



1.0 Introduction

1.1 Overview

Policies are essential, as this booklet will make clear. Drafting policies, however, is often a difficult task: fraught with legal, political, and ethical questions and possibly consequences. This booklet suggests why a site needs policies, what a policies document should contain, who should draft it, and to whom it should apply. It is not a comprehensive list of all possible policies: each computing site is different and needs its own set of policies. However, it does provide a starting point for any computing policy and the food for thought to expand to suit specific needs. The goal of this booklet is to provide a comprehensive guide to developing computer use policies that everyone within the organization will be pleased to endorse.

This booklet focuses on computing policies. This is not possible without addressing security and overall business policies as they relate to computing facilities and their use. Good computing policies include comprehensive coverage of computer security. However, the full scope of security, overall business, and other policies goes well beyond computer use and may be better addressed (or may already be addressed) in a separate document. For example, a comprehensive security document should address employee identification systems, guards, building structure, and other such topics which have no association with computing. Computing security is a subset of overall security as well as a subset

of overall computing policy. Ensure that if you have separate policy documents, they refer to each other as appropriate and don't contain excessive redundancy. Redundancy leaves room for later inconsistencies and increases the work of document maintenance.

Note that this Guide does not completely separate system administrator policy from user policy. In practice there are few if any user policies from which a system administrator needs to be exempt. System administrators are users and should be held accountable to the same user policy as everyone else in the use of their personal computer accounts. System administrators (and any other users with "extended" system access) have additional usage responsibilities and limitations regarding that extended access, i.e., extra powers via groups or `root`. These additional policies are addressed in section 5.1.11 on extended access. Further, knowledge of policies governing how staff members perform their duties (e.g. how frequently backups are done) is essential to the users. All the information on the operation of the computing facility should be contained in one document available to both the end users and the support staff to prevent confusion and redundancy as well as enhance communication. Your policy document should be considered a single guide for your users, and your support staff alike.

This handbook is the result of many people's work, from a vast array of sites: commercial, governmental, educational, contractor, and "none of the above." It should be valuable to people from all of these different types of sites.

1.2 What Are Policies

In general, policies are the rules of conduct and behavior which arise from a consensus among a constituency. They begin as voluntary descriptions of normative behavior; and with consensus about them they get implemented. Some get implemented as laws, which are policies made more specific and enforced by a governing authority. Some don't get implemented as laws enforced by the state, but they are still regu-

latory in that some group enforces them and there is some kind of penalty imposed on those who transgress. Even though policies themselves are not the same as laws, policies can act as guidelines for minimum required standards of behavior. If you don't adhere to company policies, you could get fired. The courts have generally recognized the authority of an employer to require employees to conform to minimum standards of behavior; and the best to publicize that behavior is by making the rules be policies, put into a policy binder and distributed to each employee.

The computing policies for your site will be explicit statements of expectations: the expected conduct and behavior of your users, staff, and systems in the operation of the computing facility. To be most effective and accepted, your policies should be a result of consensus in your computing community. Usually the consensus (or dictum as the case may be at your site) exists, but the documentation of that consensus in the form of a policy document does not.

Policies should not be (although they often are) impenetrable documents written in legal jargon and read only when and if there is a dispute about who does what to whom. Policies should be working documents developed cooperatively within a group of people with the aim of making life and work easier than it might be in an anarchic environment. Just as with laws, policies have little meaning if they are not universally regarded as useful and reasonable. On the other hand, a policy document must have legal bearing. A dispute will eventually arise, and the policy document should adequately address how to deal with it.

1.3 Why Have Policies

Policies establish the acceptable standards of behavior in your facility. Additionally, they are essential for communicating consensus on an issue. When a decision is made regarding how a particular situation should be addressed, write it down. The collection of decisions is effectively policies. Having them written down in an accessible location provides dis-

semination of the information, which prevents confusion and duplication of effort among staff and users.

More specifically, computer use policies should provide:

Liability Abatement: Policies prevent anyone from saying “I didn’t know I wasn’t supposed to do that.” They may prevent or mitigate external challenges (e.g., audits, complaints, lawsuits).

Fairness: Policies level the playing field; all users are treated fairly with respect to the classification of account each may have.

Consistency: Similar problems are dealt with similarly.

Understanding: Everyone knows what to expect.

Conservation of Time: When rules are laid out in advance, the time to consider how to address a specific issue is eliminated or minimized. Policies may, in fact, prevent a problem from occurring in the first place.

Training: Policies can quickly introduce newcomers, users, and staff to the operations within the organization.

1.4 Consequences of Inadequate Policies

Unless a work group is both very small and very homogeneous, there are bound to be differences among its members in attitude toward and understanding of what is or is not acceptable behavior or practice. Some people may assume that rules do not apply to them because they are too smart or too important. Others simply may not know that a particular action might have nasty consequences for others or for the group as a whole. Others (yes, they do exist) may be paralyzed by the absence of specific permission to do certain things. And all, at one time or another, will run into a conflict with someone else necessitating some sort of arbitration. In the absence of an agreed-upon policy, there is often no reasonably fair way to decide who is right.

Because policies can be difficult to write and implement, many sites go without any for years. The lack of policy leaves situations to be dealt with as they come up: often arbitrarily, unfairly, and/or by someone without authority. Such sites

have unhappy staff and unhappy users as a result of confusion or unfair treatment.

Lack of or inconsistent enforcement of formal policies can also present serious legal liability. For example, consider a site that wants to terminate an employee for particularly heinous conduct. For such termination to be “lawful” in most states, the employee must have been told in writing that such conduct would lead to termination. Even if such conduct was “well known” by the people in the group to be unacceptable, lack of documentation leaves the company wide open for an unlawful termination suit or keeping an employee no one will trust.

These days a company’s entire assets may be in its computers: information. Failure to protect and manage it with clearly documented policy is mere folly.

Consider the case of *State of Oregon vs. Randal Schwartz*. Mr. Schwartz, a consultant, was accused of violating Oregon’s computer crime laws in accessing the computers of his consulting client during his consulting contract. The legal action was his client’s response to his violation of their computing policies. However, it was well known among employees of his client that the policies were not enforced and were regularly breached by the employees. This entire unfortunate and costly situation could have been prevented with better policy practices. To be considered adequate, policies need to have complete support by management and be equitably enforced. See Section 6 on suggested reading for a Web site containing details of the incident.

1.5 Policies vs. Procedures

Policies document what is expected or what will be done. Procedures document how a policy is implemented. An example of a policy statement might be “backups are performed nightly.” Procedures are the actual steps used to accomplish or implement that policy. Procedures might take the form of a shell script, a checklist in a book, a simple cron job, or an action (or inaction) by a person.

Procedures often imply a policy that no one realizes is in place. For example, a company that has a `cron` job running backups every night has implied the policy “backups are performed nightly” in the procedure, “`cron` runs the backup command and writes the data to tape; then we take the tapes and put them in storage.”

Such implied policies are often all a site has; they are often all a company thinks it needs. This is a dangerous practice, however. To begin with, it may not be clear to everyone what policy is embedded within particular procedures. To take the above example: if the `cron` fails to run a backup, should anyone worry about it? Why? In the absence of a clear statement such as “backups are performed nightly,” staff may simply ignore the failure to make the backup. Procedures almost always imply some policy, written or not. Always consider the implied policies of existing procedure and ensure they are incorporated into the policy document being developed.

Conversely, policies do not always imply a procedure. “Thou shalt not kill” is a policy that does not imply a procedure. “An eye for an eye” does. Recognize the difference, if only to ensure procedures are devised where necessary to carry out new policy.

1.6 Types of Policies

Recognizing the various sets of policies in place, written or not, is important. Consider the following:

- Corporate policies
- Corporate security policies
- Corporate safety policies
- Computer site or facility user policies

Different sets of policies may overlap in scope. Generally, policies written at a higher level need not be repeated lower down, but not always. Many people may be confused about how corporate policies about privacy and theft apply to computer use, for example. Even though both topics may be cov-

ered under corporate policy, repeating them in specific related terms in a computer user policy is prudent.

Although several different classifications of users may be defined, consider how redundant their policies may be. As a general rule, if two policies have 50% common material, then fold them into one document, noting the differences for each classification in the relevant sections. Otherwise separate policy documents may be in order. There may be several classes of users (i.e., students, faculty, and staff at a university) for whom somewhat different policies have to be written. If several geographically separate sites exist, each may need a somewhat different policy document to adequately and clearly address various environments. In all cases, care should be taken to avoid conflicting policies within a single organization. Ensure that computer use policies are consistent with the overall organization's policies.

Sites which provide computing facilities to their customers or the public, such as Internet Service Providers, should consider primarily two separate user policies: one for the public (external) and one for employees (internal). Most likely the public systems are managed differently than employee systems. Further, the internal employee computer use policy may be confidential for system security purposes. The external user policy will be the guide not only for those users, but for the employees in doing their jobs in maintaining that environment and assisting the customers.

1.7 General Guidelines

A number of general principles should be kept in mind when writing policies documents. Among them are the following:

Simplicity: Keep things simple and straightforward. Consider that an intricately designed document will probably not be read as carefully as necessary.

Clarity: Do not underestimate the difficulty in writing policies that cannot be misinterpreted. Consider hiring a technical writer or editor to put the final touches on the policy document. If a policy is not clearly expressed, it probably is worse than no policy at all. A good principle to keep in mind is that the average user should be able to figure out whether a particular action will or will not violate the policies.

Preciseness: Write as precisely as possible. If the policy is, for example, “unacceptable behavior will be punished severely,” then define “unacceptable” and “severely.” Sometimes it is not possible to anticipate and iterate everything. In such cases, describe the nature of why behaviors are unacceptable as a guideline to apply against new situations. For example, unacceptable behavior is anything that may interfere with the use of systems by other people, or that may violate system or data security.

Language: Use simple, everyday English. Avoid jargon, especially legal and computer jargon.

Explicitness: Do not assume that what is obvious to the policy writers is obvious to everyone else. Policies should be accompanied by a short explanation of why they exist, except in the most obvious cases. A policy prohibiting reading other people’s mail may not need an explanation. One regulating access to the Internet probably does.

Length: Try to keep the policy document reasonably short. A long document will discourage readers and may not be read in its entirety by a large percentage of people.

Organization: Make sure the policy document is structured carefully: policies should be grouped according to topics, and topics should be organized from the more general to the more specific. Some key items may bear repeating or emphasis by locating them at the beginning or reiterating them in an appendix.

Generality: Do not attempt to write policies to cover every possible contingency. Firstly, it is not possible to cover the unforeseen. Secondly, broad, general statements, expressing intent rather than specific goals tend to be

more successful (assuming one measures the success of a written policy by how seldom it is challenged).

Detail: As a corollary to generality, avoid excessive details or details about matters that are likely to change often. Policies should not require revision every time some new version of a piece of software is installed or the cost of some service changes.

Tone: Know your audience. Policies to be read mostly by engineers probably should be written differently from those aimed at students in a humanities department. Try not to make policies sound authoritarian to any audience. Do not SHOUT by using lots of capital letters or bold type. Review the policy from the readers' perspective. Don't be apologetic either.

Appearance: Consider the physical appearance of your document. A good design will help convey your policies. Include a complete table of contents and index so the policy may be readily used as a reference. As with clarity, do not underestimate the value of appearance nor the difficulty of producing something that is easy and pleasant to read.

Style: The writing style should be consistent throughout. If several people contribute to it, reword the document for consistent writing style. Inconsistent style can be distracting.

Legality: Take legal requirements for your particular situation very seriously. Include the organization's legal services in the design of the policies. This does not mean lawyers should write the final text (which is usually a mistake), but they should suggest some necessary policies and provide advice on whether various policies are in fact legal and enforceable. Do not assume to know the law, especially when dealing with personnel issues and sensitive issues such as harassment and free speech.