1997. These two forms of piracy, falling under the umbrella term of 'Copyright Piracy,' have become as large a problem as software piracy, spreading faster and being more popular. Much of what is said about software piracy in this paper will also apply to copyright piracy, with notes made where there are differences.

Copyright piracy is easy at colleges because of large-bandwidth connections to the internet. This allows pirates to handle the large movie files, which would normally take days or weeks to download on a home PC, as well as downloading MP3 files faster than it would take to play them.<sup>1</sup>

## **2.4 Extent of Campus Software Piracy**

Universities are places where new intellectual property is created regularly. Yet software piracy is the theft of intellectual property, and it also occurs extensively at universities such as WPI. In fact, the problem is so wide-spread that the Software Publishers Association (SPA) has started a special campaign targeted at college software piracy. The SPA will be described more extensively in later sections.

---

<sup>1</sup> Associated Press, "Illegal Films Infiltrate Internet", April 22, 1999

One survey<sup>2</sup> of particular interest in this report involved three hundred students at an institution of higher learning. Among the information they discovered was that students believe their peers, and even professors and administrators, engage in software piracy. Also, experience with computers does not increase or decrease ethical behavior, that is the willingness of a student to be involved in software piracy. This survey took place a decade ago, and there is every reason to believe that campus piracy has increased since then, as shall be explained in other sections of this report.

Another survey was conducted by the SPA, the Student Monitor Computer Survey.<sup>3</sup> It reported that nearly one third of students “borrow” software, and that 42% of students approve of the practice.

Software piracy reaches all kinds of campuses, not just ‘tech’ schools. Andrews University, a small liberal arts school, was using 90% of its network capacity until the traffic caused by two warez sites was stopped. Network usage dropped to 20%.<sup>4</sup>

Software piracy currently makes up 27% of the software industry in the U.S., and costs 130,000 jobs per year<sup>5</sup>, although these figures are under dispute<sup>6</sup>. In 1994, the global cost of software piracy was estimated at \$11.8 billion for the year<sup>7</sup>. The numbers may be wrong if they assume the pirate would have purchased all the software s/he stole, when not given the option to steal it. Many pirates steal more software or other media than they could reasonably afford.

---

<sup>2</sup> Cohen Ph.D, Eli Journal of Information Systems Education, 3/89, “College Students Believe Piracy is Acceptable”

<sup>3</sup> [www.spa.org](http://www.spa.org)

<sup>4</sup> [www.msnbc.com/news/](http://www.msnbc.com/news/)

<sup>5</sup> <http://www.microsoft.com/presspass/> on April 28, 1999

<sup>6</sup> Masland, Molly “Software Piracy a Booming Net Trade,” [www.msnbc.com/news](http://www.msnbc.com/news)

<sup>7</sup> “INTERNET NETWORK A SOFTWARE PIRATES HAVEN DUE TO SLACK SECURITY—REPORT,” Telecomworldwire, 1-4-94

## 2.5 Methods of Software Piracy

Improvements in the methods available to commit software piracy are the primary reason for the increase in this activity.<sup>8</sup> The potential for movies to be pirated with greater ease exists because read-write DVDs have become available, holding more data than multiple CDs. Faster network connections mean quicker downloads. “Now, to download Jurassic Park with a normal modem would take days and days. But with cable modems it may be possible to do it in as little as an hour.”<sup>9</sup>

Also available to pirates are warez web sites and the growing-in-popularity IRC (Internet Relay Chat) servers, which are replacing the BBS (Bulletin Board System) pirate havens of the past. At these places pirates collect, trade, and give away ‘cracked’ software. Information on how to find software is also traded. However, this sort of activity is easily traced, as in the case of four Bates College students<sup>10</sup> arrested under Maine law for unauthorized copying of computer programs.

Methods of software piracy are illustrated by problems experienced at the University of Michigan<sup>11</sup>. Hackers would steal password with a ‘Trojan Horse’ program. This program looks like a login screen, but actually collects lists of user names and passwords. The hackers could then store their warez games and programs on the accounts of other students and faculty. This has the advantage of making the hacker very difficult to trace. Another unfortunate side effect is that even more unsavory characters are attracted to hacked sites. Having this kind of content on their network reflected badly on the school. The procedures used to combat these activities will be described in the next section.

---

<sup>8</sup> Ross, Philip E., *Forbes* web site Issue Date : September 9, 1996

<sup>9</sup> Wolf, Christopher (intellectual property lawyer), quoted at *Forbes* web site

<sup>10</sup> Associated Press, “Students Arrested in Software Case”, April 14, 1999

<sup>11</sup> “Software Pirates are Looking to You for Places to Stash Their ‘WAREZ’”, [www.itd.umich.edu](http://www.itd.umich.edu)



There are several other methods of software piracy worth mentioning here. They include two 'urban legends' used to rationalize the theft of software, 'abandonware' and the 'twenty-four hour rule.'<sup>12</sup> 'Abandonware' is the word used to describe the belief that if a software creator ceases distributing or supporting the product for five years, the program is free. Abandonware does not exist. U.S. copyright law protects software at least seventy-five years, or fifty years after the death of the creator. Another belief is the 'twenty-four hour rule,' which states that it is okay to steal the full version of a program for evaluation purposes, so long as one deletes it within twenty-four hours. This is also a myth. Except for shareware versions, this activity is against the law. Another piracy method besides spreading rumors is giving a false name and address to one's Internet Service Provider (ISP). A final obstacle in the path of law enforcement is one specific to IRC, where some servers, mainly those in some European countries, do not keep records of who is logged in, allowing piracy to happen in complete privacy. This makes it very difficult for law enforcement to track down those who deal in illegal software. These difficulties are exacerbated because consumers resist some methods of copyright protection, such as the old uncopyable floppy disks. These died out around 1986, except for a brief experiment with compact disks using the same methods in 1997.<sup>13</sup>

---

<sup>12</sup> [www.spa.org](http://www.spa.org)

<sup>13</sup> Ross, Philip E., Forbes web site Issue Date : September 9, 1996

## 2.6 Methods to Combat Software Piracy

Concern over software piracy has led to a lot of legislation in the U.S., which of course affects the campus community. Since the 1960's, software code has been protected as a form of literary expression.<sup>14</sup> In 1980, U.S. Copyright Law was amended to include programs. The maximum penalties for someone who copies (for profit) \$2500 worth of software include 6 years of prison and a \$250,000 fine. Individual states have also created laws to this effect. For example, the Florida Computer Crimes Act (1988) includes a monetary penalty of twice damage and up to 15 years in jail for serious offenders.<sup>15</sup> The Senate passed Bill S893 in October of 1992, which changed piracy from a misdemeanor to a felony. A second offense can earn up to ten years in jail. In 1997 the No Electronic Theft (NET) Act was passed.<sup>16</sup> For the first time, pirates could be prosecuted even if their stolen software had not been sold for profit. In the summer of 1999, the first case to be prosecuted under the NET occurred in Oregon. The Digital Millennium Copyright Act (HR2881) would make the development of certain encryption cracking software illegal. Another relevant piece of legislation is the Electronic Communications Privacy Act, which allows for the following in investigations: Email may be intercepted only if users sign a policy allowing this, or one of the parties involved agrees to cooperate with the investigation. Also, information obtained in an investigation may be shared only on a need-to-know basis.

In recent years, many organizations have taken legal action against pirates. The University of Oregon settled the first ever suit against a school for \$130,000.<sup>17</sup> In addition they agreed to organize and host a conference on copyright law and software piracy. The suit was on behalf of the SPA, Microsoft, and other software developers. On April 28, 1999, 15 civil suits were announced against Florida businesses allegedly involved in software piracy.<sup>18</sup> There were also criminal searches of several warehouses. It is believed that organized crime is also moving into software piracy, because it is a relatively safe and easy way to make money. The SPA has recently cooperated with the FBI in several raids.<sup>19</sup>

---

<sup>14</sup> Boyd, Marvin J. "What is software piracy?" April 10, 1997

<sup>15</sup> Florida Computer Crimes Act (1988) at [www.med.ufl.edu](http://www.med.ufl.edu)

<sup>16</sup> Laprad, David, "Digital Anarchy : Analysis of Software Piracy" at [NewWorld.com](http://NewWorld.com)

<sup>17</sup> <http://www.pclan.calpoly.edu/swpiracy.htm>

<sup>18</sup> [www.microsoft.com](http://www.microsoft.com)

<sup>19</sup> "SPA Cooperates with FBI in Five Raids" June 1, 1998 at [www.spa.org](http://www.spa.org)

The Software Publishers Association is a large organization dedicated to fighting software piracy. It has 1200 member companies, which account for 85% of the revenue for packaged and online software. The SPA is available to help universities on many levels. Colleges have the option to request an audit from the SPA in order to help them locate and remove pirate activity on campus. They will also email offenders on behalf of the university. The SPA offers the following warnings and advice for systems administrators :<sup>20</sup>

#### **Seven Warning Signs of Piracy**

- Increased or even massive FTP file transfer in a directory
- Expanded directory trees
- Excessive data transfer in a single session
- Sites labeled *Warez* or listed as involving *Cracker* or *Hacker* activity
- The posting of serial numbers used to install software
- Increased logging into an area
- Numerous unusual or hidden files or directories

#### **Risks of Piracy to Server Operators**

- Theft of services
- Server breakdowns from being overloaded
- Software companies believing server operators might be cooperating with pirate activity (especially when the server operator is licensed to distribute their software)
- Loss of customer confidence if breakdowns occur
- Incorrect billing of customers for memory usage
- 'Breaking' the incoming directory of a system's FTP. (Note: The pirates frequently create directories beginning with a space. Windows 3.x can't handle files or directories that start with a space and they'll hang the FTP application until offending directory or file is deleted. AOL users can only deposit files into the incoming directory of an FTP site.)
- Loss of disk space
- Loss of customer confidence as pirates often create obscenely named directories in both incoming and customer FTP sites
- Possible infringement of the copyright law

The SPA recommends that colleges maintain an email address to allow students to report software piracy. They also suggest the following systematic steps to deal with cases of piracy. First, system administrators should visit suspicious web sites on campus and review logs of network activity. Evidence of any infraction should be kept, including screen captures and the network logs. The system administrator can then consult with the SPA to receive information on criminal and civil penalties that are applicable. Finally, appropriate sanctions can be applied to any offending parties located, including but not limited to warnings, community service, loss of computer privileges, or expulsion.

---

<sup>20</sup> [www.spa.org](http://www.spa.org)

For those creating university software policy, the SPA recommends the following:<sup>21</sup>

It is [University's] policy to limit Internet access to [research/personal use/classwork/etc.]. Unauthorized use of the [University's] computing resources may result in loss of privileges.

The intentional introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Any such activity will result in [The University should modify to incorporate their appropriate review process.]

Users using [University's] accounts are acting as representatives of [University]. As such, users should act accordingly so as not to damage the reputation of the University.

Files that are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.

The truth or accuracy of information on the Internet and in email should be considered suspect until confirmed by a separate (reliable) source.

Users shall not place copyrighted material (software, images, music, movies, etc.) on any publicly accessible Internet computer without prior permission from the copyright holder or as granted in a license agreement or other contract defining use.

Alternate Internet Access Provider connections to [University's] internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Users should exercise caution and care when transferring such material in any form.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, students are prohibited from downloading software and/or modifying any such files without permission from the copyright holder or as granted in a license agreement or other contract defining use.

Any infringing activity by a user may be the responsibility of the University. Therefore, [University] may choose to hold the user liable for his or her actions.

[University] reserves the right to inspect a user's computer system for violations of this policy. [University] reserves the right to monitor, suspend, and/or limit a user's access to ensure compliance with [University] policies and federal, state and local law.

Users agree to adhere to all relevant federal, state and local law applicable to their computer use. [University] reserves the right to release a user's identity to an appropriate authority to comply with an investigation into computer misuse.

I have read [University's] Internet Usage Policy statement and agree to abide by it as consideration for my continued enrollment/employment at [University]. I understand that violation of any of the above policies may result in disciplinary action, including the possibility of expulsion/termination.

---

User's Signature

---

Date

---

<sup>21</sup> www.spa.org

The SPA also makes available for download audit software that can check one's software applications for legitimacy.

The survey from the Journal of Information Systems Education made the following recommendations.<sup>22</sup> Students should receive education on various aspects of software policy during orientation freshman year. Also, the school's software policy should be distributed regularly for easy access. Any course that makes use of computer work should briefly remind students of the school's policy. Universities should purchase a site license for important software to prevent piracy. Finally, shareware programs should be made easily available.

The University of Michigan article<sup>23</sup> mentioned above recommends the following : All users should keep their passwords confidential. Students and faculty should be encouraged to report suspicious activity. System Administrators should look for computers that are accessed the most, particularly those that are not involved in research but are accessed from all over campus. Users should reboot computers before logging in if they believe a 'Trojan Horse' program may be active. Students found to have broken school software policy should first receive a warning, then suspension for a further transgression.

---

<sup>22</sup> Cohen Ph.D, Eli Journal of Information Systems Education, 3/89, "College Students Believe Piracy is Acceptable"

<sup>23</sup> Hofer, Theresa, "Software Pirates Looking to You for Places to Stash Their 'WAREZ'"  
www.itd.umich.edu 1/15/97

There are also many technological solutions to deal with software piracy. The new DAT disks, unlike CDs and DVDs, have a copyright protection system.<sup>24</sup> However, the fact that one cannot own a DAT like a DVD may keep them from becoming as popular. One company is developing a 'cryptographic envelope,' which is supposed to prevent the use of a software package until one pays for it online. Another useful tool in the fight against piracy is SCAM, the Stanford Copy Analysis Mechanism, which searches the Internet for phrases that may indicate theft of ideas or software. A more powerful possibility would be an operating system based attack on piracy. However, under Windows files can easily be copied regardless of whether or not it is illegal to do so. Creating longer programs may inadvertently prevent piracy, by making downloads difficult. However, fast cable modems solve this problem for pirates, at least for now. Software companies may prevent some piracy by giving away old versions of their products for free, and then selling the latest version to those who want it. Also being considered is 'meterware,' a pay per use scheme. This is unlikely to catch on, as it would be much more inconvenient than traditional software.

A company called Pace Anti-Piracy sells a product called InterLok Pro for Windows. It allows software producers to do create the following versions for their program : try-before-you-buy, rentals, and immediate purchase. It has the option to lock software to the end users hardware, create serial number authorization systems and uncopyable diskettes, a remote feature control which changes access based on the license purchased, encrypt programs, and will also prevent debuggers from operating with the protected program.

Finally, it is possible to try to prevent software piracy by appealing to the moral standards of potential pirates. Parents should remind their children not to pirate software, and set a good example by not doing so. Universities should remind their students that software piracy is similar to plagiarism, and therefore unacceptable. Some compare software piracy to shoplifting, which is an activity that most pirates would not engage in.

## **2.7 Methods to Combat Copyright Piracy**

Luckily, many of the same methods that combat software piracy will also work against copyright piracy. This is because they use the same methods of distribution (FTP, IRC, WWW, etc.) over the same computers

---

<sup>24</sup> Ross, Philip E., Forbes web site Issue Date : September 9, 1996

and same networks. However, some techniques, such as copy-protected disks and encrypted files, will not work because copyright-pirated files are typically 'ripped' from its source into another file, through sound cards recording songs or video cards capturing movies. As these files are essentially home-made, copy-protection (such as the Macrovision system used to protect VHS cassettes and DVD movies) will not have any effect on these movies. For this reason, the main method of fighting copyright policy has rested with the RIAA and their efforts to shut down the web sites that provide illegal music files<sup>25</sup>. However, this is harder to do with movie files, as they are usually served through IRC and not the World Wide Web, making tracking down servers infinitely harder. This leaves authorities with next to no options.

## 2.8 Arguments over Software Piracy

There are many opinions about what is or is not wrong about software piracy. Microsoft warns its customers that pirated software is dangerous because it may contain viruses or be missing key features such as a manual, certificate of authenticity, and features like the hologram on the Windows98 CD.

On the other hand, there are those who believe that the problems of software piracy are exaggerated. "The cost of theft has been factored into the revenue generating model since day one."<sup>26</sup> Critics site large profits of some software companies as proof of this. Computer Underground Digest suggests that software piracy is rampant partly because of difficulties in evaluating software. They also believe it is impractical to go after smaller pirates, and that the government should concentrate its efforts against corporate pirates and other large groups who would be easier to catch.

There is also a fear of over legislation of the Internet. Because the Internet relies on the free flow of information, laws which restrict that flow hurt the users.

---

<sup>25</sup> Jon Gaw, "Copyright laws headed for digital overhaul," Minneapolis Star Tribune, 5-4-98

<sup>26</sup> Joshua Bauchner, SPA, quoted in Digital Anarchy : Analysis of Software Piracy

## 2.9 Conclusion

Software and copyright piracy is a major legal and ethical issue for colleges and universities. It takes place for more often than other types of theft, and is more widely accepted. Also, it can leave the school open to law suits from major software companies.

There are several methods available to the university to combat piracy. System Administrators can monitor their networks for suspicious activity. Students can be educated about why software piracy is wrong. If a student is found to be using the campus network in an illegal manner, the account can be revoked. Legal action may also be possible.

It is in the best interest of universities such as WPI to curb piracy by any appropriate means. When intellectual property is not respected and illegal activities take place, the integrity of this institution is damaged.



## **3. Methodology**

This section contains information on how we did what we did. It explains why decisions were made, how things were chosen, and what we were thinking.

### **3.1 Methodology of the Literature Review**

For the sources cited in the literature review, we relied heavily on the use of the world wide web, as shown by the several cited web sites. This is due to the fact that, at the beginning of the project, we felt it would be the best source of information on the subject, allowing us to browse magazine articles as well as news stories and the web sites of organizations such as the SPA.

We then collected every article that looked like it could be relevant and began to read through them, keeping those that had useful information or were relevant to the project in other ways, and discarding those that weren't.

Then, once the articles were selected, we wrote a comprehensive introduction to the topic using these articles as references.

### **3.2 Methodology of the Student Survey :**

#### **3.2.1 Purpose**

The purpose of the student survey was to determine the extent of software and music piracy at WPI. It was felt that revealing the amount of piracy that takes place among the student body would underscore the importance of this issue. Furthermore, the data would tell why and how this piracy took place.

#### **3.2.2 Design**

These are the questions used in the student survey :

Which of these describes your attitude towards software piracy :

- A: I don't pirate software.
- B: I only pirate software to evaluate it, then I buy the product if I like it.
- C: I can't afford to buy it, so the company isn't losing money.
- D: Most software isn't worth the price.
- E: Pirating software is easier than buying it.

About how many computer games have you pirated in the last year?

- A: None
- B: 1-4
- C: 5-9
- D: 10-20
- E: 20+

About how many music files (e.g. MP3's) have you pirated in the last year?

- A: None
- B: 1-10
- C: 11-50
- D: 51-250
- E: 250+

How do you get pirated software / music (choose all that fit)?

- A: web sites at WPI
- B: warez
- C: mp3 sites
- D: other web sites
- E: other students

It was decided that only four, brief multiple choice questions would be posed. Clearly, no one would want to fill out a long, tedious form. The answers for question one were derived primarily from the literature search, that is, the most commonly named reasons for pirating software / music were used. The ranges for questions two and three were guesses based on personal experience. The choices for question four were once again based on what was suggested in the literature review.

Of all the questions, only the range of question three was a problem. Several students suggested that choice E, 250+ music files pirated in one year, was too small by an order of magnitude. This was perhaps one-fourth of all the students who selected E, although this is a highly subjective remark. In hindsight, the exact number should have been recorded.

### 3.2.3 Distribution

The student survey was conducted in two parts. The first was in front of Morgan Commons during term D99. Forty-two students were questioned. During term A99, thirty-nine additional sets of data were gathered inside the Founders Hall Commons.

The sample was expanded in A99 in order to decrease the error that might result from a small data set. The questions were given in person, with students writing down their selections to the four multiple choice questions in a notebook. This information was not gathered through email because it was felt that the survey might be ignored over that medium. In fact, no one who was asked to fill in the survey refused to do so, although several required assurances that they remain anonymous.

## 3.3 Methodology of the SysAdmin Survey:

The SysAdmin Survey was originally designed to be one of the cornerstones of this project, gathering practical information straight from those who knew their campus networks best, the systems administrators. Unfortunately, this survey failed to gather any appreciable results.

The Survey consisted of thirteen multiple-selection questions, ranging from data on the student population of the college or university to the number of pirates ‘caught’ on a regular basis at that campus to whether the administrators felt the punishments given were appropriate. The questions were chosen to be easy to understand, quick to answer, and still to give viable data.

The University Pages<sup>27</sup> were instrumental in assisting with the task of gathering email addresses for systems administrators. A total of nearly 400 addresses were gathered from campuses across the country, attempting to keep an equal mix between large and small, tech and non-tech, public and private, although given the nature of some schools to be more likely to have web pages, this was not always the case. Where SysAdmin email addresses were unavailable, we decided to send our message to the campus’ version of the Helpdesk

We then had to make a decision. We could send out the survey to each address and hope they responded by typing out their answers and replying, or

---

<sup>27</sup> [http://isl-garnet.uah.edu/Universities\\_g/](http://isl-garnet.uah.edu/Universities_g/)

we could put the survey on a web page and through a combination of CGI and javascript, receive our answers via email. The second method was attractive for three reasons. One, it would involve sending out smaller mails to people. Two, it would be faster for the subjects to fill out the survey. Three, it would be somewhat more anonymous, as instead of the subject's email address, all we'd have access to would be their IP Address.

The message was sent out on May 5, 1998. The contents of the message included a brief description of the project, a request for help by filling out the survey, and the URL of the survey. Response was less than enthusiastic. Eight responses in the first two days, with two more trickling in over the next week. The decision was made to re-send the request at the beginning of the next school year, in the hopes of getting more responses. This second sending received two completed surveys.

With this amazing lack of data (12 responses out of a possible 400, a total of three percent), it was decided that the survey could no longer be used as a cornerstone of the project. It has since been relegated to this single page.

However, it is interesting to note that the responses that came in were all from smaller schools, and all cited music as being the most pirated form of data across their networks. And most of the responses said they felt the punishment for being caught was not harsh enough.

### 3.3.1. Text of SysAdmin Survey

Thank you for taking part in this survey of college and university systems administrators. The information gained from this survey will be used as part of a study aimed at finding ways to decrease software and music piracy on campuses across the country. All information we receive via this survey will be held in strict confidence. No names or specific information about you or your campus will be given in the final report. Please keep in mind that piracy includes using software without buying the appropriate number of licences. Thank you for your participation.

1) What is the undergraduate population at your campus?

0-500 | 501 - 1000 | 1001 - 3000 | 3001 - 5000 | 5001+

2) What is the undergraduate Computer Science population at your campus?

0-500 | 501 - 1000 | 1001 - 3000 | 3001 - 5000 | 5001+

3) Do you educate students about software piracy (either as incoming freshmen, or as a whole)?

Yes | No

4) How often do you receive reports of students obtaining/using pirated software?

Never | Once a semester | Monthly | Weekly | Daily

5) How often do you receive reports of faculty obtaining/using pirated software?

Never | Once a semester | Monthly | Weekly | Daily

6) What percentage of students do you feel use pirated software and are never reported?

None | 1-10% | 11-20% | 21-30% | 31-40% | 41-50% | More than 50%

7) What percentage of faculty do you feel use pirated software and are never reported?

None | 1-10% | 11-20% | 21-30% | 31-40% | 41-50% | More than 50%

8) What actions are taken when someone is reported? (please check any and all that apply)

Warning | Termination of network access | Termination of account (UNIX or otherwise)

Reported to authorities | Reported to company pirated from | Expulsion

Nothing | Other

9) If not checked above, are warnings given for first-time offenders?

Yes | No | Sometimes

10) Do you feel your campus' punishments for piracy are too strong, too weak, or appropriate?

Too Strong | A bit strong | Appropriate | A bit weak | Too Weak

11) Have companies or the federal government ever pressed charges against a student at your campus for pirating software or other forms of copyright violation?

Yes (Federal) | Yes (Corporate) | Yes (Both) | No

12) What type of 'software' (referring to any copyrighted data) is the most pirated at your campus?

Games | Graphics Programs | Music | Programming Tools | Business Educational (including programs used in classes that do not have enough licenses) | Movies | Other

On a scale of one (lowest) to ten (highest):

How bad do you feel piracy is on campuses in general?

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

How bad do you feel piracy is on your campus?

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

How quickly do you feel piracy is growing?

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

### **3.4 Methodology of the Policy Review:**

For the review and analysis of campus acceptable usage policies, we decided that one hundred policies would be an acceptable number to review and analyze. To this point, we used the University Pages to access university sites on the world wide web and dug through them to find policies, saving them onto our own computers for later review.

The policies were chosen in a random fashion, often dictated by whether the college's web site was working, or even whether it was possible to find the wanted policy on their site. Most of the policies come from the same campuses that had their email addresses used for the SysAdmin Survey. However, some of them do not, either due to finding the policy before finding there was no email address, or simply a deliberate choice to get a few policies from non-emailed campuses.

After collecting the policies, we scanned them for their compliance with 29 categories, a task occasionally made tougher by legal language. These twenty-nine categories were chosen to represent an 'ideal' policy. The results were placed into a spreadsheet and then condensed into graphs so we could better see what college policies say. This gave us the lion's share of the data needed to determine what the optimal college policy on piracy would be.

### **3.5 Methodology of the Generic Policy**

The purpose of the generic policy was to list the guidelines necessary for a university computer user policy to be complete. By making sure all of the points in the generic policy are mentioned, a school knows that their policy will have the maximum legal protection possible. Also, the policy will help motivate the correct behavior in the student body.

The creation of the generic policy was decided upon when the data of the College Software Policy Analysis revealed that many university policies were incomplete. It was felt that a guide should exist to help policy writers improve this situation.

The 29 data points were decided upon after the review of the first several policies. They included all the topics that were felt to be germane to the purpose of a software policy. The points that were selected dealt with the legal protection of the university, or with educating the students against

software piracy. It was using these data points that the remainder of the hundred software policies were analyzed. (see section 3.4)

The generic policy expands on these 29 points, explaining the meaning behind them. There is also a section on items to avoid placing in a software policy. This was added because in certain cases policies were found to be so long that vital information was buried in piles of legalese and procedures. It is doubtful that students would actually take the time to read such a document, and distributing copies of it would be impossible.



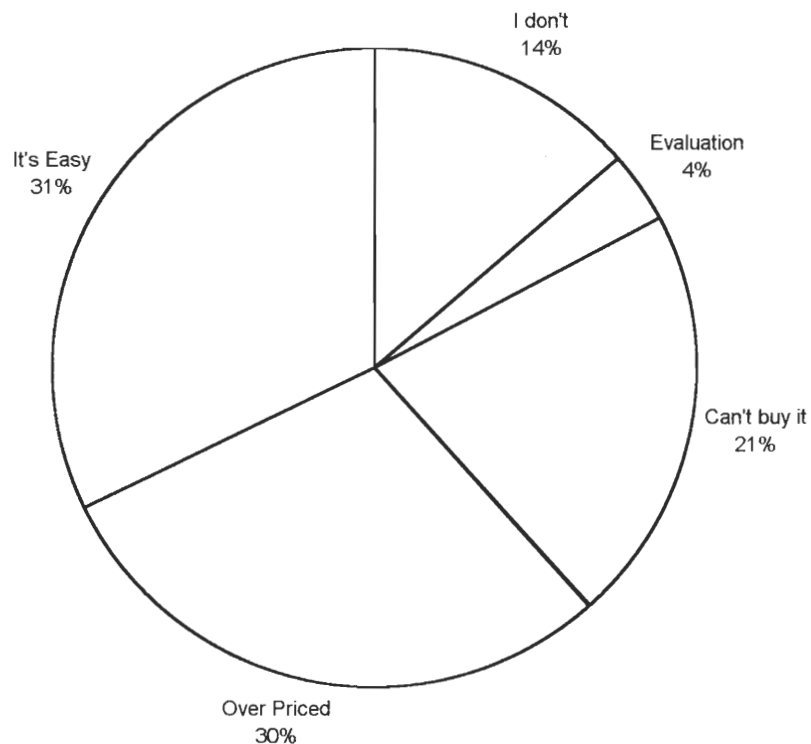
## 4 Analysis

This section contains our data, both in textual and graphical formats, along with many of the conclusions we drew from the data.

### 4.1 Results of the Student Survey

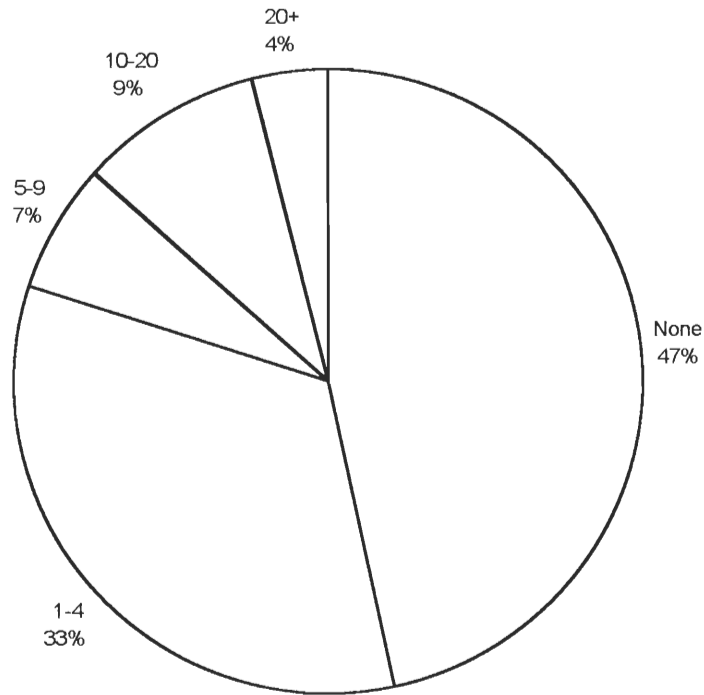
Below are the results of the survey, with each question listed in turn.

**Figure 4.1.1 : Reasons Students Pirate Software**



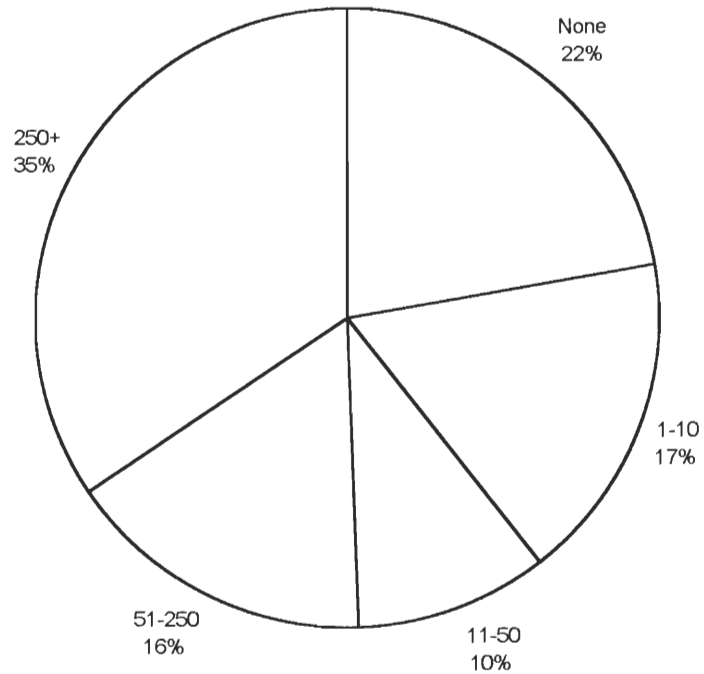
Question One of the Student survey suggests that 86% of students at WPI pirate software or music. Of all the students surveyed, I encountered none who said they did not fit into one of the five categories. Therefore, all of the piracy that takes place at WPI is because software / music piracy is easier and less expensive than buying the product, with the exception of the small group that downloads software illegally only for the purpose of evaluation.

Figure 4.1.2 : Computer Games Pirated in One Year



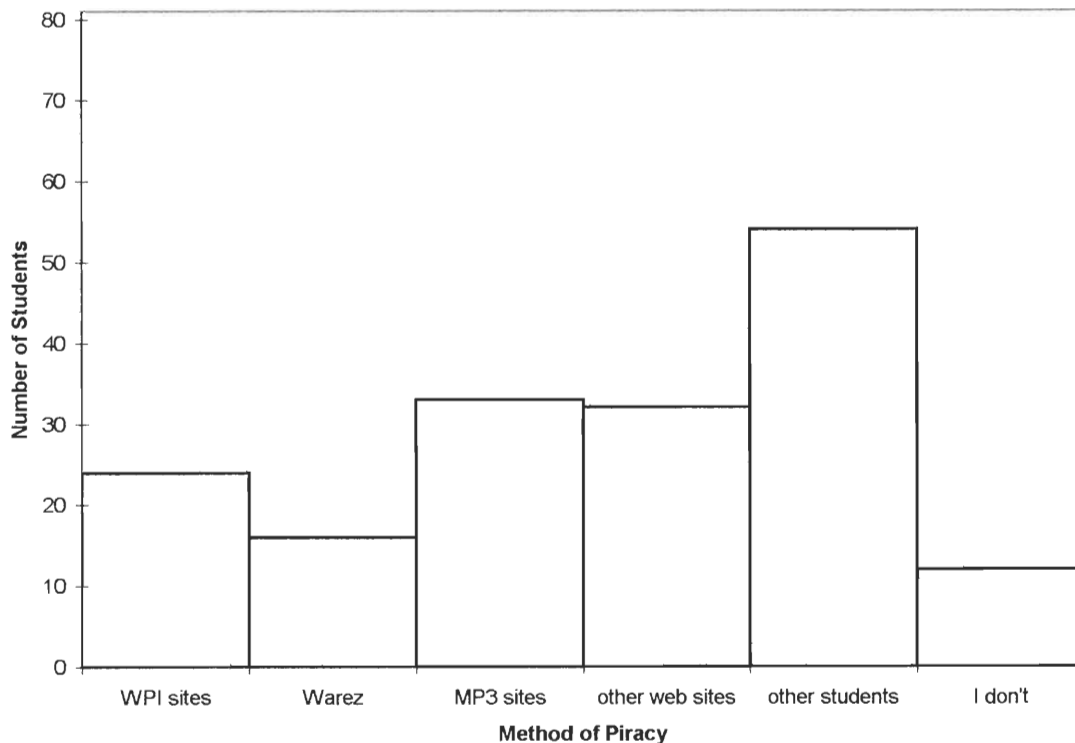
The data gathered for Question 2 shows that 53% of the student population steals computer games. However, of the pirate group 62% only take one to four games. Only 20% of the campus population steals five or more games in a year.

Figure 4.1.3. : Music Files Pirated in One Year



Question 3 reveals that pirating music is more popular than illegal computer games. Seventy-eight percent of WPI students obtain music without paying for it. Furthermore, 51% of the campus is downloading or trading large volumes of MP3's and other files (50+). Of the 250+ group, I encountered multiple students who suggested that the 250 limit was too low by five to ten times.

**Figure 4.1.4 : How Pirated Music / Software is Obtained**



The final question shows a preference among students for obtaining illegal software from their peers. This is most likely because it is far quicker than downloading these items. Sixty-seven percent of students use this method. Also of note is that 29% of students find illegal material on WPI maintained web sites. From the other categories it is clear that a large volume of illegal music / games is being downloaded to computers at WPI.

An item that could also have been added is a record of the gender of the students surveyed. It was noted that while well over eighty percent of males admitted to piracy, only fifty to sixty percent of females responded affirmatively. This is only an estimate, however there is almost certainly a correlation. Gathering this data might have caused difficulties, since it would detract from the perceived anonymity of the survey.

A separate question on business software or movie piracy might have been appropriate, however it was felt that four questions was the most that could be asked without potentially driving off students.

## 4.2. Analysis of the Policy Review

A cornerstone of the project, the policy review gave us some interesting, and surprising, results. The reader will find a pair of comprehensive graphs at the end of this section, figures 4.2.1, 4.2.2, and 4.2.3, which will be referred to in the writing. A quick glance at the graphs shows a great many low numbers where we were hoping to find high results. Although not unexpected, this is discouraging.

Twenty-nine separate requirements were decided upon as guidelines for the review, as described in the methodology section. The first discouraging statistic is that no policy in the review met all of the guidelines. Refer to Figure 4.2.1. Only one met more than twenty-five, and only five more met or exceeded twenty. The average policy met only eleven of the twenty-nine, and a full fifth of the policies reviewed met less than five. From this, it is clear that these policies require a good deal more work than is put into them.

The question, then, is what needs to be added to these policies? The purpose of Figure 4.2.2, is to answer this question. This graph shows us the ten requirements that half of the policies included, as well as the nineteen that were omitted in over half the policies. Among these nineteen include definitions of appropriate uses, penalties for violating state and federal laws, conditions for the restriction and removal of accounts, and conditions for criminal prosecution. When the lack of a requirement to report problems to the appropriate personnel and lack of requirement to pay legal fees to the school if laws are broken are added to this, we get a bleak picture of students who are told not to use unlicensed software, but aren't told why, or what the penalties are if they do, or who to report to if they see others pirating.

After the two graphs, the reader will find Figure 4.2.3., a list of the requirements used in this review, grouped into categories. Interestingly enough, the most-often discussed guidelines lie in the 'Responsibility of user' category, while the least-often included guidelines lie in the 'Rights/privileged of user' category. The most important groups, 'Definitions of appropriate uses' and 'Penalties' both rank low on the list of accomplished guidelines. In fact, the only group that is able to average above a fifty percent achievement rating is 'Responsibility of user,' with all other groups falling before the fifty-percent average level.

These numbers all create a very disturbing image of how poorly campus policies are equipped to deal with piracy. Working off of this data,

we have crafted a generic ideal policy for colleges and universities, which will be discussed in section 4.3.

Figure 4.2.1 : Requirements Met Out of 29

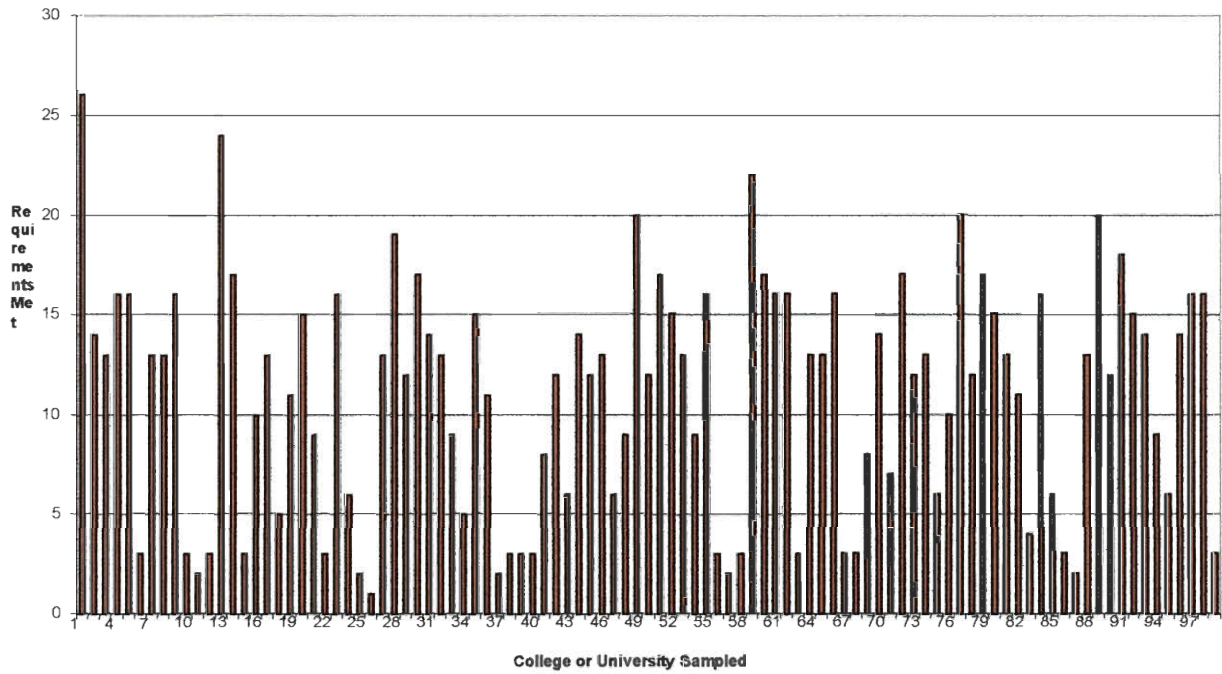


Figure 4.2.2 : Policies Meeting Requirements

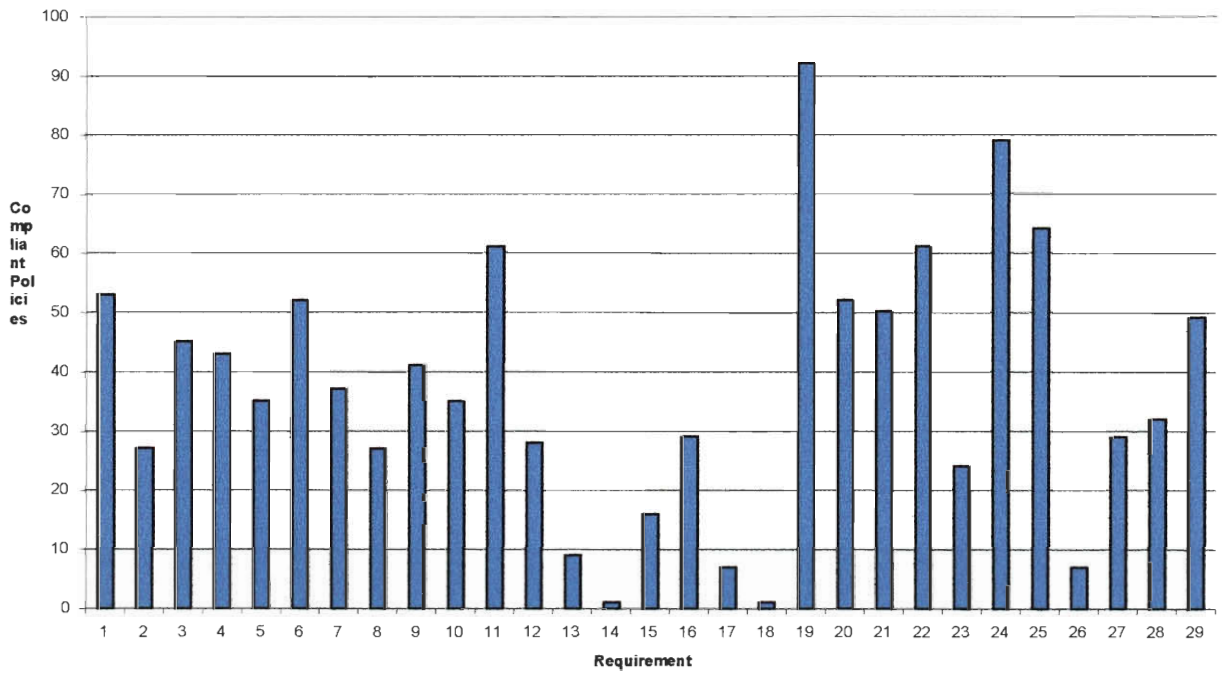


Figure 4.2.3 : Categorization Chart

x) Group Category	Requirement Number	Requirement
1) definition of appropriate uses	1	research and instruction
	2	email and Internet access
	3	must have an account to use
	4	not for personal financial gain
	5	not for inappropriate materials
2) penalties	6	for violating user agreement
	7	for violating state, federal laws
	8	conditions for restriction of account
	9	conditions for deletion of account
3) security of accounts	10	conditions for criminal prosecution
	11	who can read your files
	12	who can write to your files
	13	who can execute your files
4) rights/privileges of user	14	procedures for modifying account
	15	group software licenses
	16	access to computer labs, printers
	17	personal home page
5) responsibility of user	18	directory service
	19	software must be licensed
	20	respect privacy of other user accounts
	21	do not share accounts
6) authority of the school	22	have an acceptable password
	23	report problems to appropriate personnel
	24	correct use of school equipment
	25	refrain from abuse, profanity
	26	pay legal fees of school, if laws are broken
	27	stop abusive or wasteful actions
	28	limit disk space available to account
	29	system administrator's responsibility/authority



## 4.3 Ideal generic Policy

This generic policy can be used as an outline for an acceptable policy to be put into use at any American college. Each item is explained below.

- 1) definition of appropriate uses
  - 29 research and instruction
  - 30 email and Internet access
    - a. must have an account to use
  - 31 not for personal financial gain
  - 32 not for inappropriate materials
- 2) penalties
  - 33 for violating user agreement
  - 34 for violating state, federal laws
    - a. conditions for restriction of account
  - 35 conditions for deletion of account
  - 36 conditions for criminal prosecution
- 3) security of accounts
  - 37 who can read your files
  - 38 who can write to your files
  - 39 who can execute your files
  - 40 procedures for modifying account
- 4) rights/privileges of user
  - 41 group software licenses
  - 42 access to computer labs, printers
  - 43 personal home page
  - 44 directory service
- 5) responsibility of user
  - 45 software must be licensed
  - 46 respect privacy of other user accounts
  - 47 do not share accounts
  - 48 have an acceptable password
  - 49 report problems to appropriate personnel
  - 50 correct use of school equipment
  - 51 refrain from abuse, profanity
  - 52 pay legal fees of school, if laws are broken
- 6) authority of the school
  - 53 stop abusive or wasteful actions
  - 54 limit disk space available to account
  - 55 system administrator's responsibility/authority

### Definition of Appropriate Uses :

There were two differing opinions on appropriate use of the school's network and computer resources. While some schools allowed their use only for activities central to the school's mission, others allowed recreational activities and personal use, so long as these extras did not interfere with

research and other more important uses. Disallowing personal use of the network is only necessary for schools with very limited computing resources.

A user policy should explain if an account is needed to use the computing facilities or the network. Also, use of the computing facilities and network for personal financial gain or inappropriate materials should be prohibited.

#### Penalties :

The policy should list the penalties involved in breaking the user agreement or the law. This may cause readers to think twice about overlooking the policy. Conditions for restriction and deletion of an account should be clearly shown. Other penalties such as legal action against students can be explained.

#### Security of Accounts :

A section explaining who is allowed to read files in an account should be included. Besides the user of the account, campus authorities may be granted access if suspicion of illegal activity exists. Any unusual conditions for writing to or executing files should also be included. Procedures for modifying characteristics of the account, such as a password, need to be explained.

#### Rights / Privileges of User :

The privileges available to account users is useful information to anyone reading the policy. They can include personal home pages, directory services, group software licenses, and access to computer labs and printers.

#### Responsibility of User :

An important part of any computer usage policy is that software licenses must not be broken. If the university does not condemn software piracy, the piracy will continue unabated. Users all need to be reminded not to share accounts, to have an acceptable password, and to respect the privacy of other users. An email address or telephone extension should be available to report problems or suspected illegal activity.

The 'correct use of school equipment' covers several items. Physical theft of computer equipment must be prevented, as well as damage to the machines. This section may also include procedures for purchasing and installing software to school computers, which requires permission from the computer center or information technologies department, depending on the school. Also, attempting to 'crack' faculty or student passwords is unacceptable.

Students need to be reminded that profanity and other abuses are not tolerable and that electronic communications should be conducted in the same way that other forms are.

#### Authority of the School :

The school needs to establish its authority in the user policy. The right to stop wasteful actions and limit the disk space available to an account must be reserved. These wasteful actions may include chain letters, over use of the printer or tying up a large amount of resources without prior notification to the proper authorities. Any other responsibilities or activities of the system administrator should be listed as well.

#### Unnecessary Information :

A computer usage policy needs to be brief enough so that people can be realistically expected to read it. Too much legalese and information on Byzantine procedures clutter up the document. Defining obvious terms, such as the campus network, is also wasteful.

## 5. Conclusion

The background and results of this project show that software and copyright piracy are a serious problem in many places of higher learning. A vast majority of students are involved in these activities. This behavior is illegal and reflects poorly on the reputation of a university.

Education is one method of preventing software piracy. The schools policies should be stressed to students during their freshman orientation. Courses that involve computer use should also remind students of the appropriate uses of the network and computers.

Incentives for piracy should be removed when possible. A site license can be purchased for important educational software. Also, if students were given more convenient ways to purchase the software they needed, they would be less likely to steal it.

The university should monitor the network for suspicious activities, such as sites trading in pirated software. Shutting down these sites may decrease pirate activity. It would also free resources for academic work.

A computer usage policy is important to combating piracy. It should be distributed during orientation. However, by itself it is of limited utility. Proper enforcement is necessary for it to have maximum effect. In serious cases, legal action may be required. The appropriate set up of a software policy is discussed in a previous section. (see section 4.3)

Software and music piracy should be fought by every means available, in order to hamper these activities as much as possible.

## 6.0 Bibliography

- Associated Press, "Illegal Films Infiltrate Internet," April 22, 1999
- Associated Press, "Students Arrested in Software Case", April 14, 1999
- "INTERNET NETWORK A SOFTWARE PIRATES HAVEN DUE TO SLACK SECURITY—REPORT," Telecomworldwire, 1-4-94
- Jon Gaw, "Copyright laws headed for digital overhaul," Minneapolis Star Tribune, 5-4-98
- Boyd, Marvin J. "What is software piracy?" April 10, 1997
- Cohen Ph.D., Eli Journal of Information Systems Education, 3/89, "College Students Believe Piracy is Acceptable"
- Ross, Philip E., Forbes Magazine, "Cops versus robbers in Cyberspace" from Sept. 9, 1996
- Florida Computer Crimes Act (1988) at [www.med.ufl.edu](http://www.med.ufl.edu)
- Computer Underground Digest, "Ethical issues in hacking, phreaking, and piracy" 6/27/94
- "SPA Cooperates with FBI in Five Raids" June 1, 1998 at [www.spa.org](http://www.spa.org)
- Walz-Chojnackig, Greg, "Software Piracy - Avoid This Disk Error" [wc@csd.uwm.edu](mailto:wc@csd.uwm.edu)
- [www.microsoft.com](http://www.microsoft.com)
- "Analysis of Software Piracy," Digital Anarchy
- [www.paceap.com](http://www.paceap.com)
- "Parents Lead by Example: Don't Copy Software Illegally," [www.autodesk.com](http://www.autodesk.com)
- Hofer, Theresa, "Software Pirates Looking to You for Places to Stash Their 'WAREZ'" [www.itd.umich.edu](http://www.itd.umich.edu) 1/15/97
- Laprad, David, "Digital Anarchy : Analysis of Software Piracy" at [NewWorld.com](http://NewWorld.com), 1999
- Masland, Molly, "Software Piracy a Booming Net Trade" [www.msnbc.com/news](http://www.msnbc.com/news)
- "Online Thieves Collide with the Law," [www.msnbc.com/news](http://www.msnbc.com/news)
- [www.spa.org](http://www.spa.org)
- <http://www.usatoday.com/life/cyber/tech/ctd399.htm>
- <http://www.pclan.calpoly.edu/swpiracy.htm>