Acceptable Use of Computing Resources: Policy and Policy Analysis

by

Benjamin Tomhave

November 1, 2004

Prepared for:

Professor Daniel J. Ryan
EMSE 315
The George Washington University

This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources which I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____Benjamin L. Tomhave_____

Acceptable Use of Computing Resources: Policy and Policy Analysis

by

Benjamin L. Tomhave

Abstract

This paper includes two main sections. In Part I, a policy is articulated on acceptable use of computing resources within a commercial company ("the company"). The goal of the policy is to provide maximum coverage and minimal loopholes while being fair in its application and limitation of liability. In Part II, the policy is discussed in terms of its ethical, moral and legal implications. Part II also provides rationale for decisions made in the policy development process.

Table of Contents

Acceptable Use of Computing Resources: Policy and Policy Analysis

by

Benjamin L. Tomhave

I.POLICY: ACCEPTABLE USE OF COMPUTING RESOURCES

All company computing resources must be used in an acceptable manner consistent with this policy, the needs of the business and the Professional Standards of Conduct. Use may include, but is not limited to, access of Internet/Intranet/Extranet resources via web, email, file transfer or other network-based services, instant messaging, or accessing non-networked resources, such as through dedicated consoles or Out-of-Band management systems.

*A.*Definition and Ownership of Computing Resources[1]

Computing resources are defined as all digital or analog computational devices owned by the company. These devices may include, but are not limited to, computer equipment, software, operating systems, storage media, network infrastructure, and network or local accounts, such as for access to network- or host-based resources. The company owns all computing resources provided by the company. Permission for use of computing resources is granted to employees on an as-needed basis in accordance with this and all other application policies and agreements.

*B.*Guidelines for Acceptable Use[2]

The information security discipline oftentimes evaluates risks according to the concepts of confidentiality, integrity and availability. The evaluation of risks may also weigh applicable laws and regulations as well as company policies, standards, guidelines and procedures. The following guidelines are provided to assist users in making proper decisions about whether certain uses of computing resources are acceptable.

1.Confidentiality

Maintaining the confidentiality of data and people is of the utmost importance. When using computing resources, ask yourself the question: "Am I intentionally violating the confidentiality of the business, corporate data or an individual?" If the answer to this

[1] The SANS Institute, *InfoSec Acceptable Use Policy* (Bethesda, MD: SANS, undated, accessed 30 October 2004); available from http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf; Internet.
[2] Merit Network, Inc., *MichNet Policies: Acceptable Use Policy* (Ann Arbor, MI: Merit, 2003, accessed 30 October 2004); available from http://www.merit.edu/mn/about/policies-acceptableuse.html; Internet.

question is “yes” then determine whether or not you are authorized to view the information or data in question. If you are authorized, then determine whether or not you have a need to view the information or data. If you are not authorized to view the data or information, then do not view it. If you believe that you have inappropriate access to data or information, immediately report this finding to the proper owner or management.

2.Integrity

Integrity is defined as the soundness of data or systems and the certainty that data is authentic and unaltered. Modifying data or information without proper authorization is unacceptable use and a violation of data integrity. Accessing systems without proper authorization or through unapproved methods is also unacceptable and a violation of system integrity. Always access data or systems through approved methods. If you believe that data or systems are accessible through unapproved methods, it is your responsibility to report the error.

Violations of integrity may include, but are not limited to, circumvention of simple controls on data files, access to systems through unapproved methods, unauthorized escalation of privileges on a system, modifying data without permission, or intentionally corrupting data. Violation of data or system integrity on systems external to the company through the use of company assets is also unacceptable use.

3.Availability

Intentionally denying access to data or systems without authorization, or outside the intended function of an application or system, is unacceptable use. Some applications and systems contain locking features designed to control access to data or processes (e.g. version control software). This behaviour is expected and acceptable. Use of company computing resources to deny access to internal or external systems is unacceptable use. When accessing data or systems, ask yourself the question: “Am I denying authorized access to data or systems as a result of my actions?” If the answer to this question is “yes” then determine whether you are authorized to undertake this action, and then determine whether or not there is a business need for the action.

Availability also applies to client-side applications, such as mail readers and web browsers. Intentionally causing an application to crash, lock or otherwise perform errantly is unacceptable use. By extension, knowingly allowing your system to become or remain infected with malicious code may be deemed a violation of this policy.

All perceived violations must be reported to the appropriate contact or management immediately. Reporting suspected infections in a timely manner will often exonerate a user from direct responsibility, pending the outcome of an investigation.

*4.*Legal compliance

It is important to be aware of applicable laws and regulations when accessing or using data or systems that are internal or external to the company. Areas of consideration should include, but are not limited to, copyright, trademark, patent, privacy, wiretap, confidentiality and communication laws and regulations. Use of computing resources to violate laws or regulations represents a violation of this policy, regardless of intent or jurisdiction. Software must be used in accordance with its licensing terms and company policies. Access of systems must not be in contravention of The Computer Fraud and Abuse Act (18 USC 1030) or other applicable laws.

Use of systems to send communication in violation of Human Resources (HR) policies and applicable laws will be considered a serious breach of this policy and will be addressed swiftly and strictly. Communication must be appropriate for a business environment and inline with the Professional Standards of Conduct (PSC). All users are expected to act in a professional and courteous manner at all times and in all forms of communication.

Suspected violations of this tenet of the policy should be reported to the appropriate contact immediately. The appropriate contact may be a member of management, HR, PSC or Legal. It is recommended that management be approached first, unless the suspected violation directly involves management.

*5.*Policy compliance

All users of computing resources must be familiar with applicable policies, standards, guidelines and procedures. Training and awareness programs will be provided to inform the user of corporate policies and applicable laws in order to ensure the ability of users to comply with acceptable computing policies. If a user is in doubt of whether or not a given action is acceptable, it is that user's responsibility to seek clarification before proceeding.

*C.*Specific Prohibitions and Restrictions on Use[3456]

The following activities are generally prohibited or restricted. Certain individuals may be exempted from these rules in order to perform their required job responsibilities (e.g., Operations Security is authorized to actively monitor network traffic and respond in a disruptive manner to mitigate a detected threat). Employees are not authorized, under any

[3] The SANS Institute, *InfoSec Acceptable Use Policy* (Bethesda, MD: SANS, undated, accessed 30 October 2004); available from http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf; Internet.
[4] Earthlink, Inc., *EarthLink Acceptable Use Policy* (Atlanta, GA: 2001, accessed 30 October 2004); available from http://www.earthlink.net/about/policies/use/; Internet.
[5] America Online, Inc., *AGREEMENT TO RULES OF USER CONDUCT* (Dulles, VA: 2004, accessed 30 October 2004); available from http://www.aol.com/copyright/rules.html; Internet.
[6] Merit Network, Inc., *MichNet Policies: Acceptable Use Policy* (Ann Arbor, MI: Merit, 2003, accessed 30 October 2004); available from http://www.merit.edu/mn/about/policies-acceptableuse.html; Internet.

circumstances, to actively engage in activities deemed illegal under applicable jurisdictions (international, federal, state or local). The list provided below is not comprehensive, but should be used as a baseline for helping determine whether or not a proposed action is unacceptable. Omission of an action from this list does not imply that it is an acceptable use. Any violations of these specific prohibitions and restrictions will be treated severely and may reasonably result in immediate termination of employment.

1.Illegal use

Computing resources must be used within the confines of the law. Any use of computing resources to infringe intellectual property protections, such as copyrights, trademarks, patents or trade secrets, is prohibited. Infringing acts may include, but are not limited to, unauthorized copying of copyrighted materials, use of a trademark without authorization or exporting software, technical information, encryption or technology in violation of export control laws. Any action, intentional or unintentional, that serves to copy or transmit protected materials without proper authorization is an unacceptable use.

2.Threats, harassment or harm to minors

Computing resources must not be used to threaten, harass or harm others. Unauthorized uses of this type may include, but are not limited to:

- communication that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, tortuous, or containing explicit or graphic descriptions or accounts of sexual acts (including but not limited to sexual language of a violent or threatening nature directed at another individual or group of individuals);
- communication that victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, or disability;
- any form of harassment via email, telephone, paging or instant messaging, whether through language, frequency, or size of messages;
- use of computing resources to harm, or attempt to harm, minors in any way.

3.Fraud, forgery or impersonation

Any use of computing resources to commit fraud, forgery or impersonation is strictly prohibited. All users must truthfully and accurately represent their identity at all times. Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers, including email header information, or other identifying information is prohibited. Postings to public places intended to mask your employment status and employer, may be allowed. For example, use of a unique "handle" on a chat board or in IRC is acceptable given that the nature of the chat board or IRC channel is appropriate. Bear in mind that use of chat board or IRC from company computing resources may also be prohibited.

Users may not utilize computing resource to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters." Unless part of normal job duties, making statements about warranty, expressly or implied, is also prohibited.

4.SPAM / SPIM

Creation, sending and forwarding of unsolicited advertising, junk or bulk email ("SPAM") or instant messages ("SPIM") are strictly prohibited, unless explicitly authorized as part of your normal job duties. Undertaking any activities that serve to facilitate unsolicited commercial email or unsolicited bulk email, whether or not that email is commercial in nature, are prohibited. Use of instant messaging facilities to accomplish the same is also prohibited.

5.Unauthorized access or circumvention of access controls

Any access to systems or data that is not specifically authorized is prohibited. Any circumvention of access controls, whether for accessing systems with or without authorization, is also prohibited. Users may not circumvent authentication or security of any host, network or account.

6.Collection of confidential data

Use of computing resources to collect confidential data, such as about members, employees or intellectual property, is prohibited. Collection, or attempts to collect, personal information about third parties, without their knowledge or consent, is prohibited and may constitute a violation of company privacy policies and agreements. The company strictly limits its liability in cases where individuals act of their own accord and without proper authorization. Any attempts to harvest or collect confidential data without explicit and proper authorization is prohibited and will be subject to severe disciplinary actions, up to and including termination of employment.

7.Disrupting network services or access to data

Rendering systems, networks, applications or data inaccessible or unusable due to an unauthorized disruption or corruption, is prohibited. Such prohibited acts may include, but are not limited to, ping floods, packet spoofing, executing denial of service or distributed denial of service attacks, forging routing information, corrupting data upon which an application or system relies, or removing or disabling a service, such as a process or application, on a host or network. Port or security scanning without prior authorization by Operations Security is strictly prohibited. Using any automated tool, such as a program, script or command, to send any message with the intent to interfere with or disable terminal sessions is not acceptable.

8.Making public statements under cover of company identity

Individuals making public statements under the cover of their company identity, including through email, web postings, instant messaging or public presentations, must seek explicit authorization and approval from management. Corporate Communications is the only department authorized to publish Press Releases and to communicate with members of the journalistic community ("the press"). Any public statement made in contravention of this policy and related policies is expressly prohibited and may result in severe disciplinary action, up to and including termination of employment. "Whistle blowing," or the disclosure of information about questionable internal practices, may be a legally protected form of disclosure. However, these disclosures must not occur in a public arena, but must be limited to specific conversations with law enforcement or regulators. Disclosure of protected information in public under the guise of "whistle blowing" will be subject to legal action against the individual by the company.

9.Disclosure of protected information

Disclosing company confidential information is prohibited. Disclosures may include, but are not limited to, unique account names, account passwords or lists of employees, contractors, consultants, vendors or products. All information must be treated as confidential and protected unless labeled otherwise, in accordance with the *Confidentiality, Non-Competition and Proprietary Rights Agreement*. Certain information may be disclosed, including email address, assigned desk phone number, fax number, mailing address or title.

10.Monitoring or interception of network traffic

Monitoring or intercepting any form of network traffic or data not intended for your own host is prohibited, unless authorized as part of your normal job duties. Monitoring or intercepting network traffic may violate the privacy or confidentiality of the data being transmitted.

*11.*Introduction of malicious code or programs

Introduction of malicious code or programs into the network, servers or product source code is prohibited. Intentionally distributing viruses, worms, Trojan horses, email bombs, etc., is not acceptable. Failure to implement and maintain protective measures for these types of malicious code or programs is unacceptable. Failure to report a suspected infection is also a violation of company policy.

12.Introduction of network services or routing configurations

The introduction of routing patterns or network services that are inconsistent with established patterns or services and/or that may disrupt or interfere with the intended patterns or services are expressly prohibited. Examples of unacceptable use include, but are not limited to, broadcasting routing information, providing Dynamic Host Control Protocol (DHCP) services in conflict with authorized services, or sending network messages designed to terminate network connections (such as TCP RST packets, or "sniping").

13.Use of company resources to conduct non-company business

Company resources may not be put to use for any business purpose outside of company business. This includes, but is not limited to, the use of company computers to store, forward, copy or manage information for any other company; the use of company equipment to produce printed or electronic documents for any other company or organization; or the use of any company resources, including personnel time, for the furtherance of any other company or organization. Specific exemptions to this policy may be granted by management for specific charitable, promotional, or in-kind business partnerships, but such exemptions must be specifically authorized and must comply with all relevant laws and regulations.

14.Release of information regarding security incidents

Authorization to release information regarding security incidents involving the company is restricted solely to management and its assigned agents (e.g. legal counsel or public relations agents). In the event of a security incident involving the company, individuals are not authorized to communicate news of such incidents to any outside party. It is solely the company's responsibility to appropriately notify public agencies of security incidents in compliance with state and federal regulations.

*D.*Policy Enforcement and Limitation of Liability to the Company[7]

The company will take all reasonable measures to ensure that compliance with all applicable laws occurs with respect to the acceptable use of computing resources. The company will also undertake training and awareness programs to ensure that all employees, contractors, temporaries and vendors are informed of this, and other, policies. The company is responsible for the disclosure of expected performance with respect to acceptable use of computing resources. Any failure of an individual to comply with this policy, despite the reasonable efforts of the company to inform and educate, are the sole responsibility of the individual. Any violations that result from an internal or external investigation and that may include legal actions are strictly assigned to the individual.

1.Reporting violations or seeking clarification

All suspected violations of this policy must be reported to management or through the communication methods provided by the company. Failure to report knowledge of a suspected policy violation will itself be considered a violation and will be subject to disciplinary review and action. It is the responsibility of all employees to help minimize risk to the company as a whole.

[7] This entire section is nearly identical to the equivalent section of the previous policy assignment ("Use of Licensed Software"). A good set of policies will use consistent language and format so as to clearly communicate expectations for performance/behaviour to the reader. If I were writing these policies for use in a business environment, I would copy-n-paste this section between policies with as little customization as possible to ensure consistency.

As a general practice, the rule of "when in doubt, ask first" should be followed when considering activities that are not explicitly allowed or prohibited by this policy. All employees are responsible for seeking out and receiving explicit permission to undertake activities that may be in violation of this policy. The company will provide a method for submitting questions about the application of this policy in specific scenarios that are otherwise unclear.

*2.*Automated methods for policy enforcement

The company will implement automated methods for monitoring company assets for unacceptable use and abuse. These automated methods will assist the company in taking reasonable measures to ensure that violations do not occur. Disabling or tampering with these automated methods is strictly prohibited and may result in disciplinary action. These tools are intended strictly to monitor company assets for acceptable use of computing resources. These tools are not intended as a method for "spying" on employees or to violate any privacy protections afforded employees.

*3.*Procedures for remediation of violations

All potential violations will be considered through due process. Ownership for the violation will be determined and the need for disciplinary review and action will be addressed. If the company finds that it is in violation of this policy, immediate actions will be taken to bring the company into compliance. If the company finds that the violation is the result of individual actions that were not properly authorized, the individual or individuals directly responsible will be referred for disciplinary review.

4.Process for levying disciplinary action

Once a determination is made that a violation has occurred as a result of the actions of an individual or individuals, management will refer the matter to Human Resources for consideration and action under the disciplinary plan. Disciplinary actions may include, but are not limited to, levying of fines, suspension or termination of employment. In all cases, the violating behaviour must be immediately stopped.

If a determination is made that the company caused or authorized the violation, a decision will have to be made about whether or not the offending action should be halted or permitted. The employee will not be held in direct responsibility for the violation, though the employee will be reminded of the inherent responsibility of all employees to vigilantly protect the company from unnecessary risk and liability.

5.Periodic policy review

This document will be periodically reviewed, no less than annually, and suggestions for changes will be reviewed and voted upon by a Policy Review Committee to be assigned by the Board of Directors. This committee will collect comments and suggestions for policy change between meetings, and will decide upon suggestions in a timely fashion. Legal must review all policy changes before they can be accepted and implemented. Changes to policy will be announced to the company through appropriate channels, including but not limited to, company wide electronic mail, announcement at company meetings, and the distribution of updated company policy documents.

*E.*Agreement to and Acceptance of this Policy[8]

By accepting employment with the company and using computing resources owned by the company, the user is accepting the terms of this policy and agreeing to abide by its provisions. The following signature by the user signifies acceptance of this policy in its entirety and represents a commitment to make use of computing resources in an acceptable and responsible manner. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. The signature of a witness affirms that the user has been apprised of this policy and been given an opportunity to voice questions or concerns up front.

I, the below signed, agree to the requirements and guidelines set forth in this, the "Acceptable Use of Computing Resources" policy, and promise to use computing resources, provided by the company to perform my job duties, in an acceptable, appropriate and professional manner. Furthermore, I waive my right to privacy, except for those rights specifically guaranteed by the law, and accept that the company may monitor and respond to my use of computing resources in accordance with this, and other, company policies.

Name: _____ Employee ID: _____

Signature: _____ Date: _____

I, the below signed, have witnessed the signing of this agreement. I have ensured that the above-signed has received a current copy of the "Acceptable Use of Computing Resources" policy and that I have answered or referred for answer any questions or concerns that the above-signed has expressed.

Name: _____ Employee ID: _____

Signature: _____ Date: _____

[8] Legal and HR should be consulted to ensure that this agreement is allowable under applicable laws. Also, it may be wise to add language stating that, should any part of the policy be deemed illegal, the rest of the policy will remain intact and valid.

II. ETHICAL, MORAL AND LEGAL IMPLICATIONS OF THE "ACCEPTABLE USE OF COMPUTING RESOURCES" POLICY[9]

An analysis of the "Acceptable Use of Computing Resources" policy must necessarily consider the ethical, moral and legal implications of its provisions and entirety. This analysis has been subdivided in the following sections. Existing laws serve to frame the ethical and moral requirements of most situations. However, there remain questions of fairness and propriety within the limits of the organization.

This policy was developed through a process of research, aggregation and synthesis. An Internet search was used to find examples and discussions of acceptable use policies and policy templates. These examples were then aggregated to produce a hybrid outline. Synthesis of the hybrid outline with original content, ideas and business requirements was then utilized to complete the work.

The primary foci of the policy are to outline expected patterns of behaviour and professional conduct with respect to use of computing resources. Furthermore, provisions within the policy set expectations for monitoring and enforcement of the policy, as well as to document potential disciplinary actions. In cases where no clear rule could be inherited from higher laws, decisions were based on the needs of the business and the requirement to limit liability and indemnify the business against the wrongdoing of individuals. Ultimately, this policy is designed to limit the responsibility of the business for the illegal acts of individuals in the employ of the business.

A. Ethical Implications: Fairness

An ethical analysis of a policy must consider the fairness of the rules of behaviour codified in the policy. The concept of fairness, in this case, pertains to whether or not the company is fairly allowing and limiting access to and use of computing resources. Specifically, there is an inherent contradiction in the requirement of employees to have access to computing resources and the desire of the business to limit use and abuse of these resources. Complicating the picture is the likelihood that computing resources will not remain inherently secure at all times. The emergence of operating system vulnerabilities, new malicious code, or the failure of an authentication system may lead to an unintentional (or accidental) misuse of a resource.

Therefore, from the standpoint of fairness, the policy has been constructed to provide general guidelines for acceptable use, while adding specific prohibitions and restrictions that are considered unacceptable use under most, if not all, circumstances. Additionally, from the standpoint of enforcement, the policy and its respective disciplinary action plan must weigh all factors of an incident to determine fairness. For example, if a desktop system were to become infected with a new piece of malicious code against which no

[9] Dave Kinnaman, *Critiquing Acceptable Use Policies* (Unknown, US: Kinnaman, 1995, accessed 30 October 2004); available from http://www.io.com/~kinnaman/aupessay.html; Internet.

known remedy or protection exists, it is not fair to hold the system user or owner directly and fully responsible for the infection and its subsequent unacceptable use of the resource. However, if a user notices suspicious behaviour on their system and fails to report it, possibly in the face of training and awareness about malicious code infections, then the user becomes responsible for any further infections stemming from their infection, as well as any subsequent disclosure of confidential information. This example represents two opposing extremes on a broad spectrum of severity and responsibility. The responsibility of the end-user may be mitigated if the company has not, in good faith, maintained technical countermeasures, whereas the responsibility may be increased if the end-user knowingly and intentionally executes the mail attachment that has caused the infection.

In the end, the policy has been written to provide an objective set of rules that will guide the reader down the path of fair and appropriate use of computing resources. However, loopholes are intentionally provided for users to question policies, seek clarification and solicit improvements. As with all policies, this policy should be considered a living document and not held in such high regard that it cannot be amended. As the needs of the business change, along with the legal and regulatory environment, so should the definition of acceptable use.

B.Moral Implications: Right vs. Wrong

One of the goals of the "Acceptable Use of Computing Resources" policy is to clearly define what are considered to be right and wrong actions. This definition relies, in part, on the legal and regulatory requirements inherited from above. Companies are not allowed to promote illegal or illicit activity and are constrained to ensure, within reason, that their employees are compliant with these requirements. However, in limiting the ability and permission of employees to use computing resources, it is oftentimes the case that the business will exceed reasonable restrictions and will stipulate limits on use that are not only legal, but quite possibly protected or necessary.

In writing this policy, it has been intentionally decided to leave use as open as possible, instead focusing on those uses that are explicitly known to be inappropriate. Additionally, general guidelines that are inline with the Professional Standards of Conduct information security best-practices have been produced in hopes of helping users to make good decisions. Nonetheless, it is fully expected that situations will arise where an action will fall into the gap between acceptable and unacceptable use. In such cases, the right and reasonable approach is for the user to seek clarification before undertaking the action. This expectation has been clearly stated within the policy.

C.Legal Implications: Indemnification Against Direct Liability

The creation and promotion of policies, standards, guidelines and procedures are used by companies to limit the liability they might otherwise incur in instances where bad things have happened. In this specific case, one of the primary objectives of the policy is to clearly define legal behaviour as acceptable and illegal behaviour as unacceptable. Coupled with an active training and awareness program, the policy serves to transfer some, if not most, of the responsibility for illegal behaviour onto the individual. The company still bears the responsibility of proving that due diligence has been performed with respect to monitoring and enforcement of the policy, implementation and maintenance of access controls, and implementation and maintenance of security countermeasures. Nonetheless, by reading and agreeing to the policy, as occurs in Part I Section E, the employee accepts responsibility for their actions and indemnifies the company against being held directly responsible for the actions of an individual. Furthermore, by defining the expectations for disciplinary action as a result of violating this policy, the company protects itself against lawsuits from terminated employees in which this policy was used as the basis for the disciplinary action.

D.Legal Implications: Indemnification Against Indirect Liability

Whereas the policy serves to provide direct indemnification against liabilities stemming from the illegal actions of an employee making unacceptable use of computing resources, the company is still potentially exposed indirectly to liability resulting from those illicit activities. Specifically, if an employee were to make use of computing resources to launch a denial of service attack against a competitor using the company's computing resources, the competitor would very likely pursue legal remedy against the company, and not the individual. For this reason, in addition to clearly defining acceptable behaviour, the company must also implement reasonable countermeasures to limit the ability of the employee to act in an unacceptable manner. To that end, automated and manual monitoring and response tactics must be developed and deployed. The definition of these tactics is outside the scope of the policy, but the existence and use of these methods requires disclosure to employees so as to forewarn that monitoring and enforcement may occur. This forewarning will be discussed in the next section.

Reasonable countermeasures must be deployed by the company to defend against indirect liability resulting from the actions of individuals. Examples of these countermeasures include implementing network monitoring and response tools like anti-virus software and intrusion detection and prevention systems, log aggregation and review, event correlation, and anomaly detection. Furthermore, access control systems must be implemented, reviewed and monitored. System security must also be addressed, such as through patch management processes. Failing to implement adequate and reasonable countermeasures may introduce liability to the company that cannot be mitigated by transfer of responsibility from the business to the individual.

E.Legal Implications: Privacy

To protect against the assumption of unnecessary legal risks and exposure, the company must implement reasonable measures to monitor for and respond to violations of the acceptable use policy. In so doing, the company potential infringes on the privacy of its user-base. However, in signing the policy, the user effectively waives their right to privacy, with the exception of those rights guaranteed by law, and agrees to let the company monitor for policy violations. The matter does not stop here. Whereas the user agrees to be monitored and waives their right to privacy, the company, or its agents, may not abuse this privilege to the extent of violating the rights of the individual. For example, detecting unacceptable use originating from a specific host and tracking that activity to a specific user is allowed, but tracking a specific user at all times with the intention of finding unacceptable use without establishing reasonable suspicion is not allowed. Therefore, the approach used within this policy is to advise the user that monitoring and enforcement may occur, but to reassure the user that they will not be singled out unfairly for application of this law.

F.Legal Implications: Fairness and Due Process

The legal implication of fairness and due process is not specific to this policy, but common to all policies. To quote my own analysis in a previous paper:

> "This implication has to do with the fair and consistent application of rules to all employees without discrimination. These rules must be applied to every employee in the company, regardless of title, race, gender, etc. If the policy is not applied fairly and consistently, then the legal issue of discrimination may arise. Whereas the question of fairness speaks to an ethical concern, it also speaks to legal concerns because the codes of law, to which this policy must be aligned and compatible, stipulate fair application of rules, such as within the business environment."[10]

To recapitulate, this policy must be applied fairly and without discrimination. All resulting actions, whether for monitoring and enforcement or a resulting disciplinary action, must be undertaken in an objective manner that does not target the individual out of context, but instead considers the situation objectively and within the full context.

G.Legal Implications: Adequate Training and Awareness

A comprehensive training and awareness program is fundamental to the success of policies like the acceptable use policy. Furthermore, in the specific case of acceptable use, publishing guidelines and prohibitions have limited effectiveness in helping the user understand the risks represented by unsafe computing. In this day and age, the

[10] Benjamin L. Tomhave, *Use of Licensed Software: Policy and Policy Analysis* (Ashburn: Tomhave, 2004, accessed 31 October 2004); available from http://falcon.secureconsulting.net/professional/papers/315-wk5-Use-of-Licensed-Software-Policy.pdf; Internet.

responsibility is increasingly being placed on the company to fully educate its users about the hazards of interconnected computing and how to make use of computing resources in an acceptable, responsible and safe manner. To that end, Part I Section D articulates the responsibility of the company to provide for employees adequate training and awareness programs and a reasonable opportunity to seek clarification on the acceptability of specific uses. Adding this measure helps further fulfill the responsibility of the company to perform due diligence while transferring additional responsibility for ownership of violations to the employee.

H.Legal Implications: Implied Contractual Obligations

Last, but not least, the "Acceptable Use of Computing Resources" serves as an implied set of contractual obligations. The company sets forth its expectations for behaviour and performance, commits to performing due diligence in providing training, awareness and countermeasures, and requires that the employee abide by the terms of the agreement. Breaking with the promise made in Part I Section E may be considered a breach of contract and could result in termination of the employee. Whereas this policy is not formally presented as a contract, it has the same power as a contract and could be enforced as such in a court. The agreement is not only signed by the employee, but it is also signed by a witness who could attest under oath that the employee was provided with the terms of the agreement and given opportunities to resolve questions or seek clarification.

It is important to consider the policy as a contract for behaviour because it further allows the company to transfer responsibility to the employee in a situation where a violation or incident has occurred. For example, given that the company has implemented reasonable countermeasures, monitored for abuse, and acted in good faith on perceived violations, it would be very difficult for a victimized organization to win a case against the company on the grounds that the actions of an individual, contrary to company policies and efforts, represented actions approved or endorsed by the company.

In contrast, if the actions were undertaken within the defined acceptable use policy and as authorized by the company, then a victim would have a much stronger case against the company. The individual could point to the policy as evidence that they were acting in an acceptable manner and place the responsibility on the company.

REFERENCES

1. America Online, Inc. *AGREEMENT TO RULES OF USER CONDUCT*. Dulles, VA: 2004, accessed 30 October 2004; available from http://www.aol.com/copyright/rules.html; Internet.

2. EarthLink, Inc. *EarthLink Acceptable Use Policy*. Atlanta, GA: 2001, accessed 30 October 2004; available from http://www.earthlink.net/about/policies/use/; Internet.

3. Kinnaman, Dave. *Critiquing Acceptable Use Policies*. Unknown, US: Kinnaman, 1995, accessed 30 October 2004; available from http://www.io.com/~kinnaman/aupessay.html; Internet.

4. Merit Network, Inc. *MichNet Policies: Acceptable Use Policy*. Ann Arbor, MI: Merit, 2003, accessed 30 October 2004; available from http://www.merit.edu/mn/about/policies-acceptableuse.html; Internet.

5. SANS Institute, The. *InfoSec Acceptable Use Policy*. Bethesda, MD: SANS, undated, accessed 30 October 2004; available from http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf; Internet.

6. SoftCom Technology Consulting Inc. *myhosting.com Acceptable Use Policy*. Toronto, Ontario: 2004, accessed 30 October 2004; available from http://myhosting.com/Policy/aup.asp; Internet.

7. Tomhave, Benjamin L. *Use of Licensed Software: Policy and Policy Analysis*. Ashburn, VA: 2004, accessed 31 October 2004; available from http://falcon.secureconsulting.net/professional/papers/315-wk5-Use-of-Licensed-Software-Policy.pdf; Internet.