Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Use of Case Law in Negotiating the Acceptance of Post Secondary Computer Policies

This author provides a compelling argument to facilitate cooperation and compliance of adopting a policy scheme that will act as the first line of defense for organizations and provides a framework for the development of Acceptable Use Computer Policies.

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

February 6, 2003

SANS Security Essentials GSEC Practical Assignment
Version 1.3

George B. Koszegi
Date: Thursday, February 06, 2003

Re: **The use of Case Law in Negotiating the Acceptance of Post Secondary Computer Policies**

ABSTRACT:
One of the most important initiatives that an organization will undertake is the development of Acceptable Use Computer Policies. The Computer Security Specialist is usually confronted with a situation where individuals are reluctant to accept the implementation of these policies. These individuals often include system, network and database administrators. They often believe that their functions are more important than security related issues and therefore security will be a forgotten entity until a security related incident has occurred. It is the intent of this paper to provide a compelling argument that will facilitate cooperation and compliance by persuading all individuals that there is little or no choice but to adopt a policy scheme that will act as the first line of defense for their organization. Hopefully this paper will assist the reader in facilitating cooperation and "buy in" while providing a framework to establish their policies.

INTRODUCTION:
I was tasked with the responsibility of developing computer use policies for a post secondary institution. This organization was composed of approximately 3000 workstations, 70 servers and a student population of:

- Total individual credit students - 11,210
- Annualized full-load equivalent - 6,457
- Continuing Education registrations - 38,206
- Languages Institute and International registrations - 3,483
- Conservatory course registrations - 9,610

Before developing the policies, it was evident that an open academic environment required a consensus rather than a dictatorial approach to introducing an action that could potentially limit the freedom of its users. As this would be a dramatic shift in the computing philosophy of the organization, it was determined that the presentation of case law would provide a convincing rationale for the implementation of the proposed policies. It is important to note that not all cases deal specifically with post secondary institutions, however, post secondary institutions could be subject to each of these situations.

This paper will be divided into a number of sections that will introduce concepts that are supported by current legal decisions from Canada and the U.S. It will begin by examining the fundamental issues that impact an organization:

A. Computer Policy and Policy Implementation.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Are computer policies key instruments that regulate computer use?
- Do banners and policies limit an employee's reasonable expectation of privacy?
- What online mechanism will be used to disseminate Acceptable Use Policies and provide a binding contract?

B. Defining Liability.
- Direct liability.
- Downstream liability.
- Reasonable precautions vs. due diligence.
- Criminal Activity Facilitated by Email (threatening email, fraud, cyber stalking etc).
- System Intrusions from within or outside an organization – This type of attack will effect an organization by compromising the following:
  - I) Confidentiality/Privacy – unauthorized access or theft of private information.
  - II) Integrity – the alteration of information.
  - III) Availability – the disruption of computer services.
- Manipulating Computer Resources to launch a Denial of Service (DDOS) attack against an outside organization. This is the most common type of attack and its main purpose is to disrupt the ability of an organization to carry out its normal course of business.

C. Factors effecting Information Technology Staff.

D. Software piracy.

These examples should provide sufficient impact to convince any organization that Acceptable Use Policies are essential to ensure that an organization mitigates its liability.

After an organization has been convinced that they must have an Acceptable Use Computer policy, they need a mechanism that will assist them in its development. In a post secondary institution, the methodology of developing the policy is very important as the document must satisfy a number of groups that may have competing interests. In this section the four month process that led to the development of the policies will be detailed. The discussion will be concluded with the presentation of sample templates that can be used in the development of various Acceptable Use Computer Policies. The last three sections are as follows:

I) Methodology for the development of Acceptable Use Policies.
II) Conclusion
III) Sample Policies for Post-Secondary Institutions.

A) Computer Policy and Policy Implementation:

Computer policies are the key instruments that are used to regulate computer use. In Canada, the case Blaber v. University of Victoria outlines the importance of not only developing

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

computer use policies but having the user acknowledge them. In this case, the petitioner sent a threatening email message to a member of the board of governors. Upon receiving the message, the recipient was "immediately distressed and frightened". In response to the email, Mr. Blaber's user account was suspended because he violated the University policy according to the "Computer User Responsibilities". Mr. Blaber then took action against the University of Victoria via the British Columbia Supreme Court to seek a remedy for the University's actions. The court ruled the following:

- *"... the University and its Department of Computer Science limits the use of the University-paid accounts by students in accordance with the policy of use which is specifically agreed to and accepted by the students before issuance of account privileges."* (Blaber, p.2)
- *"I further find that the petitioner agreed to this policy of use prior to obtaining his computer privileges."* (Blaber, p.2)
- *"I find support for my conclusion that the Charter does not apply to the case at bar in the wording of section 46.1 of the University Act which reads:* ***46.1 (1)*** *The minister shall not interfere in the exercise of powers conferred on a university, its board, senate and other constituent bodies by this Act respecting* ***(a)*** *the formation and adoption of academic policies and standards,"* (Blaber, p.9)
- *"…I observe that on the whole of the evidence I am not persuaded that the conduct of the respondents constitutes an infringement of the petitioner's right to "life, liberty and security of the person" or his right to "freedom of expression" as guaranteed by the Charter."* (Blaber, p.9)
- *"In the case at bar, the Harassment Policy is really best characterized as a set of rules establishing the boundaries of acceptable behavior for all members of the University community, including visitors. In essence, the Policy defines the limits of "academic freedom".* (Blaber, p.10)

This has become a landmark case in Canada because the Judge determined that the Computer Acceptable Use policy was a valid document that could be used as a legislative guide in regulating computer use. Once the policy was accepted by the court, it could be used as a standard to measure acceptable use. The Judge also identified a key element that must be present in order to validate the use of the policy. This element is an agreement between the organization and the user. In this case, the petitioner (Mr. Blaber) attempted to nullify the computer use policy by stating that it infringed upon his Charter of Rights and Freedoms (civil rights). He further stated that his other rights: the right to life, liberty, security and freedom of expression were also violated. None of these defenses were accepted by the court as it was determined that both parties accepted the terms of the contract in regulating computer use.

The U.S. has made similar rulings when dealing with computer policies and they have broadened the interpretation of the effects of legislation on an employee's reasonable expectation of privacy. In reviewing the "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" report (published January, 2001 and prepared by the Computer Crime and Intellectual Property Section, Criminal Division of the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

United States Department of Justice), I have extracted the sections that deal specifically with an employee's expectation of privacy. These cases can be summarized as follows:

- "*…courts have agreed with the approach articulated in Simons and have held that banners and policies generally eliminate a reasonable expectation of privacy in contents stored in a government employee's network account. See Wasson v. Sonoma County Junior College, 4 F. Supp.2d 893, 905-06 (N.D. Cal. 1997) (holding that public employer's computer policy giving the employer the right to access all information stored on the employee's computer defeats an employee's reasonable expectation of privacy in files stored on employer's computers); Bohach v. City of Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (holding that police officers did not retain a reasonable expectation of privacy in their use of a pager system, in part because the Chief of Police had issued an order announcing that all messages would be logged); United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000) (holding that Air Force sergeant did not have a reasonable expectation of privacy in his government e-mail account because e-mail use was reserved for official business and network banner informed each user upon logging on to the network that use was subject to monitoring).***"** (CCIPS, p.11)

These cases provide two additional elements that will help guide the Computer Security Specialist in determining the scope of the computer policy. Firstly, the policy must be communicated to the user in a form where it can be established that the user had knowledge of the existence of the policy. This is usually made available to all employees at the point of log on and it can be in the form of a banner. Secondly, if it can be established that the users had knowledge of the policy then they automatically waive their expectation of privacy. This was a very contentious issue during our policy development process. If the organization provides a reasonable expectation of privacy, then that same organization has no right to inspect its computer systems. This could lead to chaos in an organization and it could prevent the system administrators from performing routine maintenance on any system that stores user data. This potential problem was removed from our policies as we extended the expectation of confidentiality and not privacy to our users.

The last component in this category is the implementation of the various acceptable use policies. The U.S. courts have ruled that the click wrap agreement is a binding form of an online contract. In the case ***Steven J. Caspi, et al. v. The Microsoft Network, L.L.C., et al.***, 1999 WL 462175, 323 N.J. Super. 118 (N.J. App. Div., July 2, 1999), the court ruled the following:

- *"On this appeal, the Appellate Division affirmed the determination of the Superior Court of New Jersey that the plaintiffs had entered into a binding contract by agreeing on-line via the click of a mouse to be bound by the terms of the Microsoft Network's subscriber agreement. The terms of this agreement appear in a scrollable window next to blocks containing the words "I agree" or "I disagree." The user cannot commence use of the Microsoft Network unless she clicks the "I agree" button. Each of the plaintiffs clicked the "I agree" button, thereby indicating their assent to be bound by the terms of the subscriber agreement. Both the trial and appellate courts held this created an enforceable contract between the defendants and their subscribers."*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- In a second case, ***Groff v. America Online, Inc.***, File No. C.A. No. PC 97-0331, 1998 W L 307001 (R.I. Superior Ct., May 27, 1998, the court gave the following opinion:
  "Our Court ... stated the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively "signed" the agreement by clicking "I agree" not once but twice. Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement."

The final piece of the puzzle is to be able to prove that the users were presented with the opportunity to read the Acceptable Use policy at each log on. It was determined that it was simpler to have the policies presented at each log on with an "accept" button than to manage the log on acceptance in a data base. This ensures that the user cannot use the defense that he/she did not see the policy at a particular log in and therefore felt that the policy did not apply to that particular computer session.

Both cases clearly demonstrate that this type of click wrap agreement is held as a binding contract between both parties and therefore it can be used as an instrument to convey agreement for acceptable use computer policies.

B) Defining Liability:

The two basic types of liability that effect organizations that utilize information technologies are:

- Direct liability – This type of liability could result from individuals sending offensive email to one another, exposing sensitive company information to the Internet, or offending a third party while viewing offensive material on a computer monitor. Incidents which result in the offending of a third party are usually categorized under legislation that regulates hostile work environments. This type of case was highlighted in an article in the CIO Insight Magazine (September edition) which stated:
  - *"In late May 2001, the U.S. Equal Employment Opportunity Commission determined that the Minneapolis Public Library may have permitted a hostile work environment by giving library patrons unfettered access to the Internet, which resulted in the display and printing of explicit sexual images on the library's public Internet terminals. This determination gives the affected employees the right to file a federal civil rights lawsuit for compensatory and punitive damages. The EEOC is reported to have suggested a settlement that would have required the library to pay each of the complaining employees $75,000 in damages. The employees, of course, may sue for more."* (Scott, p69)

  This case effectively provided the rationale for limiting the location of where research concerning sexually explicit material could be conducted. During our hearings, representatives from our library insisted that limiting research in sexually explicit material was a form of censorship and it violated the principles of an open academic

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

environment. The position, that some individuals may find the material offensive was rejected by the staff. This case provided sufficient evidence to convince the staff that if this type of research was to be conducted in a public area then special care must be taken to ensure that individuals would not be subjected to material that may be deemed offensive. The simple solution to this problem was to ensure that this type of research be conducted in a reasonable private location.

- Downstream liability – This concept is described in an article in SC Security Magazine, August 2001, Liability Worries:
  - *"Downstream liability, too, is fast becoming a frequently discussed term nowadays. When attackers use various companies' equipment without their knowledge to launch their assaults it could be possible for victims to file suits against those e-businesses and service providers that are found to be lax in their security controls. With distributed denial-of-service (DDoS) attacks on the increase, companies used as unknowing pawns could very likely be held accountable in the near future, adds Predictive's Rasch."* (Armstrong)

This new concept should be included in a company's Acceptable Use computer policy so that all users are aware that not only is this behavior unacceptable but it could translate into liability of both the user and the organization. It is important to note that if this type of activity is generated from within a company, all effort should be made to ensure that the liability is passed from the organization to the user/offender. In order for the company to escape or mitigate their liability, they will have to establish reasonable precautions to prevent the occurrence of the activity.

The SC Security Online Magazine article outlines two principles that should guide companies in limiting their liability. These principles are:

- Reasonable precautions: *"A company will, generally, not be held liable, or may at least avoid punitive sanctions, for actions that it took reasonable precautions to prevent. However, reasonableness is a sliding scale based on knowledge of a threat, ability to avoid that threat, and the sensitivity or potential liability caused by the threat…"*. (Armstrong)
- Due diligence: *"An organization must meet the standard of due diligence to minimize potential liability from information security breaches. In effect, due diligence requires managers to implement standard business practices and take precautions that a reasonable business manager in their business environment would take."* (Armstrong)

These articles should send warnings to all organizations that believe that it is sufficient to develop their security policies and then place them on a shelf to collect dust. As threats continue to develop and mutate, the computer security role will continue to change. In order to ensure that an organization is able to mitigate their liability, they must progress past the policy stage and develop an aggressive vulnerability analysis and intrusion detection strategy. Organizations must also have a good understanding of the types of threats that threaten their computer systems.

1) Criminal Activity Facilitated by Email:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This section can be divided into three categories: cyber stalking, fraud, and email abuse. The advent of information technology has spawned a new conduit that facilitates old crimes. In the 1999 Report on Cyber stalking (A report from the Attorney General to the Vice President, August 1999), they defined and examined this new phenomenon.

- *"Although there is no universally accepted definition of cyber stalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat.[(1)] While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously."*
- *"First, data on offline stalking may provide some insight into the scope of the cyber stalking problem. According to the most recent National Violence Against Women Survey, which defines stalking as referring to instances where the victim felt a high level of fear:[(3)]*
  - *In the United States, one out of every 12 women (8.2 million) and one out of every 45 men (2 million) have been stalked at some time in their lives.*
  - *One percent of all women and 0.4 percent of all men were stalked during the preceding 12 months.*
  - *Women are far more likely to be the victims of stalking than men - nearly four out of five stalking victims are women. Men are far more likely to be stalkers - 87 percent of the stalkers identified by victims in the survey were men.*
  - *Women are twice as likely as men to be victims of stalking by strangers and eight times as likely to be victims of stalking by intimates."*
- *"…as part of a large study on sexual victimization of college women, researchers at the University of Cincinnati conducted a national telephone survey of 4,446 randomly selected women attending two- and four-year institutions of higher education. The survey was conducted during the 1996-97 academic year. In this survey, a stalking incident was defined as a case in which a respondent answered positively when asked if someone had "repeatedly followed you, watched you, phoned, written, e-mailed, or communicated with you in other ways that seemed obsessive and made you afraid or concerned for your safety." The study found that 581 women (13.1 percent) were stalked and reported a total of 696 stalking incidents; the latter figure exceeds the number of victims because 15 percent of the women experienced more than one case of stalking during the survey period. Of these 696 stalking incidents, 166 (24.7 percent) involved e-mail. Thus, 25 percent of stalking incidents among college women could be classified as involving cyber stalking.[(5)]"* (Attorney General)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

These statistics are very concerning because many post secondary institutions provide unfettered computer access to their students. The unfettered access is consistent with the open academic philosophy; however it presents a large potential liability.

The next threat effects all organizations that utilize computer technology to facilitate communication. With the advent of email an organization must be concerned with its potential uses and abuses. A clear case of abuse and potential third party liability is presented in the U.S. Department of Justice case:

- *"A federal grand jury in Los Angeles today indicted a Southern California man on charges that accuse him of fabricating a press release that led a publicly traded company to temporarily lose more than $2 billion in market value. Mark Simeon Jakob, 23, of El Segundo, was named in an 11-count indictment for causing numerous investors to suffer millions of dollars in trading losses because of his distribution of a false press release. Jakob is a former employee of Internet Wire and until recently was a student at El Camino College, where the computer used to send the bogus press release was located."* (Emulex)

In addition to prohibiting this type of behavior via a policy document, it is important to have sufficient auditing capabilities in a network so that there is a reasonable expectation of a successful conclusion to this type of investigation. I suggest that liability may potentially be mitigated if auditing measures have been incorporated into the network environment. When confronted with the possibility in sharing in a percentage of a $2 billion dollar loss, purchasing additional storage media to ensure that audit logs are kept for a reasonable length of time appears to be inexpensive insurance.

2) System Intrusions from Within or Outside an Organization:

Examples outlining what could happen when a person obtains unauthorized access to University computer systems is outline in three articles. The first article is a U.S. Department of Justice news release titled, Orange County, California Computer Hacker Pleads guilty to Hacking University Computers, Defrauding Western Union:

- *"A Mission Viejo man plead guilty this morning to federal charges of hacking into computers at Oregon State University and using stolen credit card numbers in an attempt to wire transfer money through the Western Union Corporation. According to statements made in court today, as well as a criminal complaint filed in April after his second arrest, Diekman used his personal computer at home to gain unauthorized access to computers at Oregon State University in Corvallis, Oregon. Diekman hacked into the university's computers 33 times from February through April of this year. Diekman used the account of an OSU student to gain access to the school's computer system, where he stored computer programs to control Internet Relay Chat channels on the Internet.*

The second article is titled, "Russian Computer Hacker Convicted by Jury":

- *Francis J. Diskin, United States Attorney for the Western District of Washington, and Charles E. Mandigo, Special Agent in Charge, Seattle Division, Federal Bureau of Investigation, announced that a jury returned guilty verdicts yesterday against*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

VASILIY GORSHKOV, age 26, of Chelyabinsk, Russia, on 20 counts of conspiracy, various computer crimes, and fraud committed against Speakeasy Network of Seattle, Washington; Nara Bank of Los Angeles, California; Central National Bank of Waco, Texas; and the online credit card payment company PayPal of Palo Alto, California. Sentencing for GORSHKOV is scheduled before Chief United States District Judge John C. Coughenour in Seattle at 9:00 a.m. on January 4, 2002. GORSHKOV faces a maximum sentence of five years in prison on each count, for a total statutory maximum of 100 years in prison, as well as a maximum fine of $250,000 on each count."

In addition to the above, vulnerabilities in network systems can span both liability and monetary loss. The U.S. Department of Justice recently published a case that depicts what can happen when a person gains illegal access to a College's telecommunication system:

- *"Patrick W. Gregory also used these unauthorized access devices to listen in and/or disrupt teleconferences of legitimate third parties using the telecommunications services of these victim companies. Specifically, in June 1998, Gregory participated in an AT&T teleconference for which he and others caused billing in excess of $4,200 to an innocent third party for using these conference services. In October 1998, Gregory, using stolen teleconference access information from Latitude Communications, gained access to Dallas Community College District's teleconference system and caused teleconference classes at the College to be disrupted and caused a telephone charge in excess of $18,500.00 to be made to the College."* (Gregory)
- *"United States Attorney Paul E. Coggins announced today that Patrick W. Gregory, also known as "MostHateD," was sentenced today in federal court by the Honorable United States District Judge Jorge A. Solis to 26 months imprisonment; three years supervised release, and was ordered to pay $154,529.86 in restitution. Gregory, age 20, of Houston, Texas, had pled guilty in April to conspiracy to commit telecommunications fraud and computer hacking, a violation of Title 18, United States Code, Sections 371, 1029 (a)(2) and 1030 (a)(5). Gregory was immediately taken into custody."* (Computer Hacker Sentenced)

In the first two cases the post secondary computer systems are being used as conduits to facilitate the various crimes. In the third example, the hackers are actually causing a monetary loss to occur to the educational facility. This example provides a different type of threat to post secondary environments. Educational institutions do not suffer the same types of losses as business because their operations do not generate revenue on a daily basis. Their business model focuses on specific times of year when they receive revenue through student registration. Therefore they do not suffer the traditional losses that are associated to profit driven businesses. This case illustrates that educational institutions must guard against losses associated to liability and revenue.

3) Manipulating Computer Resources to Launch a Denial of Service (DDOS) Attack:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

One of the most notorious cases of a DDOS attack involved a young offender and an American University computer. The article "Meet the World's Baddest Cyber Cops" accurately depicts the exploits of Mafia Boy:

- *"On Monday, February 7, 2000, a 15-year-old from suburban Montreal with the online moniker Mafiaboy launched a weeklong Internet attack on Yahoo, CNN.com, Amazon.com, eBay, Dell, Buy.com, and several others, causing losses estimated in the millions.*
- *Mafiaboy was not a sophisticated hacker. He begged the software—now widely available on several Internet hacker sites—from other hackers and then used it to break into and gain root access to more than 50 servers, most of them located at American universities. He then used those servers to launch his assault.*
- *Investigators were able to trace the attacks to Mafiaboy by examining the log files of a computer at a University of California at Santa Barbara research lab, which was among those used to attack the CNN.com site.*
- *Judge Gilles Ouellet ruled that the 17-year-old teenager from Montreal committed a criminal act when he crippled major internet sites like Amazon and Yahoo last year, causing an estimated $1.7 billion in damages.*
- *The judge also ordered the teenager to face one year of probation after his detention ends, and fined him $160."* (Galvin)

This example has been included to demonstrate the insecurities of many computer systems. It also demonstrates the constant need to examine and re-examine existing systems in order to ensure that vulnerabilities have been resolved. With the proliferation of peer to peer systems (i.e. Morpheus etc) it is becoming easier to disseminate hacker related tools to the masses. As these tools become the future trading cards of the virtual play ground, the threat organizations will increase exponentially.

C) Effect on Information Technology Staff:

The next issue is one that will dramatically affect the way most organizations conduct their business. Most system administrators do not feel that it is their responsibility to police their networks. This will no longer be a philosophical, ethical or moral debate as various government agencies have enacted legislation to regulate this issue. The legislation effecting Information Technology Staff has undergone significant change in South Carolina. In an article published in Information.com, the state legislature expanded the work responsibilities of technology support staff. The legislation is summarized as follows:

- *"Techies in that state are now required to give authorities the names and addresses of computer users with child pornography on their machines. The law doesn't compel IT workers to search for child pornography, but it does require them to report it upon discovery. It's an extension of an existing state law that requires film processors to report child pornography when they see it at their facilities. The law doesn't establish any penalties for techies who neglect to report pornography, but that's "an oversight," says Sharon Gunter, staff attorney for the South Carolina Senate. When the state legislature resumes next year, she expects the law will be changed to include penalties of no more than six months in jail or no more than $500 in fines (or both)--*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the same as the current penalties for film developers who don't tell authorities about child pornography they discover." (Swanson)

In a follow-up article dated August 8, 2001, additional modifications were made to the legislation:

- *"In addition to having to report child pornography found on computers to the authorities, they're required to report child abuse and neglect. Computer technicians have been added to a list of professions--including nurses, dentists, schoolteachers, and undertakers--who must report to county officials if they have reason to believe that a child's physical or mental health "has been or may be affected by abuse or neglect". It protects IT professionals from civil and criminal liability if they report in error, but it doesn't protect them if their actions are proven to be malicious."* (Swanson)

The introduction of this type of legislation foreshadows what can be expected in Canada. This type of legislation will force the development of a Code of Conduct for IT support staff.

D) Software Piracy:

Software Piracy has moral, ethical, and legal implications for an organization. In examining this topic it is important to understand the different categories of software piracy. Software piracy can be divided into the following categories:

- **Under-Licensing** - When large corporations or government departments purchase fewer software licenses than the number actually being deployed on desktops in the organization.
- **Consumer Copying and Downloading** - When an employee or consumer copies software from work or home and shares it with friends or when pirated software is downloaded from the Internet.
- **Academic Product Leakage** - When academic product (intended to be sold to people involved in education at a discount price) is illegally sold to people who are not a part of the education industry.
- **Hard Disk Loading** - When unlicensed software is illegally loaded onto the hard drive of a new computer without providing the purchaser with software media, manuals, licenses, etc.
- **Counterfeiting and Rental**

In reviewing the news releases on the CAAST (Canadian Alliance Against Software Theft) web site, it is evident that they have mounted an aggressive campaign against software piracy. In an article titled, "CAAST applauds crackdown on international software piracy ring" a Quebec University Web site was used to store over $1 million U.S. worth of pirated software:

- *"Toronto, ONT, May 10, 2000 -- The Canadian Alliance Against Software Theft CAAST) commends the investigation that resulted in a one count indictment of seventeen individuals for conspiracy to infringe*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

copyrights. According to the indictment, all of the defendants were either members or contributors to "Pirates with Attitudes" (PWA), an underground group that disseminates stolen copies of software programs and was working through a hidden Web site located at a Quebec university.

Supported by computers based in the University of Sherbrooke, Quebec, the hidden site stored large amounts of pirated software accessible to pirates who had secret passwords. FBI and Canadian authorities seized those computers earlier this year.

Two unidentified group members that were affiliated with the University of Sherbrooke, Quebec, helped authorities crack the case. The two were part of the "PWA" software piracy ring for years before they began to cooperate with the authorities.

The indictment issued by the U.S. Attorney's Office charges that the defendants who were members of the "Pirates with Attitudes" software group resided in various states across the U.S. and in Europe. According to the indictment, at various times between January 1998 and January 2000, more that 5,000 copyrighted computer software programs were available for downloading on a restricted Internet site operated by PWA. The programs included operating systems, utilities and applications such as word processing and data analysis programs. While the site was operating, more than 1,200 gigabytes of software were uploaded and more than 4,300 gigabytes were downloaded. (Walker)

In a second article titled "Toronto Student Faces Criminal Charges for Distributing Copyrighted Software and Pornography" a student utilized the York University computer systems to establish an international software and file distribution center. The article provided the following information:

- *"TORONTO, Ont. — December 15, 1998 – A York University student will appear in Newmarket Provincial Court today for a judicial pre-trial relating to charges of illegal software distribution, fraud over $5,000, possession of child pornography and circulation of obscene material. Twenty-nine year-old Wei-Tai Lee of North York faces a combined maximum penalty of 22 years imprisonment on a conviction of indictment, a fine up to one million dollars, or both.*

  The charges are the result of a six-month RCMP investigation alleging that Lee was illegally distributing copyrighted software via York University's Internet service provider. The RCMP obtained a search warrant based on the suspected software distribution and seized Lee's

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

hard drive. While gathering forensic evidence from the hard drive, investigators determined that it contained numerous images of child pornography and other obscene photographs.

The student's file transfer protocol (FTP) site, is suspected of being part of a worldwide group of 10 mirrored web sites engaged in similar illegal activity. The web site allegedly included a wide variety of copyrighted software that ranged from business applications, to computer games to high-end developer tools. The site listed numerous software titles available for download, and illegal copies of software were made available from many major software publishers.

The RCMP first learned of the illegal web site when they received a call from the network administrator at York University. The administrator became suspicious when a noticeable percentage of the university's bandwidth was used by one designate connection. An investigation led the RCMP to Lee, and a search warrant was obtained to collect evidence from his computer hard drive." (Alletson)

It is clear from the above information that adequate precautions must be taken in order to mitigate liability that may be perpetuated against an organization through the conduit of information technology. The first line of defense is the development of comprehensive Acceptable Use Computer Policies. Once the policies are developed users must be trained and technology must be deployed in order to ensure that the principles of the policies are maintained.

I) Methodology for the Development of Acceptable Use Policies:

Before beginning this type of project, the Computer Security Specialist should ensure that sufficient time is allocated to the development of the security policies. This project was completed in four months and could not have been completed sooner as there were numerous scheduling difficulties with the various individuals that took part in the process. I had a tremendous advantage during this project as senior management had decided that the implementation of Acceptable Use Computer policies were a priority for the institution. This endorsement was extremely important and without this support the project would not have succeeded. The next step was to develop a draft copy of the various policies. Once these policies were developed, they were presented to a number of groups, committees and associations. Information sessions were also conducted with the general Faculty, Support Staff, and Student populations. These meetings produced a tremendous amount of spirited debate and the policies were amended to satisfy the interests of the various groups. It was stressed that the goal was consensus and each of the participants were required to be flexible without compromising their specific interests. In order to ensure that the basic principles of the policies were maintained, the documents were later reviewed by the College's lawyers to ensure that the best interests of the College were preserved.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

This may appear to be the completion of the process but it merely signified the transition from Phase I to Phase II. The policies had been approved but there was no system to ensure that the users had the opportunity to view the policies. I was convinced that the best approach to the dissemination of the policy documents would be to have a log on banner that would require the user to press either "accept" or "log off". This would ensure that a user could not use the computer systems unless they agreed with the policy. A meeting was then scheduled with the network and server administrators and they were requested to develop and implement this log-on system. During the course of this meeting they presented a number of reasons why this form of implementation would not work. The meeting became very animated and it ended with a resounding "no" to this and any other form of electronic policy dissemination. It appeared that members of the group were resistant to this idea because they did not have the time to develop a program that would provide the log on banner. This problem initially appeared insurmountable however our Director was able to find another institution that developed a similar program. They were willing to share their code and within a few short weeks our network administrator developed a working program. Within an additional two months the program was disseminated to the users.

II) Conclusion:

This paper has been structured as a resource for the development of Acceptable Use computer policies. There should be sufficient examples included in this paper to convince anyone of the importance of the development and implementation of these policies. Sample policies have been included below to assist in the development of Acceptable Use policies. In many respects we are guided by threats and liability. Both areas must be addressed in order to maintain the viability and safety of an organization. The Computer Security Professional should be a vital part of all organizations and they should concentrate their efforts on; policy development, anti-virus protection, vulnerability analysis, intrusion detection, and software auditing. The monitoring of these components should eliminate risk and mitigate potential liability.

III) Sample Policies for Post Secondary Institutions:

Acceptable Use Policy for College Computer Resources:

INTRODUCTION: This is a College-wide policy pertaining to computers, to data networks and to the resources these technologies make available in support of the College. It applies to any devices and/or computers owned by the College as well as those owned by individuals who have been authorized to install or connect personal equipment either on the premises or to the network. In this context, the College community includes: all registered students, both full-time and part-time; all paid employees, full-time, part-time and casual; all others associated with the College such as board members, consultants, contractors (and their employees), retirees, volunteers, and such visitors as are granted temporary user status by the College.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

< College Name > encourages the use of computing and network resources to enhance the learning and working environment of the College community. However, access to the computing and network environment at < College Name > is to be used in effective, ethical and lawful ways that support the values of the College. The College will endeavor to create an atmosphere that balances respect for individual computer users and College facilities while maintaining the ethical and community standards of the College.

COLLEGE COMPUTER RESOURCES: The College computer resources are defined to include but not limited to such devices as personal desktop computers, laptop computers, monitors, hard drives, printers, scanners, network devices, Personal Digital Assistant devices (PDAs), network routers, network bridges, network switches, servers, the College network (LAN, WAN and Internet gateways), computer labs, software acquired by the College and relevant data. This section is also extended to include any computer system that is owned or managed by the College regardless of its location.

SUPPORT: < College Name >'s Information Technology Services Department is available to assist, advise and consult with users on the proper use of College computer resources and interpretation of this policy. If there are any questions or uncertainty about this policy, users are encouraged to contact the Director of the Information Technology Services Department or his/her designate for clarification. There is also a separate document called the Code of Conduct for Technology Support Staff which regulates the activities of all Technology Support Personnel.

PRINCIPLES

1. Computing and network resources are provided primarily to support and further the College mission.
2. Individuals using College owned computer technology resources are expected to comply with provincial and federal laws and relevant < College Name > policies and procedures. Some of the material used at the college is copyrighted, protected by intellectual property law and/or license agreements. Members should undertake reasonable efforts to ensure that they do not violate the various laws, policies, procedures and license agreements.
3. Members of the College community are responsible and accountable for their actions and statements in the electronic working and learning environment, according to the disciplinary policies of the College.
4. Members are expected to use reasonable restraint in consumption of these valuable shared resources, and to use them in ways that do not interfere with the study, work or working environment of other users.
5. < College Name > computers, systems, networks and data should primarily be used for College educational, research and administrative purposes.
6. Any data stored by or transmitted to members of the College community is confidential and will not be accessed by the College without just cause and due process. In any circumstances of alleged impropriety, formal procedures permit persons responsible for computers or networks to request specific institutional authorization to examine directories, files, email or other electronic records that are relevant to the investigation of the allegation.
7. In addition, College users accessing external networks are bound by their policies, and the more restrictive policy will apply.

15

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

8. Anyone who observes actual or apparent use which appears to violate the Student Computing Resources Acceptable Use Policy and/or the Acceptable Use Policy for College Computer Resources is encouraged to seek further information from the Information Technology Services Department.

UNACCEPTABLE USES: *(Unacceptable uses as outlined here are not limited to these examples)*

Unauthorized access (hacking): This may include using unauthorized user names, passwords, computer addresses or identities or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or "crack" security provisions of College or external systems. The Criminal Code of Canada has two related sections: Section 342.1 Unauthorized use of computer and Section 342.2 Possession of device to obtain computer service

Unauthorized Distribution and Disclosure of Information: Every effort must be made to prevent the unauthorized disclosure and distribution of information that is the property of < College Name >.

Vandalism of data: Deliberate alteration or destruction of computer files is a Criminal Code offence (Section 430.1). Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access. The Freedom of Information and Protection of Privacy Act (FOIP) also deals with deliberate destruction of data.

Interference with other users' work: This includes use of any process that causes a user to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of "spam (excessive email distribution)," and the introduction of viruses or electronic chain letters.

Squandering resources: Resources are shared and no user may degrade the systems by: unwarranted data space, time and bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs. As the use of College resources changes and the technology capabilities change over time – users are encouraged to work with the Information Technology Services Department in the defining appropriate and efficient uses of computer resources.

Personal uses: The College computer resources are to be used primarily for College business purposes (i.e. instruction, teaching, educational research and administration). All users have the responsibility to ensure that incidental personal use of College computer resources does not interfere with the normal course of their duties. Incidental personal use of computers would include but is not limited to personal email.

Telecommuting: Incidental personal use of < College Name > and/or any other computer systems that are used for telecommuting is permissible so long as the usage does not compromise or violate either the network, computer, or data's security and/or the ethical principles set forth by the College.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Sharing of account: The College's computing resources are allocated to groups and individuals for specific academic and administrative purposes. It is not acceptable to give, sell, or otherwise provide computing resources to other individuals or groups that do not have explicit permission to use them. Users are not to share computer accounts without getting permission from College administration and/or the Information Technology Services Department.

Commercial uses: Faculty and staff are governed by various policies concerning these matters.

Breach of copyright: This includes installing, reproducing and/or distributing copyrighted materials such as proprietary software, publications or files without permission. College software is provided under license agreements with various vendors and may not be copied or otherwise removed. Third party copyrighted information or software that the users do not have specific approval to store and/or use, must not be stored on College systems or networks.

Offensive material: Materials not subject to legal sanction may be objectionable or extremely offensive to persons other than the computer user. Importation or distribution of such material (including, but not limited to racist material, hate literature, sexist slurs or sexually explicit material) is permitted for academic or research purposes as long as it complies with the Offensive/Discriminatory Materials Policy. In some cases it is recommended that prior consultation with an Instructor, Dean or Director of a Department be obtained to ensure that the College's community and ethical standards are maintained. If required, consultation with the Information Technology Services Department is available in order to facilitate the above activities.

Hostile atmosphere: The display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content contravene the College's Human Rights policy.

Harassment: Harassing or defamatory material may not be sent by electronic means, including email and voice mail, or posted to news groups. The Criminal Code of Canada outlines the offense and punishments for Criminal Harassment in Section 264(1) C.C.

DISCIPLINE, JURISDICTION AND PENALTIES

Preamble: If the College learns that offensive material is being distributed or there is an inappropriate use of College computer resources, the College will take action. The Information Technology Services Department will investigate properly identified allegations arising within the member/users to ensure compliance with applicable federal and provincial laws and with College policies and procedures. Users of College computer resources may be requested to justify their actions or uses of College resources to the appropriate Dean, Director and/or Vice-President.

Disciplinary action: Misuse of the College's computing and network resources may result in disciplinary action by the College.

EMPLOYEES: Any employee discipline will occur in a manner that is consistent with the appropriate Collective Agreement for employees who are members of the <Support Staff Association> or <Faculty Association>. Discipline will follow the "progressive discipline" principles for employees who are not members of the Associations. Staff violations will be handled in accordance with the College's approved Progressive Discipline Procedure.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

STUDENTS: Violations of law will result in immediate loss of privileges and will be reported to the appropriate College executives and law enforcement authorities. Lesser violations by students will be dealt with under the Appeals, Complaints and Discipline Policy. Failure to comply with these guideline can result in a student losing their access and privileges to using College computer resources. Such cases will be forwarded to the appropriate Dean and/or Vice-President for review.

THIRD PARTY CONSULTANTS & CONTRACT STAFF: Any such individual accused of inappropriate use of College computing resources will be referred to the appropriate Dean, Director and/or Vice-President for a review, investigation and appropriate course of action. Proven inappropriate use of computer resources may result in the individual having their contract terminated with the College immediately.

ALL: In most instances of unacceptable behavior or misconduct, disciplinary action progresses in steps from reprimand to discharge and will be consistent with the individual's prior disciplinary record and the flagrancy of the offense. In either case, access privileges may be revoked immediately and long-term outcomes may include temporary or permanent loss of access privileges, depending on the nature of the activities.

DEFINITIONS

Data **–** the quantities, characters, or symbols on which operations are performed by computers and other automatic equipment and which may be stored or transmitted in the form of electrical signals, records on magnetic tape or punch cards, etc.

Information - knowledge acquired or derived from data. For the purposes of this policy, the term *information* refers to both information and data in all their forms, collected, maintained, accessed, modified, or synthesized by and for all members of the College community to perform the operations of the College. This policy uses terms whose meanings may not be obvious to all readers.

Record - In accordance with the *Freedom of Information and Protection of Privacy Act*, "record" means a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records. For the purposes of this policy, any other information includes, but is not limited to, the following: hand-written notes, draft documents, Post-It notes, paper files, emails, calendars, voice mails, and electronic information (e.g., databases, spreadsheets). The definition also includes a record that can be created from existing data in a computer system.

Telecommuting - Telecommuting and telework are synonyms for the use of telecommunication to work outside the traditional office or workplace, usually at home or in a mobile situation.

<u>Student Computing Resources Acceptable Use Policy:</u>

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

INTRODUCTION: < College Name >'s student computing labs are not a dedicated private facility exclusive to any class or course. The equipment in the computing labs are the property of the College and subsequently falls under the supervision and jurisdiction of the Information Technology Services Department and are also governed by the Acceptable Use Policy of College Computer Resources. It is a privilege for the students at < College Name > to have access to these computing facilities**.**

This is a College-wide policy pertaining to computers, to data networks and to the resources these technologies make available in support of the College. It applies to any devices and/or computers owned by the College as well as those owned by individuals who have been authorized to install or connect personal equipment either on the premises or to the network. In this context students include: all registered students, both full-time and part-time.

< College Name > encourages the use of computing and network resources to enhance the learning and working environment of the College community. However, access to the computing and network environment at < College Name > is to be used in effective, ethical and lawful ways that support the values of the College. The College will endeavor to create an atmosphere that balances respect for individual computer users and College facilities while maintaining the ethical and community standards of the College.

COLLEGE COMPUTER RESOURCES: The College computer resources are defined to include but not limited to such devices as personal desktop computers, laptop computers, monitors, hard drives, printers, scanners, network devices, Personal Digital Assistant devices (PDAs), network routers, network bridges, network switches, servers, the College network (LAN, WAN and Internet gateways), computer labs, software acquired by the College and relevant data. This section is also extended to include any computer system that is owned or managed by the College regardless of its location.

SUPPORT: < College Name >'s Information Technology Services Department is available to assist, advise and consult with users on the proper use of College computer resources and interpretation of this policy. If there are any questions or uncertainty about this policy, users are encouraged to contact the Director of the Information Technology Services Department or his/her designate for clarification. There is also a separate document called the Code of Conduct for Technology Support Staff which regulates the activities of all Technology Support Personnel.

GUIDELINES:

The following protocols, rules and regulations are implemented as the result of a request that students have equal and secured access to the computing equipment, software programs, accessories and working space:

1. At the start of each session on a computer, students must log on properly and subsequently log off. At the end of the day or week please turn the computer off.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2. The computer equipment will be treated with respect; any accident and/or damage must be reported to the department immediately to ensure additional damage does not occur.
3. Absolutely no food or beverage of any type will be allowed in the computer room unless it is secured in a storage receptacle (i.e. back pack).
4. When leaving the computer room, users will clean up the area they have used, including the printer area; any paper/test sheets or printed material must be removed or discarded in the bins provided.
5. Only registered students, authorized users, Faculty or College employees are permitted in the computer rooms to use College computer resources. No guests are permitted to use the equipment.
6. Any student who breaches the security system in any manner, including lending their access security card to others, may have their privilege to use the computer room revoked.
7. Students may leave a computer on and unattended for no more than 15 minutes: if a computer is left on unattended for more than this allotted time, other students will have the right to clear the material and use the computer.
8. The computer may be shut down if unattended for more than 15 minutes by faculty or designated computer lab monitor.
9. Users must ensure that viruses are not intentionally introduced into the Mount Royal computer systems.
10. It is the responsibility of each user to ensure that all transitory diskettes such as floppy diskettes or zip drives are free of any and all viruses before they are used with the Mount Royal computer systems.
11. Students may be liable for any and all intentional damage caused to the computer systems, networks, and/or data.

PRINCIPLES

1. Computing and network resources are provided primarily to support and further the College mission.
2. Individuals using College owned computer technology resources are expected to comply with provincial and federal laws and relevant < College Name > policies and procedures. Some of the material used at the college is copyrighted, protected by intellectual property law and/or license agreements. Students should undertake reasonable efforts to ensure that they do not violate the various laws, policies, procedures and license agreements.
3. Students are responsible and accountable for their actions and statements in the electronic working and learning environment, according to the disciplinary policies of the College.
4. Students are expected to use reasonable restraint in consumption of these valuable shared resources, and to use them in ways that do not interfere with the study, work or working environment of other users.
5. < College Name > computers, systems, networks and data should primarily be used for College educational and research purposes.
6. Any data stored by or transmitted to members of the College community is confidential and will not be accessed by the College without just cause and due process. In any circumstances of alleged impropriety, formal procedures permit persons responsible for computers or networks to

20

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

request specific institutional authorization to examine directories, files, email or other electronic records that are relevant to the investigation of the allegation.

7. In addition, students accessing external networks are bound by their policies, and the more restrictive policy will apply.
8. Anyone who observes actual or apparent use which appears to violate the Student Computing Resources Acceptable Use Policy is encouraged to seek further information from the Information Technology Services Department.

UNACCEPTABLE USES: *(Unacceptable uses as outlined here are not limited to these examples)*

Unauthorized access (hacking): This may include using unauthorized user names, passwords, computer addresses or identities or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or "crack" security provisions of College or external systems. The Criminal Code of Canada has two related sections: Section 342.1 Unauthorized use of computer and Section 342.2 Possession of device to obtain computer service.

Unauthorized Distribution and Disclosure of Information: Every effort must be made to prevent the unauthorized disclosure and distribution of information that is the property of < College Name >.

Vandalism of data: Deliberate alteration or destruction of computer files is a Criminal Code offence (Section 430.1). Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access. The Freedom of Information and Protection of Privacy Act (FOIP) also deals with deliberate destruction of data.

Interference with other users' work: This includes use of any process that causes a user to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of "spam (excessive email distribution)," and the introduction of viruses or electronic chain letters.

Sharing of account: The College's computing resources are allocated to groups and individuals for specific academic and administrative purposes. It is not acceptable to give, sell, or otherwise provide computing resources to other individuals or groups that do not have explicit permission to use them. Users are not to share computer accounts without getting permission from College administration and/or the Information Technology Services Department.

Squandering resources: Resources are shared and no user may degrade the systems by: unwarranted data space, time and bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs. As the use of College resources changes and the technology capabilities change over time – users are encouraged to work with the Information Technology Services Department in the defining appropriate and efficient uses of computer resources.

Personal uses: The College computer resources are to be used primarily for College purposes (i.e. instruction, teaching, educational research and administration). All users have the responsibility to ensure that incidental personal use of College computer resources does not interfere with the normal course of their duties. Incidental personal use of computers would include but is not limited to personal email.

21

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Telecommuting: Incidental personal use of < College Name > and/or any other computer systems that are used for telecommuting is permissible so long as the usage does not compromise or violate either the network, computer, or data's security and/or the ethical principles set forth by the College.

Breach of copyright: This includes installing, reproducing and/or distributing copyrighted materials such as proprietary software, publications or files without permission. College software is provided under license agreements with various vendors and may not be copied or otherwise removed. Third party copyrighted information or software that the users do not have specific approval to store and/or use, must not be stored on College systems or networks.

Offensive material: Materials not subject to legal sanction may be objectionable or extremely offensive to persons other than the computer user. Importation or distribution of such material (including, but not limited to racist material, hate literature, sexist slurs or sexually explicit material) is permitted for academic or research purposes as long as it complies with the Offensive/Discriminatory Materials Policy. In some cases it is recommended that prior consultation with an Instructor, Dean or Director of a Department be obtained to ensure that the College's community and ethical standards are maintained. If required, consultation with the Information Technology Services Department is available in order to facilitate the above activities.

Hostile atmosphere: The display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content contravene the College's Human Rights policy.

Harassment: Harassing or defamatory material may not be sent by electronic means, including email and voice mail, or posted to news groups. The Criminal Code of Canada outlines the offense and punishments for Criminal Harassment in Section 264(1) C.C.

DISCIPLINE, JURISDICTION AND PENALTIES

Preamble: If the College learns that offensive material is being distributed or there is an inappropriate use of College computer resources, the College will take action. The Information Technology Services Department will investigate properly identified allegations arising within the member/users to ensure compliance with applicable federal and provincial laws and with College policies and procedures. Users of College computer resources may be requested to justify their actions or uses of College resources to the appropriate Dean, Director and/or Vice-President.

Disciplinary action: Misuse of the College's computing and network resources may result in disciplinary action by the College.

STUDENTS: Violations of law will result in immediate loss of privileges and will be reported to the appropriate College executives and law enforcement authorities. Lesser violations by students will be dealt with under the Appeals, Complaints and Discipline Policy. Failure to comply with these guideline can result in a student losing their access and privileges to using College computer resources. Such cases will be forwarded to the appropriate Dean and/or Vice-President for review.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In most instances of unacceptable behavior or misconduct, disciplinary action progresses in steps from reprimand to discharge and will be consistent with the individual's prior disciplinary record and the flagrancy of the offense. In either case, access privileges may be revoked immediately and long-term outcomes may include temporary or permanent loss of access privileges, depending on the nature of the activities.

DEFINITIONS

Data - the quantities, characters, or symbols on which operations are performed by computers and other automatic equipment and which may be stored or transmitted in the form of electrical signals, records on magnetic tape or punch cards, etc.

Information - knowledge acquired or derived from data. For the purposes of this policy, the term *information* refers to both information and data in all their forms, collected, maintained, accessed, modified, or synthesized by and for all members of the College community to perform the operations of the College. This policy uses terms whose meanings may not be obvious to all readers.

Record - In accordance with the *Freedom of Information and Protection of Privacy Act*, "record" means a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records. For the purposes of this policy, any other information includes, but is not limited to, the following: hand-written notes, draft documents, Post-It notes, paper files, emails, calendars, voice mails, and electronic information (e.g., databases, spreadsheets). The definition also includes a record that can be created from existing data in a computer system.

Telecommuting - Telecommuting and telework are synonyms for the use of telecommunication to work outside the traditional office or workplace, usually at home or in a mobile situation.

If you need clarification on these guidelines– please contact the Director of Information Technology Services Department.

Information Technology Services Department – Help Desk can be contacted:

Student Declaration

I have read the Student Computing Resources Acceptable Use Policy.

I understand the above protocols, rules and regulations and agree to adhere to them at all times, including regular academic hours/days, evenings, weekdays, weekends and holidays.

I understand that Faculty, Support Staff, Lab Monitors and College Security have the right to challenge the student's actions based on the above.

23

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

I understand that if I compromise or disregard any of the above through any action and/or activity that access to < College Name > computer equipment and systems will be suspended immediately and that these privileges may be unavailable for a specified period of time from the date of suspension; I may be allowed to be reinstated by submitting a written request to the ITS Department.

Student Name _____
(Print Name Clearly)
Student Signature _____
Date _____

NOTE: There is also a broader college wide "Acceptable Use Policy" should students need additional information on College computing policies.

(If you need clarification on these guidelines, please contact the Director of Information Technology Services Department).

Code of Conduct for Technology Support Staff:

The policy defining "Acceptable Use of College Computer Resources" outlines for users the principles governing the use of < College Name >'s computing facilities. To ensure that < College Name >'s computing environment is available to satisfy its intended uses, the College must take appropriate steps to manage and protect its facilities. To this end, some Technology Support Staff have certain privileges and powers. With these privileges, come responsibilities and this Code of Conduct for Technology Support Staff describes the responsibilities and rights associated with the management of the College's computing facilities.

1. **Guideline Applicability**
   1.1 These guidelines apply to all personnel who, in the course of their duties, have physical or logical control or custody of components of the College's computing environment. Some individuals are defined as "System Administrators" with access (physically and/or logically) to sensitive information residing on the College's computer resources. This includes some employees of the Information Technology Services (ITS) Department and other College Departments who also employ Technology Support Staff. Other examples of technology support positions include, but are not limited to Technical Support Analysts, IT Security Coordinator, Network Analysts, Network Administrators, System Analysts, Programmer/Analyst, Client Support Analysts, Computer Lab Support Analysts, Computer Electronic Technicians and IT Supervisors/IT managers. For the purposes of this document, all such people are referred to as "Technology Support Staff (TSS)".

2. **Management Responsibilities**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2.1 College Management and TSS must take all reasonable steps to protect systems and contents. Specific requirements are dictated by physical location, connectivity, sensitivity of data, contractual requirements and user characteristics. The term "protect" includes taking appropriate actions to enable systems to meet their intended purposes. Responsibilities include, but are not limited to, those described here. TSS with limited access only have those responsibilities reasonably under their control.

2.2 College Management and TSS must manage computer facilities and computer resources with the intent of meeting their prescribed goals.

2.3 College Management and TSS must control access as appropriate to specific computer facilities. This includes, but is not limited to, ensuring that all access is via appropriate access codes except those systems with controlled limited function. Any security vulnerabilities that may allow a user to bypass security must be corrected where possible.

2.4 College Management and TSS must take reasonable steps to ensure that users do not violate the Acceptable Use Policy. Specifically, facilities and services that allow users to easily bypass security measures of local or remote systems must be minimized.

2.5 College Management and TSS must respect confidentiality. Data may only be accessed in accordance with the actions outlined in section 4 of this document.

2.6 College Management and TSS must provide for data backups, hardware maintenance and software maintenance commensurate with < College Name > norms, user needs, expectations and finances.

2.7 College Management and TSS who observe actual or apparent use which violates the Acceptable Use Policy are obligated to report such use as specified in section 3.

2.8 Major infractions of the Acceptable Use Policy, and in particular those related to intrusive or malicious behavior must be reported to the Director of Information Technology Services Department or duly identified delegate.

3. **Management Privileges and Limits**

3.1 In the course of carrying out the preceding responsibilities, TSS are empowered to take certain actions. As described in the sections that follow, these actions generally can be taken only under certain circumstances and with due regard to the Acceptable Use Policy, users as a whole, and individual users.

3.2 In many cases, actions require permission for investigation and reporting of details. Such permission must be obtained from, or reports filed with the Director of Information Technology Service and the appropriate Vice President.

3.3 System privileges permit the following actions:

3.3.1 Access to systems with privileges exceeding those of a normal user must be restricted to those personnel who specifically require such privileges. Within the limitations of the system involved, only those privileges actually required should be granted. It is understood that some systems do not allow granting of certain privileges with fine granularity. In such cases, privileged users may have more rights than they absolutely need. The granting of such privileges does not confer the right to use them.

3.3.2 TSS may take all reasonable steps to control the use of and access to the College's computing environment. This may include setting access and use priorities and limits,

25

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

restricting access to and availability of the computing environment, performance management, and making decisions regarding the services to be provided. All such actions and decisions must be made with the conscious requirement to support the intended use of the specific facility and the mission and the administrative functions of the College.

3.3.3 Data maintained by the system (log files, audit trails) may be used in fulfilling the TSS' obligations. General release of detailed content of system log files without authorization is prohibited.

3.3.4 System or sub-system failures may yield access without prior permission. In such cases, TSS must act with discretion.

3.3.5 In circumstances where the TSS believes that illegal acts or acts violating < College Name > Technology policies are involved, the Information Technology Security Specialist must be consulted.

3.3.6 System maintenance, security, integrity or performance issues may indicate that data privacy or system integrity may have been breached, or that system access has been compromised. In such cases, problem analysis will clearly prescribe a course of action. Actions must be reasonably justified. In such cases, prior approval should be obtained from the Director of Information Technology Service, or, if that is not practical or possible, the action must be reported promptly after the fact.

3.3.7 In exceptional cases not covered by the above points, permission must be obtained from the appropriate Vice President to carry out actions such as monitoring and investigations that are reasonable given the indicated situation. Such investigations should always be done in such a way as to minimize intrusiveness. Where the threat to the College justifies urgent action, and where time would not allow prior consultation, the appropriate Vice President must be advised as soon as possible after the fact. If the Vice President does not agree with the action it may disallow use of any information so obtained.

3.3.8 All actions requiring the permission of senior management or reports according to these guidelines must be logged (electronically or manually). Such logs must be retained for at least one year.

4. Examples of Technology Support Staff Actions

4.1 In exercising the rights described in this set of guidelines, questions arise as to what TSS who are responsible for day-to-day support may do on their own volition, and what actions require permission and/or reporting. These are examples; no claim is made that this is an exhaustive list.

4.2 Actions not requiring permission/reporting

- Data backups
- Systems management (including starting/stopping system, system recovery, repair)
- Data line and network monitoring where intent is performance management or problem diagnosis
- Controlling systems resource allocation
- Routine mail re-routing and support
- Routine file management (with prior notice if appropriate)
- Scanning systems for viruses

26

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Scanning systems for potential security holes including poor passwords
- Managing the data of terminated employees
- Altering ownership or access rights
- Statistical Analysis for the purpose of system monitoring, performance or utilization.

4.3 ***Actions requested by the user***

- Inspection, alteration or deletion of user data in support of the user.

4.4 ***Actions requiring prior notification to user***

- Alteration or deletion of user data where policy infractions are suspected. An un-inspected copy of the data may be made prior to notification.

4.5 ***Actions requiring the permission of the Director of ITS or his/her designate***

- Inspection of user data where policy infractions are suspected. An un-inspected copy of the data may be made prior to notification.
- System-wide inspection of user data which includes scanning for copyright violations, programs designed to thwart security (such as password cracking programs), software license verification or other violations of the Acceptable Use Policy.
- Altering data ownership or access rights where system integrity is involved.
- Inspection, alteration or deletion of user data where policy infractions are suspected and potential impact is urgent. System penetration or intrusion will often be present.
- Denial of access to the computing environment for a particular user(s).

4.6 ***Actions resulting in notification of the Vice President***

- Accessing data for the purposes of identifying potential infractions. Data may be "live" or copied previously.

4.7 ***Action resulting in notification of the College's Executive Committee***

- Implementation of software to perform automated scanning of user data for violations of the Acceptable Use Policy.

In the event that actions are initiated, the involved parties will be notified as soon as is practicable of the nature and scope of the investigation(s).

I acknowledge that I have read the above Code of Conduct and will use this special access in accordance with the Acceptable Use Policy for College Computer Resources.

User Name _____ User Signature_____
Director of Human Resources (Name)_____
Director of Human Resources (Signature) _____
Date _____

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES:

1. Blaber v. University of Victoria, [1995] B.C.J. No. 558, Victoria Registry No. 94 4823 [944823], British Columbia Supreme Court, Victoria, British Columbia. http://insight.mcmaster.ca/org/efc/pages/law/court/Blaber.v.UVictoria.html

2. CCIPS, Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, United States Department of Justice, January 2001. http://www.cybercrime.gov/searchmanual.htm

3. Caspi, Steven J. et al. v. The Microsoft Network, L.L.C., et al., 1999 WL 462175, 323 N.J. Super. 118 (N.J. App. Div., July 2, 1999 http://www.phillipsnizer.com/int-click.htm

4. Groff v. America Online, Inc., File No. C.A. No. PC 97-0331, 1998 W L 307001 (R.I. Superior Ct., May 27, 1998) http://www.phillipsnizer.com/int-click.htm

5. Scott, Michael D. "Rules and Regulation - The Risk of Risque." CIO Insight September 2001, Number 05.

6. Armstrong, Illena. "Liability Worries – Avoiding Courtroom Drama". SC Magazine Online. Second Feature. August 2001 http://www.westcoast.com/cgi-bin/redirect.pl

7. Swanson, Sandra. "Add Neglect To Crimes IT Workers Must Report". Informationweek.com. August 8, 2001. http://www.informationweek.com/story/IWK20010808S0006

8. A Report from the Attorney General to the Vice President of the United States. Cyberstalking: A New Challenge for Law Enforcement and Industry. August 1999. http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

9. U.S. Department of Justice. Second "Global Hell" Hacker Pleads Guilty; Patrick Gregory Faces Up to Five Years in Prison for Conspiracy to Commit Telecommunications Fraud and Computer Hacking. U.S. Department of Justice. April 12, 2000. http://www.usdoj.gov/criminal/cybercrime/gregory.htm

10. U.S. Department of Justice. Computer Hacker Sentenced. September 6, 2000. http://www.usdoj.gov/criminal/cybercrime/gregorysen.htm

28

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

11. U.S. Department of Justice. Emulex Hoaxer Indicted for using Bogus Press Release and Internet Service to Drive Down Price of Stock. September 28, 2000. http://www.usdoj.gov/criminal/cybercrime/emulex.htm

12. U.S. Department of Justice. Orange County, California Computer Hacker Pleads Guilty to Hacking University Computers, Defrauding Western Union .August 1, 2001. http://www.cybercrime.gov/diekman4.htm

13. U.S. Department of Justice. Russian Computer Hacker Convicted by Jury. October 10, 2001. http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm

14. Galvin, John. "Meet the World's Baddest Cyber Cops." Ziff Davis Smart Business. September 12, 2001. http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2811892-3,00.html

15. Walker, Lisa. "Quebec University Web site used to store over $U.S. 1 million worth of pirated software." The Canadian Alliance Against Software Theft (CAAST). May 10, 2000. http://www.caast.org/release/default.asp?aID=12

16. Alletson, Lisa. "Toronto Student Faces Criminal Charges for Distributing Copyrighted Software and Pornography." The Canadian Alliance Against Software Theft (CAAST). December 15, 1998. http://www.caast.org/release/default.asp?aID=5

17. Wood, Charles Cresson. Information Security Policies Made Easy. Pentasafe Security Technologies, Inc., Sausalito, CA, USA; 1999.

29

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced