2 *Short Topics in* Systems Administration

# A Guide to Developing Computing Policy Documents

Edited by Barbara L. Dijker

SAGE
THE SYSTEM ADMINISTRATORS GUILD

*Short Topics in*
**System Administration**

2

# A Guide to Developing Computing Policy Documents

**Edited by Barbara L. Dijker**

Published by the USENIX Association for
SAGE, the System Administrators Guild
1996

ISBN 1-880446-57-80-4

Copies of these publications are available to members of SAGE for $5.00 and to non-members for $7.50. Outside the USA and Canada, please add $3.50 per copy for postage (via printed matter).

For copies and for membership information, please contact:
The USENIX Association
2560 Ninth Street, Suite 215
Berkeley, CA 94107 USA
Telephone: 510.528.8649
Email: *office@usenix.org*
Web: *http://www.usenix.org/*

First Printing, September 1996



Printed in the United States of America, on 50% recycled paper, 10-15% post-consumer waste.

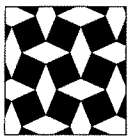
## ACKNOWLEDGMENTS

Many people contributed to this document, including the entire SAGE Policies Working Group. Of particular note are those who contributed text: Dan Appelman, Lee Damon, Rob Kolstad, Hal Miller, Wes Morgan, David Parter, Mary Seabrooke, and Elizabeth Zwicky. This document would not exist without their contributions.

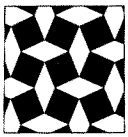
*Barbara Dijker*

## NOTE

This document liberally uses terminology and references common to UNIX systems and TCP/IP network administration. No attempt is made to define them here.



# Contents



# 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.

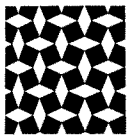
**Legality:** Take legal requirements for your particular situation very seriously. Include the organization's legal services in the design of the policies. This does not mean lawyers should write the final text (which is usually a mistake), but they should suggest some necessary policies and provide 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.

## 2.0 Overview of Policy Documents

Computing use policy documents actually cover a much broader collection of topics than simply usage of one's login. The outline guide in Section 5.0 covers all these areas, assuming, as is all too often the case, that other written policies do not exist. Splitting the policy document into separate documents may be appropriate. For example, a comprehensive security or safety policy may already exist. Don't reinvent anything. Reference appropriate documents as needed.

The following are the primary components of a comprehensive set of policies:

**Usage:** basic user policy
**Security:** all aspects of security, including computer and data security
**Safety:** all aspects of safety, including the safety of users as they use the computers as well as the safety of computers from the hazards of things like soda in the keyboard (A safety policy may already exist as a result of government regulations.)
**Facilities and Resources:** where you might maintain an exhaustive list of the computing services available to your users, the conditions of use specific to each resource, and the support provided for each
**Use Agreements:** usually a one page-document users sign to acknowledge the existence of the policies and their responsibility to follow them (It's a formality that can prevent many headaches.)



# 3.0 Writing Guidelines

Before we get into the meat of the policy document writing process, here are some things to keep in mind.

## 3.1 Goals

The primary goal of a policy document is to communicate information to the site staff and users. Keep this in mind throughout the process. To enhance understanding of the policies, consider for each policy statement the following *W*s:

**Circumstances (What, When):** Under what circumstances or time considerations does the policy apply?
**Principles (Why):** Users are often more agreeable to a policy when they can understand the need for it. If a policy exists to comply with the law, say so.
**Methods (Ways):** If there are specific procedures a user must follow to comply with a policy, reference or include them.
**Security and Privacy (Why not):** A policy often has a flip side for why it exists. For example, the reason users are not allowed to disclose their passwords is because each account is for use by one person. The flip side may be that without such a policy, verifying authorized access becomes impossible. Consider including the flip side if it enhances understanding.

## 3.2 Tools

Your policy document should be composed using the most appropriate word processing program available to you. For the easiest and most effective distribution and availability of

the document, use something that can generate or be converted easily to HTML. TEXinfo is ideal if you support many text terminal users. In addition, your document will have many internal references and should have an table of contents, index, and bibliography. Ideally your choice of tool will automatically maintain the consistency of this information, such as FrameMaker. FrameMaker was used for this booklet.

### 3.3 Style

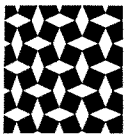
The style of your policy document is secondary to its contents. The most important aspect of style to consider is consistency. Whatever writing style you use, use it consistently throughout the document. Changes in writing style will be distracting to your readers. Remember there is no excuse for spelling mistakes – use a spell checker. You should also have the document read by a copy editor who can clean up grammatical errors, awkward sentences, and those spelling errors a spell checker cannot find. Good grammar enhances comprehension. Poor grammar is distracting for those who know better.

### 3.4 What To Leave Out

The most important things to leave out are those that change frequently. Change people's names to titles, and add an easily updated appendix showing who has that title today – with phone number and email address. Do the same for primary computer resources. Avoid procedural detail. When you feel compelled to document some procedure, go ahead and do it, but put it in a separate procedures document. Start one if one doesn't already exist. Also try to avoid other excruciating detail or legal jargon, which can get in the way of more important information.

### 3.5 Document References

You'll find yourself referring to documents both internal and external to your site. Try to keep a bibliography that includes the location where your reader can find the reference document. A hypertext link to the document is ideal.



# 4.0 Developing Policy Documents

Use this section as a step-by-step guide to developing a formal computer user policy document. Each step corresponds to a "phase" in the development of a policy document.

## 4.1 Determining Authors

Assemble a team to develop the policy documents. Developing a set of policies should be a cooperative venture. There are too many potential consequences of establishing a policy to leave its development to a single individual. Consider a team comprised of the following individuals to address each perspective:

- A senior system administrator who is well acquainted with the site for which the policies are being written and knows the implicit policies already in place
- Someone in a position to make decisions and to make them stick, i.e., someone reasonably high up in management
- A representative from the legal department or the company's attorneys
- A good writer; not necessarily a technical writer as policies do not need to be technical documents
- A typical user, one who is representative of or can represent the overall user population affected by the policies to be developed

None of these people, except the writer, should be expected to be involved with every line of every policy, but all should

have the opportunity to offer comments, and all should come to an agreement about the spirit, if not the actual wording, of each policy. The user representative will need to communicate with the user community during the process to ensure its acceptance of the final product. The management representative must "sell" the policies to the head of the organization. In addition, during the process of writing the policy documents it will be necessary to actually set policy that may have not yet been decided or may currently be in dispute. The development team needs either the authority to make these new policy decisions or a direct channel to someone with that authority – preferably via the team management representative. Regardless of the authors or origins of your policies the final policy document(s), to be useful, must eventually be accepted by those in charge as well as the rank and file.

Elect someone to be in charge. Without a leader, the project will stagnate. The leader must "champion" the project. The leader should be someone with the time and motivation to do the work who will shepherd the others into finishing their parts. The leader is often the system administrator or user, whose life will be much simpler when the document is completed, or the manager, who may be skilled at leading a project of this magnitude. In cases where most of the team members are too busy, the writer may lead the project – extracting the data from the appropriate gray matter as necessary.

The leader's first job is to develop a project time line. Each following step of development will need a deadline and someone responsible for ensuring the deadline is met with quality results.

One approach in the roles of the team members would be to have the user representative primarily develop the first draft of policies. This ensures the perspective of readability and support by those affected which is essential for effective policies. The system administrator should then review the policies for completeness and technical implementation feas-

ability. Then give them to management for substantive review, the writer for style and grammar, and finally the lawyers for legal review.

## 4.2 Determining Scope

Develop the scope of the policy document(s). This includes developing an outline and determining to what and whom the policies will apply. Use the outline in Section 5.0 of this booklet as a starting point, and then agree upon the scope of the document: which users are affected, what systems are covered, other policy documents this one augments, etc. The entire team must arrive at a consensus on this issue before development can progress. Once everyone agrees on the basic structure and where the document is going, then parts of it may be delegated as necessary.

After developing the scope and outline, reread this booklet to check for anything you may have overlooked.

## 4.3 Existing Policies

Collect all existing policies. Consider these sources:

- Existing incomplete or scattered policy documents
- Policies implied by current unwritten practice
- Policies implied by current written or unwritten procedures

Remembering all the unwritten policies already in place is no easy task. The details in Section 5.0 should jog your memory. Use Section 5.0 as a guide to scribble down existing policies to be embellished later. This step is best accomplished by the system administrator and the user on the team.

The purpose of collecting existing policies is to ensure they are included in your new document and to provide a substantial starting point.

## 4.4 Writing the Document

Everyone on the team should be familiar with the guidelines and information in this booklet. Sections of the document

can be delegated to various members of the team or outside the team if appropriate for the topic. Review progress regularly to keep up momentum. The entire policy team should review drafts of the document before it is considered done. You might have some additional people review the close to final document to gauge readability and ease of comprehension – a market focus group of sorts consisting of users, staff, and management.

The user representative on your policy development team is supposed to act on behalf of the users. However, if practical in your organization, an open review by all users of the final draft would greatly increase the acceptance of the policy document. As an alternative, only excerpts of the document which describe any resulting newly formed policies might be made available for an open user review. A user community will be more readily inclined to support policies to which they were able to contribute.

## 4.5 Approval and Authorization

The highest levels of management must be committed to the necessity of a set of computer use policies, and then to the final policies themselves. Anything short of this commitment allows individuals to appeal policies to those members of management who are perceived not to be committed to them. This leads to unfair or inadequate enforcement that undermines the purpose of your policies.

Once the policies writing team is satisfied with its draft document, it must have management "sign off" on it. This means having the site's highest manager actually sign the document. This is one of the good reasons for having a team putting together policies: management can be assured that all who are being affected by the policies have been represented in the process.

When distributing the final document, make sure it is clear who signed off on it so there is no confusion about the authority standing behind it.

### 4.6 Distribution

At the very least, every person covered by the policy should be sent a written notice (signed by the same manager[s] who signed the policy) that the policy exists, where a copy can be reviewed, and when it takes effect. Ideally, each affected person should also be required to sign a use agreement to acknowledge the existence of the policies and receive a printed copy for future reference. Ensure that the hiring and new user procedures at your site are modified to continue to distribute the policy information and obtain the required user agreement signatures when necessary.

### 4.7 Reviews and Changes

Your new policy document is a living entity. It will require ongoing care and feeding. Your team should be prepared to meet on a regular basis to review and revise the document. This doesn't need to happen frequently, but it needs to occur. The policy document itself will contain information on how frequently this should happen and how suggestions for changes are submitted and reviewed.

### 4.8 Enforcement

This step is also ongoing. The policy document will contain information regarding how the policies will be enforced and how grievances about them will be resolved. If a new committee or title has been invented to deal with policy enforcement, now is the time to ensure the committee or responsible person is given the tools to do this job. If a new procedure is warranted, develop and document it. Enforcement, or the application of the policy, is the most important step in its life cycle. You don't want all your work to be for naught.

# 5.0 Policy Document Detailed Outline

Use this section as a recommended outline. Your document doesn't need to use the same sequence or number of topics. This is a recommended starting point. The sections marked with a ‡ are considered essential if not mandatory; think thrice before omitting them. Those sections marked with a † are highly recommended. Those sections with neither marking would make your document more complete. To help get you started, each of the outline sections includes a brief description of the intended contents of that section or questions it should answer for the intended audience. In some sections are suggested approaches to your policy. Your policy does not need to address everything here. Choose what is appropriate and necessary for your site to the level of detail your team can muster. The outline we use here has five sections which can be parts of a single document or merged into one: Usage Policy, Security, Safety, Facilities and Resources, and Use Agreement.

## 5.1 Usage Policy ‡

The first page of this document should be the management signoff, usually in the form of a foreword or the letter of notice of its existence to the users and staff.

### 5.1.1 General Information

Include in this paragraph any information you want to highlight at the beginning of the document. You might want to include here things like why this document exists, who made it happen, and how important it is to your organiza-

tion. This should set the tone for the document. If this policy document is considered confidential to your organization for security reasons, make certain you spell that out here. You may also want to put a "confidential – for internal use only" footer on the document as a reminder.

### 5.1.2 Scope and Applicability †

Once the scope has been determined in the policy planning, it should be made explicit in the policy document, preferably at the very beginning. This section can and should be written by the entire team and agreed upon before continuing.

### 5.1.3 User Accounts ‡

Include basic user information as close to the beginning of the document as possible so your document can assist new users.

#### 5.1.3.1 Account Types †

If your site has more than one classification of user, describe them here (e.g., students, faculty, and staff at an educational organization). In a company, you may have regular employees, contractors, vendors, and guests. Any time a policy may apply to some users and not others, you have different user classifications. If support is prioritized by some perceived importance of the user, then that also implies different user classifications. Note that we treat systems staff just like other users throughout most of this document, with specific policies for them in Section 5.1.11. Because extended `(root)` access may be given to any user in any account category, it really isn't its own category. However, if you feel that your policies should specifically not apply, or apply differently to your system staff, then identify them as a separate account type here.

#### 5.1.3.2 Account Eligibility †

For each login account type, document how people become eligible for that categorization. For example, are consultants or subcontractors eligible for accounts in the same category as their employee peers? Do student users have to be majors

in your department to qualify for certain access or just enrolled in a department course?

#### 5.1.3.3 Application

Use this section to document how users obtain an account. Is there an authorization policy for any of the account types? Where is the application form? To whom should it be given? How long does the process take?

#### 5.1.3.4 Login Security ‡

Identify here the measures users are expected to take to ensure the security of their account. Security is addressed more comprehensively throughout the document. Include here requirements for passwords, `.rhosts` files, etc. If you have different account login security policies for local access vs. modem or `telnet` from the outside, document them both here.

#### 5.1.3.5 Intended Use ‡

Use this section to outline the purpose for which accounts are given, i.e., what use is expected, sanctioned, and encouraged. This doesn't need to be an exhaustive list. It may require different statements for each account type. The idea is that identifying the intended use will make the specifics of the next section more palatable and understandable. If different systems have different intended uses, a general list of system categories would be appropriate. Include a reference to the facilities and resources section (see 5.4).

#### 5.1.3.6 Acceptable Use ‡

Outline more specifically the limits of what usage is generally acceptable. For example, maybe you expect users to do only work on the systems, but occasional personal use is allowed. Try to draw the line as clearly as possible. You can't itemize every possible infraction here. The users need enough information to be able to make their own judgment calls. Liberally use examples to illustrate the policy. For example, "casual personal use is OK. However, this use should not interfere with other users, use significant resources such as

CPU and paper, or support any commercial or illegal endeavor. As an example, composing and printing a letter is OK, printing flyers for your sideline business is not."

This is the area that can give you the most trouble. You need to be restrictive enough to give you the support to take disciplinary actions if necessary. At the same time, you need to be realistic. If users are commonly known to be allowed to engage in use prohibited in one part of this document, the entire document loses weight and value.

#### 5.1.3.7 Expiration/Deactivation/Revocation †

All sites need a policy for aging or expiration of accounts – usually when an employee or student leaves the organization. But how soon after that is the account actually removed? What happens to the user's files? In addition, address here account deactivation or revocation for any other reason. Can users lose their accounts for violating these policies? Are there any other conditions under which users could lose their accounts? Are these events treated the same or differently?

#### 5.1.3.8 Reactivation/Recourse

How are accounts reactivated? The policy may be the same as applying for a new account. But what if the account was previously terminated with prejudice or under other atypical circumstances? Does the person responsible for handling new accounts have a mechanism to find out an applicant's previous account was terminated (you can't rely on memory here)? If an account application is rejected, what recourse does the user have? Is there a committee appeal? Are accounts a right or a privilege? Refer to Section 5.1.5 on general conduct.

### 5.1.4 Getting Started

This section is more procedure than policy. It is generally included here to help new users find their way around the computing facility. If this document will not be available to new users before they login, then you should consider removing this section to or replicating it in a small document or sheet that is printed and given to each new user. If you

do separate this section, don't forget to include a reference to this main document for further information. Address these essential new user topics:

**Logging in:** basic procedure as well as any site specific information
**Changing your password:** run `passwd`, `yppasswd` or something else
**Staying informed:** where and how users may find important notices
**Getting help:** pointers to documentation and the support section of this document

### 5.1.5 General Conduct ‡

Treat this section as a more comprehensive guide to usage than Section 5.1.3.6. Where that section addresses more about the right and wrong, this section should address more about etiquette.

#### 5.1.5.1 Resource Conservation

What resources are generally considered scarce, expensive, or otherwise at a premium? Maybe it's a main system where specific time sharing policies apply. Maybe it's the high cost of toner and paper. In this section address these issues and how the users are expected to exercise restraint. If there are specific guidelines that may help, include them here. For example, a short treatment of how to use the available software for screen previewing and 4-up layout can go a long way toward conserving printing resources.

#### 5.1.5.2 Professionalism

This area may or may not require express iteration at your site. For example, you might want to include here some discouragement regarding practical jokes upon other users. Rely on past experiences to decide how far to take this section.

#### 5.1.5.3 Common Courtesy

This is the "do unto others" section. Examples of policies you might include here are:

- No printing of jobs >N pages on X class printers
- `nice` all jobs expected to run more than N minutes
- No games during business hours

#### 5.1.5.4 Employer Reputation †

Use this section to remind users that their use of the system for communicating outside the organization makes them representatives of the company. If your organization requires a disclaimer on external email or USENET news articles, provide that here and/or reference it in the appropriate part of Section 5.1.6.

#### 5.1.5.5 The Law †

You can't expect to reiterate all laws which may affect computer use at your site. Use this section to remind your users of the most important ones – those that could put your organization at risk without compliance, e.g., copyright law, patent law, and the Communications Decency Act. At the very least, simply state that illegal activity is not permitted. This is extremely important. Your computing facilities could be seized by law enforcement authorities because of the activities of your users. Even worse, your organization could be implicated in those activities.

#### 5.1.5.6 Offensiveness and Harassment †

Your organization may already have policies regarding sexual harassment in the workplace. Use this section to interpret that policy as it applies to computing facilities. For example, data that could be considered offensive to others should not be left in unprotected file areas such as `/tmp` or displayed on unattended terminals or in public areas. Do not limit your treatment of this topic to images and text. Scratch and sniff files are almost on the market. You don't know what else will be next.

#### 5.1.5.7 Access of Other Sites ‡

Are there computing resources outside your organization to which your users will have sanctioned access? If so, refer to their policies here. This section is also appropriate for a gen-

eral statement that use of other computing facilities must comply with the policies of that site. You may want to include a statement regarding the use of your facilities to attempt to or actually violate the security or policies of another site. Consider a case where you have a generally well behaved user who is using your facilities to hack into other sites, e.g., running `satan`, a port probe, or `crack` on others' `passwd` files. If you were on the other side of this coin, what policy would you expect?

#### 5.1.5.8 Maliciousness †

You might think it wouldn't need saying, but an explicit policy against any malicious or suspected malicious use is wise. For example, deleting other users' files is probably considered malicious. Running `crack` on the `passwd` file or running the "`rootkit`" suite, `satan`, or other security tools should be considered suspicious. For example, maybe your policy is that users who are not directly responsible for system security are prohibited from running such programs or even having copies of them in their file area. Consider this issue carefully, and make your policy statement here succinct. Remember that this policy must be uniformly imposed on all users in each account type category. Exceptions should be explicitly stated here.

### 5.1.6 Resources and Services †

Describe here the resources that as a policy are made available to users. In the previous section you outlined the conduct expected of users. Here you'll outline the conduct of the systems. If there are specific usage restrictions or user conduct for a specific resource, make sure you state this here. In this section, describe the basic computing environment available to all users at your site. Don't get carried away here. Limit your treatment to site-specific information. Don't get mired in configuration details that will hinder the systems staff when a change is warranted. If you choose to omit this section, at least provide a reference to where the information may be obtained. In the worse case, this would involve asking support staff.

#### 5.1.6.1 Disk, Memory, and CPU

What computing and disk resources are available? Is there a public scratch disk area? Are memory limits imposed? Are disk quotas used? What should users do if these resources are inadequate for their needs?

#### 5.1.6.2 Software

Where are locally installed programs? Generally, what packages of software can the user expect to find installed?

#### 5.1.6.3 Electronic Mail

What does the mail environment look like? Does each user have a POP account? Is non-POP mail accessible from multiple machines (cross-mounted spool)? What is the preferred way for users to advertise their external email addresses? Is email to the Internet supported? Is there a gateway or proxy? Is email to other networks (internal or external) supported? Do you use "first.last" alias conventions? Where is an internal email directory?

#### 5.1.6.4 Printing

What types of printers can users expect to find? Color? Laser? Line? Postscript? HPGL? What tools are available to get various types of data out to the printers in the appropriate printer interface language? Are duplex mode printers available, and what tools or invocation options are used to access that feature? Are banner pages printed? Are printouts delivered, or must users pick them up? Are old unretrieved printouts thrown away? How often? Does your organization have a recycling policy?

#### 5.1.6.5 Data Archival

What off-line storage devices are available to users? Are media also available, or must users provide their own? What are the logistics for using shared devices? You might include here a reminder that copyright software and confidential data should not be written off-line except as required in the user's job responsibilities.

#### 5.1.6.6 Network †

What network access exists? A simple, logical network diagram is appropriate here. Include on it connections to external networks (other sites, the Internet), WAN speeds, and the location of major resources. Describe your firewall and proxy configurations. What external network services require a proxy, what services do not, what services are disabled entirely? Is USENET news available? What is the policy for accepting newsgroups? Are posts restricted or filtered? Use this section to discuss or refer to netiquette. If sales or marketing staff will have access to the Internet, explicitly state here policy on advertising via the Internet or refer to Section 5.2.1.4 on publication and dissemination. Inappropriate advertising activity may pose serious risks for your organization.

#### 5.1.6.7 Remote Access (dialin) †

These days users expect their employer to provide some sort of remote access for use from home or while travelling. What remote services are available? Modem speed? Protocols? Is this access behind or in front of the firewall? Are users allowed to set up a modem on their office workstation? Are there restrictions on what a user may connect remotely? For example, you would expect users to connect just their home or laptop computers. But what if users have a LAN at home with another external connection? This represents a serious security problem if remote access is behind your firewall. Is special approval required to obtain remote access? What is the policy for remote access when travelling? Can the user expect to be provided a local dialin at another facility? Is there a toll-free number?

#### 5.1.6.8 Other Primary Resources

If you have any other significant types of resources, don't forget to address them here: scanners or other specialized input devices, video conference, etc.

### 5.1.7 Training

Use this section to describe the computer and technical training available to your users. This should not be limited to

training provided internally by your organization. Include references to sanctioned external training resources as well. In addition, you may want to include information on who is responsible for aspects of training: providing, scheduling, funding, etc. Consider providing a training session or orientation for new users to help them become familiar with your computing facilities and its policies.

#### 5.1.7.1 Eligibility

Is training available to all users or just some or under special circumstances? What approval is required? Is any training required to use certain resources?

#### 5.1.7.2 Internal Courses

Itemize here the topics, if not the entire list of course scovered by internal training. Reference where users may obtain detailed course descriptions and schedules.

#### 5.1.7.3 Third-party Courses

When are third-party courses allowed? Are eligibility and approval requirements different than for internal training? Is there a list of sanctioned training providers?

#### 5.1.7.4 Adding Courses

How do users suggest courses or obtain training for a topic not listed here? Can users volunteer to teach a course in their area of expertise?

### 5.1.8 Usage Monitoring †

An important part of the support staff's responsibilities is to monitor resources both for security and to ensure resource availability. This can be a very sensitive area for users. Clarify in this section what will be monitored. Make sure you give support staff enough room here to trace a hacker. For each type of data below, address the following concerns:

**When:** routinely, occasionally, in a security event, with prior permission only, to provide support only?
**To what extent:** all data, random sampling, for gathering statistics only?

**Disposition of monitored data:** destroyed, kept confidential, made public after reducing to statistics (with or without user identity)?

Address these types of data with the above concerns:

**User input and output:** user keystrokes, mouse movement, terminal output, and window displays
**Command execution and history:** process accounting information and user and system history files, e.g. `~/.history`, `wtmp`, `sulog`, `~/.rhosts`, `.forward`
**Printing logs:** printer accounting logs and fax logs
**Disk usage:** file size, type, age, permissions, ownership, and contents
**Remote access:** modem logs, `telnet` logs, etc.
**Network packets:** headers and/or data
**Message and data transfers:** email, news, and FTP transfers and their transaction logs

### 5.1.9 Data Integrity †

Use this section to address how the integrity of both system and user data is safeguarded. Users need this information so they can supplement with their own archival if needed. Remember to address all user data areas. This section also is an important guide for support staff.

#### 5.1.9.1 Goal of Backups

Every backup strategy has a primary goal. It may be expeditious recovery from catastrophe. Or it may be to provide a product history. State the goal of your backup policy, emphasizing any calculated risks that may be acknowledged. For example, if your goal is catastrophe recovery, you may do a full backup every night and keep tapes for only two days. That means a file that was accidentally removed last week is unretrievable. This goal and policy may be fine for support staff and the organization, but the user will want to be warned.

#### 5.1.9.2 Frequency

Describe the frequency for live data (incremental backups) as well as static data (full backups). Are any archival snapshots taken outside of this schedule?

#### 5.1.9.3 Storage Period

How long are backup tapes stored? Are all the tapes stored, or just the full backups? For example, let's say you perform daily incrementals and monthly fulls, and keep the incrementals for two months and the fulls for two years. This means a file that existed last year for less than a full month may not be on any tape.

#### 5.1.9.4 Storage Access and Security

What physical and logistical access controls are used for the backup media archive? Are they in a locked cabinet? Who has access to the key?

#### 5.1.9.5 Off-site Storage

If you use off-site storage, what backups are sent there? By whom? When? Who has access to them?

#### 5.1.9.6 Restore Requests

Can users request file restores? Is there a special procedure for doing so? What information is required to complete the request? Can users restore their own data? If online automatic filesystem "trash cans" provide instant recovery, describe where this is available, and refer to documentation on how a user may retrieve lost files.

### 5.1.10 User Data Privacy †

This is another important and potentially sensitive area. Describe here the extent the user can expect privacy – which implies the limits of system staff access. For each set of files listed below, describe the level of privacy and when and why the privacy may ever be breached. This may at first seem redundant with Section 5.1.8 on usage monitoring, but that section deals more with monitoring the system for resource utilization and security. This section should address overall privacy and confidentiality issues. You can choose to merge the two sections.

**Messages:** email, news
**Personal files:** any user data not related to your organization

**Work files:** user data related to the organization
**System files:** `.cshrc`, `.mailrc`, etc.
**System logs:** `wtmp`, etc.

Remember that system staff need to look at a user's system configuration files to diagnose some problems. If all user data are considered corporate property, explicitly state this here. There is legal precedence in the USA (*Steve Jackson Games vs. the Secret Service*) to support the notion that email messages are considered private personal, not corporate, property. If your organization wishes to assert its ownership of user data, which is also commonly legally defensible, this should be explicitly stated. This is, of course, an area for your lawyers' input.

### 5.1.11 Extended Access ‡

Address here extended or privileged access of all types. This includes `root` access. You may also want to include access to groups or tools which provide some special level of access on your systems, e.g., a tool used to add users. Users with extended access need specific policies to address their special powers. For example, a user delegated the task of adding new user accounts needs to know that this doesn't mean s/he can use this privileged access to add accounts for friends. Don't think Section 5.1.3 on user accounts makes this obvious. Although your system administrators are usually the focus of this section, keep in mind that any extended access may encompass a much larger audience. Your policies regarding the use of extended access must apply to anyone wielding that access, regardless of job title. The following aspects of extended access should be addressed.

#### 5.1.11.1 Available and Supported Mechanisms

Define here what is meant by extended access at your site. You may simply state that any user with the privilege to modify a system's configuration in any way is considered to have extended access. Or you may choose to list the tools that provide extended access. Keep in mind that extended access may also be physical access such as keys to a restricted machine console area.

#### 5.1.11.2 Eligibility

Use this section to address those cases where users request certain privileges. For example, you might state here that extended access will be provided when the user wears a pager with a number published to other users. Also use this area to describe any trial period you may have for newly hired systems staff before you give full `root` access.

#### 5.1.11.3 Demonstrating Need

If eligibility for extended access includes the requirement of demonstrating need, you can address that here or in the eligibility section.

#### 5.1.11.4 Obtaining Authorization

If obtaining extended access requires some sort of authorization, document here exactly who has the authority to grant it, under what circumstances, and the form it will take (in writing preferred).

#### 5.1.11.5 Appropriate Use ‡

Use this section to outline what the extended access is to be used for and expressly what it should not be used for. If you have a large number of users with different forms of extended access, you may want to outline specifics for each user separately in the process of providing that access. At the very least, document here what is expressly prohibited activity. At a university, you may need to state that students with extended access should not use it to read tests before they are given or change grade files. Don't forget to state the obvious, e.g., don't give out the `root` password. There are two basic issues to address:

**Security:** remind users that extended access needs to be safeguarded for system security. For example, maybe your policy for how often users need to change their passwords is different for those with extended access.

**Data privacy:** remind users that extended access is to be used only in performing the tasks for which it was given – not reading other's mail or files.

#### 5.1.11.6 Expiration/Deactivation/Revocation

Describe how extended access privileges are terminated. If there are any events for which you would immediately terminate extended privileges, be certain to note them. For example, what if a staff member gives out the `root` password or reads a user's mail? This is an important and potentially dangerous section. Consider that terminating extended privileges of full-time systems staff is effectively firing that person. Does your policy have the legal ground to do that?

#### 5.1.11.7 Reactivation/Recourse

As in Section 5.1.3.8 on general reactivation and recourse, describe here the recourse users have if their extended access was terminated under Section 5.1.11.6.

#### 5.1.11.8 Root Password Management †

If you don't currently have a policy that dictates how the `root` password is to be managed, create one. For example, "all root access is provided via `sudo`. In those situations for which the `root` password is required, it may be obtained from the `root` password envelope. The location of this envelope will be given to you if you require it for your job duties. Whenever the seal on the envelope is broken, the [`root` password person] will change the `root` password and seal it in a new envelope. If you break the seal on the `root` password envelope, you are required to provide justification."

### 5.1.12 Restricted Access

Do you have any user accounts which provide only restricted access, i.e. more restricted than common accounts described in Section 5.1.3 on user accounts? Use this section to cover those accounts. You should address the circumstances under which users would get a restricted account and the special limitations applied to its use.

### 5.1.13 Fees and Charges †

Describe here all the types of fees charged for any service. You may want to have a separate fee schedule document and reference it here. Or put it in the appendix. The fees them-

selves may change frequently, but the services which incur a charge should be rather static as it is how that service usage is measured. You also may have a policy for how and when the actual numbers are changed which is different than changing the list of fee services and their metrics. Remember to include here the policies for updating this information.

If you have a fee schedule, consider at least these items: access time, disk usage, printer usage, CPU usage, modem usage, archivals and restores, support, bandwidth, and products or parts (tapes, cables, paper, security access cards, keys). Remember to include refundable deposit fees as well as miscellaneous fees like late charges, penalties, and interest.

#### 5.1.13.1 Billing/Invoicing

Describe here your billing policy. Are bills generated? Are they sent to the user via email or paper mail? How frequently? What are the terms or due dates? Are fees ever waived? Who has the authority to provide these fee credits?

#### 5.1.13.2 Payments

What are acceptable forms of payment? Where should payments be made? When, what hours, are payments accepted? What are the penalties for late payment? Will services be terminated for late payment? If you allow payment via any electronic or automated mechanism, provide the reference to how users apply for that service.

### 5.1.14 Support †

Detail here the support provided by your facility support staff.

#### 5.1.14.1 Office Hours and Availability †

What are the regular available hours of support staff? Are there holidays? When are they determined and where are they posted? What is the location of the support staff? Is support available outside the regular office hours? How is this emergency support limited or controlled? Is it available to only certain users or systems?

#### 5.1.14.2 Levels of Support †

Describe the levels of support provided. For example, for all systems you support the OS but not applications or user assistance, which may be provided for an additional fee. Or maybe user workstations are supported at a different level than those of servers. If you don't already have one, you might develop a support level classification and identify how systems and/or users qualify for the different categories. The specific list of systems and their level of support would be documented in the Section 5.4. on facilities and resources.

#### 5.1.14.3 Requesting Support †

What are the accepted mechanisms for requesting support? Is a phone call sufficient? Do you prefer email or submission via a Web form or tracking system program? Refer to an appendix where phone numbers and other relevant details are provided. Do users need to classify their problems and call the right number, or is there a central help line?

#### 5.1.14.4 Support Prioritization

How does your support staff prioritize requests? Usually your staff already has an implicit priority scheme in use – maybe subconsciously. Try to document it. For example, you might define a priority based on the level of severity of the problem and the user type experiencing it as shown in Table1.

**Table 1: Prioritization Scheme for a University Environment**

| Level of Severity | User Type |
|---|---|
| A: System on Fire<br>B: System Down/unusable<br>C: Workaround exists<br>D: Nice to haves | 1: Multiple users, or management escalated<br>2: Faculty<br>3: Staff<br>4: Others |

Each probelm is assigned a level from each column. In this scheme, a B2 would have a higher priority than a C1 – sorted by severity first. This is a common implicit scheme and may be slightly different at your site. Explicitly stating a prioritization scheme helps both users and staff understand

how support loads are handled. Actually implementing an assignment of priority designation to each task in your queue can help you manage time and staff.

#### 5.1.14.5 Resolution †

When and how will users receive information about the resolution of their requests? Provide here any information on response times you either attempt to meet or guarantee. Do users have to request status? If so how? Maybe you have a tracking system that allows users to obtain the status of their own requests. Does the staff provide periodic status information? If so, how often? Is there an escalation policy for requests not satisfactorily resolved after a designated period?

#### 5.1.14.6 Notification †

Invariably, there are events of which the users must be notified, e.g., scheduled downtime, support holidays, upgrades, etc. How are these notices provided? How much advanced notice is required for different types of events or systems (this may vary for the diverse levels of support in Section 5.1.14.2 on levels of support). You'll usually want to have a specified notice location(s) and remind users that monitoring those locations for notices is their responsibility.

#### 5.1.14.7 Complaints and Suggestions

You should accept support and facility complaints and suggestions. Describe here how they should be submitted. In addition, provide information on how they will be reviewed and potentially remedied.

### 5.1.15 Disaster Recovery †

Disaster recovery policy is an essential part of any policy document. Carefully describe how you are prepared for disasters. List the types of disasters your facility has planned for, e.g., natural (fire, flood, earthquake, hurricane, tornado, storms), security, and other hardware failures. You may have specific policies for different types of disasters or for the results of them, e.g., power outage, water damage, structural integrity loss, loss of physical security, compromise of data,

etc. For each "type" of disaster you've chosen to address, provide first the preventive and preparedness provisions in place and second the drills to be conducted to exercise them.

### 5.1.16 Policy Management ‡

Use this section to provide the policies that govern the policies themselves.

#### 5.1.16.1 Enforcement ‡

Who is responsible for monitoring activities and enforcing policy? This is usually system support staff. Will enforcement be proactive or reactive? What are the consequences of noncompliance? Is there a committee or arbiter who decides if a user has actually violated policy and what disciplinary action will be taken? Is there recourse in case of a dispute over compliance or the application of consequences?

#### 5.1.16.2 Exceptions †

If you will ever allow any exceptions, describe them here. Use this section for general policy exceptions. Exceptions for specific policies should be noted in the same section as the policy itself. For example, you might be more lenient regarding a late fee payment than staff snooping in users' files. You don't need to exhaustively list all exceptions. Describe the spirit under which an exception might be allowed, who has the authority to grant it, and what form it will take (in writing).

#### 5.1.16.3 Revision Management †

Anyone should have the ability to suggest a change to your policies. Every time a member of the support staff has to make a nontechnical or "political" decision, that means a new policy has been made and should be submitted for inclusion in the next policy revision. How are change/add submissions reviewed? How are they approved or authorized? How are users notified of policy revisions? How are the revised policies distributed to users? Consider that appendices may need to be updated more frequently than other sections.

### 5.1.17 Appendices

Your appendices might contain these lists:

- Titles of functional responsibilities referred to in this document with the names, phone numbers, and email addresses of those currently holding those positions (e.g., User Account Administrator, System Security Officer, Policy Administrator, Support Manager
- Fee schedule
- Summary of important telephone numbers and email addresses
- Definition of terms
- Bibliography of referenced documents
- Suggested further reading
- Training course details and/or schedules
- Application or other relevant forms

## 5.2 Security †

This security section is separated out of the main user policy document because it typically gets incorporated into an existing, more comprehensive site security document. If you won't have an overall site security document, you may want to fold this section into your main Usage Policy document where you feel it is appropriate. It should address both data security and physical security of your computing facilities. Although security issues have been addressed throughout the entire user policy, this section provides security information that may not be directly related to any of the issues the Usage Policy document covered in section 5.1.

You should describe here your general security philosophy in plain English to set the tone for this section. For example, your policy may be that security isn't a concern – anything goes. Or your site may take security very seriously.

### 5.2.1 Data Security †

#### 5.2.1.1 System Data †

How important to your site are the security and integrity of system data like the `passwd` file and other configuration

files. What would you do if a user mailed the `passwd` file off-site? How are these files protected?

#### 5.2.1.2 Corporate Data †

What about data considered to be the property of your organization? Does this include user data? How are these data files protected and controlled? How are corporate data identified?

#### 5.2.1.3 User Data

If personal user data are not part of corporate data, how are they distinguished? How are they safeguarded from other users, including staff? Do you have default permissions for data areas of new users?

#### 5.2.1.4 Publication and Dissemination †

Address here how users are allowed to communicate data outside your organization. Treatment of this should be independent of the transmission vehicle. For example, if it's inappropriate to disseminate the `passwd` file, it doesn't matter if it was done with email, news, a Web page, or some other mechanism. Do you allow users or staff to create their own forums for publication and dissemination, such as newsgroups, Web pages, anonymous FTP areas, `gopher` spaces, etc.? If so, which ones and what limitations apply to their configuration and content?

### 5.2.2 Physical Security

Overall physical security is often addressed in a noncomputing document. In this section, cover those physical security issues specific to your computing facilities. Do you have any limited access areas? Where are they? Who can have access to them? How is access provided, e.g., key or electronic? Is access logged? Consider any place where you would find computers: offices, labs, and common areas. Is any equipment physically secured to a fixed object? This section is where you would address stealing or tampering with equipment.

#### 5.2.2.1 Equipment Removal

Is anyone allowed to remove equipment from its designated room or the facility? If so, under what circumstances? By whose authority? How is it accounted for? What are the limits on the length of time it can remain out? What if it isn't returned? How is equipment identified as being owned by your organization?

#### 5.2.2.2 Personal Equipment

Do you allow people to bring their personally owned computer equipment on-site? Cover this with the same detail as the previous section, with special attention to identification. How do you distinguish between personal equipment and equipment that is missing a company inventory sticker? Can personal equipment be used for corporate data? Can personal equipment be connected to your network?

### 5.3 Safety

Like Section 5.2 on security, this section is separated here because it often becomes part of the overall safety document that contains non-computer related information. If no such document exists, fold this section into your main Usage Policy or keep it separate, as appropriate for your site. Document in this section any computer safety-related issues that may not have been addressed elsewhere in your policy document. For example, are different alarms, evacuation plans, and drills in place for your computing facility than elsewhere in your buildings? What is your policy on smoking and eating in computer labs? Do you have hardware labs with specific handling policies like clean rooms or electrostatic sensitive areas?

### 5.4 Facilities and Resources †

This set of information is often separated from the main Usage Policy because it generally contains information that may change frequently, allowing it to be kept up-to-date without the same modification policies as the Usage Policy

document. The first trick here is to determine to what level of detail you want to identify resources: by types of systems, per each system, systems and subsystems, software, peripherals, lab space, etc. Then document each identified resource as outlined below.

### 5.4.1 (For each one)

For each facility or resource being identified, provide at least the following information. Clearly, this information would be ideally maintained in a database. An asterisk identifies attributes which may be common to some or all of your resources. You may omit any common attribute data provided that information is included in your Usage Policy document. For example, if all users have access to all resources, you can omit the eligibility information for each resource as long as this fact is stated in your Usage Policy document.

- Type (model/revision)
- Location
- Features
- Availability *
- Eligibility for use *
- Acceptable use *
- Level of support provided *
- Support contact *

### 5.4.2 Adding, Changing, or Deleting

Describe here the policy for adding, changing, or deleting facility resources. For example, what if a user requests that the level of support or vendor support contract be changed?

### 5.4.3 Purchasing

Describe here any policy you may have for purchasing facility resources. Can users purchase only preauthorized vendor systems or configurations?

### 5.4.4 Acceptance for Support

How does new equipment get accepted for specific levels of internal support?

### 5.5 Use Agreement ‡

The Use Agreement is typically a separate document which simply provides a way for your organization to maintain written acknowledgment that a user knows the policies exist and apply to him. The Use Agreement should be short and sweet and minimally satisfy the following four requirements. Every existing and new user should sign a use agreement. At the very least this draws the users' attention to the importance of the policies. Having a signed acknowledgment of your policies may also prevent a dispute or support your organization's position during one.

#### 5.5.1 Purpose †

Why are you doing this? For example, "In consideration of granting the use of XYZ Company computing facilities, each user is responsible for complying with the computing policies of XYZ. The undersigned acknowledges receipt of computing privileges and the policies governing their use." Remind the user that this is a two-way street: the user is getting something, the use of the facilities, in exchange for following policy (which may include paying a fee).

#### 5.5.2 Term †

How long does this apply? Primarily, this part is to satisfy a common legal requirement that any "contract" have a term. For example, "This Use Agreement is effective as of the date noted with the signature until the user terminates association with XYZ Company."

#### 5.5.3 Policy Document Reference †

Where are the policies? For example, "XYZ Company policies are available to the user in electronic form on *http://www.xyz.com/policy* and in printed form in room 222. The policies are amended periodically. This use agreement applies to each current version of the policies. Each user will be notified by email when the policies have been revised."

#### 5.5.4 User Responsibility †

What do you expect of the user? For example, "The undersigned agrees to become familiar with and comply with each current revision of XYZ Company policies."

# 6.0 Suggested Reading and Other Resources

This booklet is not the last word on site policies. There are several other sources of information to assist you in compiling and developing your policies. The information sources referenced here are broken down into archives and specific articles, papers, or books. All electronic references are in uniform resource locator (URL) format. An electronic location is provided for each specific citation if one exists.

## Archives & Directories

**Ethics Policies:** policies from university sites which primarily address ethics and sometimes copyright and access.
*ftp://coast.cs.purdue.edu/pub/doc/law+ethics/University-Policies*

**COAST Security Archive:** archive of security related information which includes some links to documents about policies and the law. *http://www.cs.purdue.edu/coast/archive*

**IETF Internet Drafts:** recent relevant works-in-progress here include an update to the Site Security Handbook and a catalog of Internet training material.
*http://www.internic.net/ds/dsintdrafts.html*

**SAGE Policy Archive:** policy documents developed using this Guide.
*http://www.usenix.org/sage/hypertext/policies*

*State of Oregon v. Randal Schwartz.* Documentation on this case is maintained by the Friends of Randal Schwartz.
*http::://www.lightlink.com/fors*

## Articles, Papers & Books

D. B. Chapman & E. D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates, Inc., 1995, pp. 377–392.

S. Hambridge & J. C. Sedayao, "Horses and Barn Doors: Evolution of Corporate Guidelines for Internet Usage," *USENIX LISA VII*, 1993. *ftp://coast.cs.purdue.edu/pub/doc/institutional_policies/horses.ps.Z.*

S. E. Hanson, *Legal Issues: A Site Manager's Nightmare*, Stanford University, 1993. *ftp://coast.cs.purdue.edu/pub/doc/law+ethics/legal_issues_site_managers_nightmare.txt.Z*

P. Holbrook, J. Reynolds, *RFC1244: Site Security Handbook, Internet* IETF, 1991. *ftp://ds.internic.net/rfc/rfc1244.txt.*

E. Nemeth, et al, *UNIX System Administration Handbook*, 2nd ed., Prentice-Hall, 1995, pp. 722–750.

# 7.0 Sample Documents

Here are a few sample documents. Note that we are not calling them "model" documents: these are simply examples of the kind of policies in use today. You may find some to your liking, others not. Some policies are clear and useful, others are not. We have made the policies anonymous by removing any identifying elements (in some cases indicated by elisions), and we have tried to normalize spelling, punctuation, and grammar. In a few cases, however, we have left things just as they are: if you are confused by some policy listed here, think how the users at that particular site must feel! We have included a city document, two corporate documents (one short, one long) and a university document.

A Web site collection of policies written using this Guide is available at *http://www.usenix.org/sage/hypertext/policies/*. If your policy is not a secret, email it to Barb Dijker (*barb@usenix.org*) for inclusion. All document references to your organization will be deleted if requested or a dynamic link to your policy will be used if provided.

## 7.1 A document issued by a City.

This document details staff Internet usage policies and procedures established by the City's Information Services department. The City operates the computer systems collectively known as the domain [. . .] – currently operating through [. . .] and [. . .]. In addition, these policies pertain to any connection made by staff to any equipment, terminal server, router or bridge owned or operated by the City and con-

nected physically or logically to the public telephone network or through private connection to the collection of networks commonly know as the Internet.

These systems are maintained and offered for use to staff in the employ of the City. These policies pertain to ALL City staff activities whether through interactive or machine-machine connection. In general, City staff granted an Internet account are given access to the facilities and programs available through normal command use from the standard UNIX shell prompts and/or through use of client programs on the user's own or City owned computers when connected through the City's network access facilities, subject to the provision that they not deliberately cause problems with the use of the system by others.

Specific prohibitions are detailed later in this document, but include such things as:

- Deliberately crashing the system
- Deliberately using large amounts of system resources
- Trying to break any security feature/setting
- Copying Copyright software without vendor license
- Using system resources to attack any other system in any way
- Any activities which may be illegal under [local law].

## Definitions

### Internet Account.

Provided on the basis of one account to one staff member. Staff will be provided a unique user-id/account-id. Each staff member using the Internet must have a separate account. Staff may not share an account.

### Passwords.

Each account-id will be safeguarded through the use of a unique password that will be assigned to each staff member's account(s). Only the employee will be made aware of this password. This password must be kept secret and the employee should change it periodically.

**Logging in**

Internet Client software, when installed on one's PC, inserts a startup Icon in Windows. This Icon invokes a network startup and login script. Passwords should not be hard coded into this script. This login is used to establish the network connection and, as such, is the one which will be charged with the hours used.

E-mail requires logging-in again with the provision of an account-id and password through the mail reader. This protects your mail.

**Account Usage**

Accounts, in general, are not charged for. However, usage charges may be pro-actively applied, if it has been found that the account is primarily being used for non-City related business. Regardless of who pays the bill for an account, the information and mail it contains is considered the property of the registered USER of the account, and the account may not be passed on to any other.

**Software**

Machine (UUCP/SLIP/TCP-IP/Etc.). Client Software, such as Internet in a Box, will be provided for each computer accessing the Internet.

**Postmaster**

The City will maintain at least one mail account. This account, named "postmaster," which may be addressed by client computers, will be monitored periodically for account status and information.

**News Groups**

Certain facilities of the system, notably certain news groups may be governed by either strict usage guidelines or, as in the case of the XYZ news groups, site license restrictions. The following details the Rights and Responsibilities of the City and their Information Services support staff. These Rights and Responsibilities are subject to change without notice.

It is the City's premise that continued use of an account with the City is a privilege, not a right. Internet services may be purchased from others. Information Services will try to make your use of these services as easy, productive and cost effective as possible, however in order to do so, we must enforce a high degree of user responsibility and cooperation in keeping it a premium service.

**The City's Rights**

The City retains the right to prohibit access to our computer systems and communication services at any time for any reason. If access is permanently denied, the City may provide machine readable copy of the staff member's home directory and mail files. A reasonable fee consistent with hourly consulting rates in the computer industry may be applied for this labor.

The City retains the right to prohibit access to certain newsgroups, forums, chat services, web pages, etc.

The City retains ownership of all commercial software purchased by the City for use by staff on the system, and may remove such software at any time.

The City retains the right to substitute hardware and operating software as it sees fit, but will endeavor to maintain a consistent City staff interface and working software set.

The City retains the right to monitor Internet usage to capture usage statistics. Staff usage statistics (similar in nature to the City's departmental long distance phone reports) will be provided to the Directors which will detail staff usage.

**The City's Responsibilities**

The City is responsible for providing staff with a consistent set of tools and resources.

The City will endeavor to make available a full Internet News feed subject to applicable laws regarding minors and access to adult oriented news groups, along with facilities for interactive reading/response and batch pass through.

The City will endeavor to pass Electronic mail in a timely and consistent fashion from/to staff and their addressees.

The City will not knowingly release the contents of mail except to the addressed user unless required by court order. The City will not view or log the contents of mail except as required to deliver it or forward it to the next delivery agent in its path. In any case, viewing and/or logging of mail will be limited to the header lines conforming to the Simple Network Mail Protocol up to the first blank line, and/or the last six lines regardless of content.

The City provides information and/or programs "as is." The City is not responsible for the fitness or correctness of the information or programs in its systems, or any system connected by whatever means to City's systems.

The City, through its Internet providers, will maintain some information such as the XYZ news groups under agreement that they are for direct on-line reading only. The XYZ news groups are covered by copyright and users are not allowed to redistribute them to others, use them on radio or television, or cause them to be printed in media such as newspapers, magazines, or newsletters.

**City Staff Rights**

City staff has the right to private correspondence via Electronic Mail. City staff have the right to private storage of work related information in their home directories, subject only to size limitations unless prior authorization has been obtained from Information Services.

City staff must assume any and all liability, if they download to their media any public domain software and information contained on or available for retrieval through the Internet. Public domain software, freeware, shareware etc. may not be free. In most instances these products are copyright and a fee is imposed by their creator for corporate use. In situations, where downloaded software is required for corporate use, a Purchase Requisition must be completed and submitted to Purchasing for approval and the ensuing lawful acqui-

sition of the product. If approval is denied, the software and/or any materials downloaded must be deleted from any and all PCs that it has been installed upon.

Staff are responsible for any materials, graphics, databases, and files downloaded from the Internet. Care should be taken to insure these are being acquired for business use.

**City Staff Responsibilities**

Staff are responsible for backing up critical information downloaded to reside on their PC's hard drive and/or any which may reside on their home directories if located at the Internet Provider's site. The Internet Provider does perform periodic backups, but staff should not rely on there being a backup maintained for lengthy periods. Information Services does full system backups of any and all information and files located on its servers.

City staff are responsible to make use of such security measures as are available to limit access to their private information or correspondence stored on their home or office PC. Home directory permissions by default allow others to read and list a hard drives contents.

City staff are responsible for maintaining the security of their assigned account(s) on the system. A login name is public knowledge. However, the password associated with the login name is privileged, and should not be published or given to any other. If a City staff member knows or feels that their password has been compromised, he or she should immediately change their password. City staff should avoid the use of trivial passwords. A City staff member must change his or her password if requested by Information Services for any reason.

Staff are responsible for all activity on the system performed under their login unless the staff member informs Information Services of any breach of security in a timely fashion.

Staff are responsible for paying for all services and charges incurred under their account that have not been agreed

upon or granted under the terms and conditions of usage set out by the Purchasing Agent and Information Services. No services or charges may be indebted to the City without first pre-authorization from the Purchasing Agent. Failure to do so, will result in immediate suspension of the account until the balance has been paid. Account restoration will be solely at the discretion of Personnel. Additionally, at the discretion of the Personnel, further disciplinary or legal action may be undertaken.

**System Security Aims**

The City aims to provide privacy for its staffs' mail and home directory contents. In addition, the City aims to control and prohibit any security breach from within the system, or from outside via the Internet connection.

**Security Policies and Procedures**

The security on any multi-user system is based upon the premise that the user is responsible for all activity run from the user's account/login. This requires that there be a policy limiting each account to the use of a single person. In addition, batch accounts which pass mail and/or commands to the system have a similar policy.

Accounts which are used by more than one user will be subject to suspension of service.

Batch accounts which exhibit multiple use of internal accounts will be warned that such a policy is not in keeping with a secure site. If any account exhibits problem behavior, the batch account will be terminated until it can be determined that the One-user/account policy has been implemented, and the problem user has been dealt with appropriately.

The first line of defense on a public system is the account password. The City enforces a policy of requiring a password on all accounts used for general access. The adequacy of account passwords will be tested from time to time using similar techniques to those used by system crackers.

Accounts whose passwords are found using these techniques will be warned to change their password immediately to one conforming to the password guidelines. Accounts which consistently fail this audit will have a random password generated for them.

Passwords will NEVER be provided via email over the Internet. If you require a new password or account, please call Information Services or email us a phone number where you can be reached at a particular time.

Having established that the owner of the account is the only one that is allowed to use the account, it follows that anything done in the name of the account is the responsibility of the account holder.

**Signature File**

All staff must include the following disclaimer within their Signature File. Information Services will set this up for staff. The following signature will be automatically appended to any and all Newsgroup postings and/or Electronic Mail created under a City Internet account:

The contents of this posting or electronic mail message are solely the writings, thoughts and/or ideas of the account holder and may not necessarily reflect those of the City.

If you have any concerns regarding the inappropriate use of this account. Please email to [. . .].

**Sensitive Information**

Information Services maintains logs of system activity which show "who did what, when." Beyond this, City staff activity is not monitored – i.e., the fact that a staff member ran a particular program at a time, for a time, is tracked. What the staff member entered into or read from the program is not tracked. This information is used to compile the monthly usage reports to City managers, and in cases of policy breach, to track violations. These logs are rarely looked at by Information Services staff, but rather are summarized and tracked for gross violations by computer scripts. These

reports will be retained for audit purposes for a y
determined period of time.

City staff may not maintain sensitive information on the Internet Provider's system. It should be noted that those systems are not configured for more than "traditional" UNIX security, and so has no certification or security classification. The City's Internet Providers endeavor to track and stop any security attacks, however this is done in the interests of keeping the system available for use, rather than in the interests of protecting information stored. This reflects the reality that this Internet system is connected to a publicly accessible network which has been proven to be insecure.

The City, through its Internet Providers, is doing its part to elevate the security of the Internet by monitoring for and, if necessary, prosecuting the perpetrators of cases of security violation.

**Prohibited Activities**

- Crashing the system (i.e., running "crash" or any similar program) It is noted that systems crash sometimes, and that a user may not recognize that they have caused such a crash. In cases such as this, if the user's actions are traced as the cause of the crash and the user is notified of such, any repeat of the circumstances will be taken as a "deliberate" crash and dealt with accordingly.
- Using inordinate amounts of system resources without first notifying Information Services (Deliberately running the system out of disk space or hogging CPU cycles/network bandwidth/etc.). Exceptions may be allowed at the discretion of Information Services.
- Trying to break any security features implemented by Information Services (Includes running any password cracking programs, viruses, Trojan horses, sniffers etc. as well as trying to circumvent file permissions both on these systems, and on systems connected via any network connection). Research into these types of activities are specifically prohibited.

- Copying of Copyright software from the City's or connected systems without explicit license from the owners of such software Many institutions make their income by writing and selling commercial software, and we will not condone the actions of those who would steal software.
- Distributing to outside parties, electronically or via any media, the City's corporate data files, databases of information, software, and/or other electronic files considered the property of the City. Permission to do so must firstly be obtained from the departmental manger and Information Services.
- Using the system as the base for an attack of any type on other systems. This includes continued harassment of individuals by Electronic Mail. Additionally, this includes Spamming numerous newsgroups and/or the posting of inappropriate Mail (e.g., Hate Mail, Libellous items, etc.).
- Creating any mail or network commands with false or anonymous origination information. This is in keeping with our policy of enforcing user accountability for all traffic on the system.
- Any activity which is prohibited by law in [locality]. In addition, since this system is connected to computers in virtually every jurisdiction in the world, the City will take action against any account holder using the system as a base to break the laws of another jurisdiction via a computer in that jurisdiction.
- Any activity which contravenes the spirit of the Internet as a cooperative environment. This last prohibition is of necessity very vague since there is no one governing body or set of governing rules for the Internet. In essence, the prohibition covers any act to which anyone even indirectly affected by such acts can say "This is not why I have been granted my network connection for." This covers such things as not contravening "Acceptable Usage Policies" and not sending out "broadcast" unsolicited email messages and not trying to force your moral/ethical/religious/etc. standards on any other net user. In general, if the staff member's actions cause any reaction from others on the Internet to an extent that draws attention from the City's Council,

Directors and/or Information Services, continued access via the City's facilities may/will be revoked. If the staff member does not understand this last policy prohibition, then that staff member should NEVER! send anything via email or Usenet News, or use any facility other than direct interactive READING of information from anywhere on the Internet.

**Response to Policy Violations:**
The City will, depending on the nature of the violation, respond by any of:

- Denial of service for a period
- Denial of service permanently
- Provision of information to Police Authorities
- Filing of complaints to Police Authorities
- Filing of Civil Suits
- Any other action deemed necessary by Personnel up to and including dismissal

**Appeals**
Appeals to actions taken by Information Services of the City may be made in writing to Personnel.

**Problem Reporting Procedures**
Email to: [. . .] or call Client Services at [. . . ].

Detail the problem and provide examples – from captured online sessions if possible – or real log file entries. If possible, explain what you feel is the required solution.

## 7.2 A-site Computer Security Policy

["A-site" is a pseudonym. The policy is interesting for its brevity.]

A-site is responsible for assuring the integrity of its computing systems. Ultimately, however, the integrity of shared computing resources depends on responsible behavior on the part of the users of these systems.

The purpose of this policy is to ensure that all computing and network users understand their responsibilities to safeguard the access privileges granted to them.

Every user of A-site's computer/communications/information systems is expected to know their obligatory requirements for protecting technology and information assets and to follow this policy.

### General Use

A-site's computer/communications/information systems are for A-site business use only.

Computing systems facilitate manipulation and sharing of data and information. These systems and facilities can be used in similar fashion to traditional mail and telephone services. In all informational exchanges, A-site employees are responsible for using these facilities in an effective, ethical and lawful manner.

### Access Policy

Anyone given access to the system is accountable for its use. It is the user's responsibility to protect the integrity of accessible systems and preserve the confidentiality of accessible information as appropriate. In particular, users shall not share with others the access codes, account numbers, passwords or other authorization which have been assigned to them.

Unauthorized electronic access is prohibited.

### Privacy Policy

Users have a right to a reasonable expectation of privacy. However, system failures or design faults may compromise this privacy and users should also recognize that authorized A-site personnel may have access to data and software stored on A-site systems.

### Accountability Policy

Anyone who has reason to suspect a breach of established security policy or procedure should promptly report it to [their management].

### Policy Enforcement

A-site regards any violation of this policy as a serious offense. Violators of this policy are subject to disciplinary action as well prosecution under the terms of applicable laws.

All personnel must sign a statement indicating that they have read, understood, and agree to abide by the policy.

### Supported services

At this time, A-site computer security policy supports the following outbound network services:

- ftp
- telnet
- http browser
- smtp

and the following inbound network services:

- ftp (to external net-based server)
- smtp (to external net-based server)

It should be noted that all receipt of data, regardless of the method used to obtain it (smtp, ftp, http, etc.), onto the local network should be considered a possible security concern. Users are cautioned to use appropriate measures when initiating such a transfer of data.

## 7.3 Big Company Policy

### Introduction

The Big Company (BC) staff develops controls and operates the BC computer center. The computer center was implemented in direct support of the research and engineering efforts at BC. The center consists primarily of but is not limited to Sun Microsystems fileservers and workstations. Other equipment includes DEC Microvaxes and workstations, Xterminals, printers, plotters, and a multitude of other peripherals. The BC network itself uses ethernet running the TCP/IP protocol and consists of three distinct local area networks. These networks interconnect directly to two other

campuses located in [. . .] via dedicated T-1 phone lines. BC currently operates many local area networks. The three primary campuses are also connected to Sales offices, design centers, and overseas facilities. The BC center also has access to the Internet and USENET.

The policy presented here applies to all computer systems of the Center, regardless of their manufacture or operating system. As used in this policy statement, the term "users" refers to any person consuming resources of the Center (e.g., CPU cycles, printer paper, toner, etc.). The term "Center" refers to the UNIX computing and associated facilities assigned by R&D [and others] to Center Staff for operation and maintenance. The term "Center Staff" refers to the group of Center employees who work in the area of basic software system support, hardware maintenance, operations, and user support.

## General

The Center makes available computing facilities consisting of hardware, software, and documentation. The use and operation of these facilities is subject to the following:

The Center is the property of BC, including but not limited to computers, software, magnet media, printers, and plotters. All work created by the use of Center resources is the property of BC. All data on the Center, including but not limited to software, and administrative files is the property of BC. All communications originating from or received by the Center are the property of BC.

The Center Staff makes every effort to prevent the loss of data in the event of hardware or software failure or human error. This is done by making daily, incremental backups of the filesystems to tape. An attempt is made to limit potential loss to at most one day's work.

In order to adequately protect the proprietary information contained within the Center, deviations to the "operational practices" outlined in this policy will not be permitted.

The following policies and procedures supersede this document in overlapping areas: [list of two corporate documents].

**Authorized Access**

Access to the Center is restricted and monitored. Authorized access is granted by applying for an account from the Center staff.

Computer facilities and accounts are owned by BC and are to be used for company business only. Access to fileservers, computers, servers, and workstations is regulated and monitored by the Center staff group.

Individuals may only access accounts to which they have been authorized. Furthermore, individuals will not authorize anyone else to have access or use their Center account.

To minimize the probability of compromise or disruption of Center operations, Center users will immediately report to the Center staff any suspected instance of ``unauthorized access'' to their accounts (i.e., files missing or changed, or someone else logging into their account).

The only acceptable method of gaining telephone access to the Center is through a [special procedure]. Call the Center help desk to request the procedure and be trained in using it.

**System User Responsibilities**

A user of the Center's Network has the following responsibilities.

Each user is responsible for any and all activity initiated in or on Center facilities by his or her account.

Users are responsible for protecting their access passwords by:

- Using a mixture of 7 or 8 upper and lower case letters and nonalphabetic characters in the password and changing the password every 30 to 60 days via the *passwd* command. Passwords should be easily remembered.
- Refraining from creating passwords using: "login names," first, middle, or last names; nicknames; names of family members, friends or pets; words that can be found in word

lists (i.e., dictionaries, spelling lists, etc.); information unique to the user and still easily obtained (i.e., license, telephone, or address numbers); all digits; or all the same letter.

- Refraining from giving out the password to any; storing or embedding the password on the computer system; recording the password anywhere but in the user's memory.

Users are responsible for protecting their own files and data from reading and/or writing by other users.

The ability to read another user's files does not implicitly grant permission to read those files.

Under no circumstances may a user alter a file that does not belong to him or her without prior permission of the file's owner. The ability to alter another user's files does not implicitly grant permission to alter those files.

Users are responsible for reporting any system security violation, or suspect violation, to Center staff immediately.

If a user sees a system that a co-worker has left unattended and is logged in, the user should [lock] the system and leave a brief note on the system stating what they did.

Terminals logged in to the Center will not be left unattended or unprotected. If a terminal must be left unattended, the user is responsible for terminating the session by logging off or [lock]ing the system to protect the session.

Note: [lock] programs or any application designed to block the access of a workstation that have excessive run times or [block] access to a public workstation may be subject to termination by Center Staff, either through manual intervention or automatic programs. This may result in possible loss of data.

Whenever a process (job) is expected to require excessive resources, the user is responsible for notifying Center Staff to avoid inadvertent process termination.

Users are responsible for reporting damaged equipment to Center Staff immediately upon discovery.

Users who borrow hardware, software, or documentation from Center lending collections are responsible for their proper care and returning them in a timely fashion.

Users are responsible for adhering to all official notices released via mail, email, attached to Center equipment, or displayed in the login message of the day.

Users are responsible for the proper maintenance of the files in their account and in any directories that they use for temporary storage.

At all times, users are responsible for using Center facilities in a manner that is ethical, legal, and not detrimental to other users or to other users of to BC.

**System Staff Rights and Responsibilities**

The Center Staff generally may do whatever is necessary to carry out its responsibility to maintain effective and secure operation of the Center facilities and the ownership of information by BC.

The Center Staff has the responsibility to make every reasonable effort to maintain the privacy of a user's files, electronic mail, and printing listing.

In the normal course of examining and repairing system problems, and when investigating possible instances of improper use of Center facilities, the Center Staff may need to examine user's files, electronic mail, and printer listings, as they relate to the system problem being worked on. The Center Staff has the right to do this, subject to the previous paragraph.

In order to protect data against hardware and software failures, Center Staff is responsible for backing up all data stored in the Center on a regular basis.

The Center Staff has the right to monitor any and all aspects of a system.

The Center Staff has the right to alter the priority or terminate the execution of any process that is abnormally consuming excessive system resources or objectionably degrading system response, with or without prior notification to the user. The Center Staff will make every effort to inform the owner of the process (via direct phone, pager, or personal contact) prior to taking action.

The Center Staff has the right to remove files that are automatically generated by programs and take up large amounts of diskspace such as *core* or FrameMaker ".backup" files.

The Center Staff has the right to terminate login sessions that have been idle for long periods of time or unattended sessions, or in order to free resources. The definition of a "long period" of time may vary from system to system, depending upon resource availability.

The Center Staff has the responsibility to provide advance notice of system shutdowns for maintenance, upgrades, or changes so that users may plan around periods of system unavailability. However, in the evening of an emergency, the Center Staff has the right to shut down a system with little or not advance notification. Every effort will be made to give users a chance to save their work before the system is shut down.

Staff members have the responsibility to report any violations of Center policy, BC policy, or [local] law pertaining to the use of Center facilities to the appropriate authorities whenever such violations come to their attention.

The Center Staff has the responsibility to document infractions of this policy by any persons for subsequent management determination as to whether Center access should be denied or restricted.

**Proper Use**

The Center facilities are provided for the use of employees of BC. All employees using the Center facilities are responsible for using these facilities in an effective, ethical, and lawful manner.

To maximize effective use of shared resources (i.e., disk space, CPU cycles, printers, and software licenses), all users are prohibited from monopolizing these resources and are encouraged to make use of as little disk space as possible. This is accomplished through file compression and archiving and removing files that are no longer needed.

Users should not execute software that they have not been trained in or that they have no idea of what the software does or how the software works. Doing so may result in the loss of data or seriously impact computer performance.

To assure only authorized software is executed on the Center [resources] and to protect the integrity of the network, the Center Staff must approve all software prior to loading it onto the system.

Users are expected to relinquish [use of] licensed software when no longer using it, [thus allowing] other users to maximize effective use of the limited number of licenses purchased.

Center users are specifically prohibited from researching or attempting to defeat network security measures, implementing self-replicating codes, possessing "cracker tools," as well as intentionally developing and or using programs that are designed to:

- Harass other system users
- Bypass system security mechanisms, steal or "crack" passwords or data sets.
- Attempt to consume all of an available system resource (memory, swap space, disk space, network bandwidth, etc.) with the exception of approved lock programs.
- Replicate themselves or attach themselves to other programs (i.e., worms, viruses, trojan horses, etc.)
- Evade software licensing or copying restrictions.

### Copyrights and Licenses

All software used on the Center facilities is operated under legitimate license agreements with the companies that either

originated or legally possess licensing authority for that software.

[Local] copyright and patent laws protect the interests of authors, inventors, and software developers in their products. Software license agreements serve to increase compliance with copyright and patent laws. It is against [. . .] law and BC policy to violate the copyrights or patents on computer software or to violate the software license agreements.

Software in use on Center facilities, unless it is stored in areas specifically defined as containing copyable software, may not be copied to magnet tape, hard or floppy disks, or otherwise removed from Center Facilities. Backup copies of licensed software are maintained by the Center staff; users may not make copies of licensed software.

**Internet Access**

Access to Internet is restricted to an as-needed basis.

**Enforcement**

Following thorough investigation, situations contrary to directives set forth in this document will be addressed in accordance with applicable BC Policies and Procedures, and may include management action up to and including termination. Minor infractions may be handled informally while "serious infractions" will be dealt with formally.

Minor (usually accidental) infractions (i.e., poorly chosen passwords, overloading systems, excessive disk space consumption, etc.) will normally be handled informally via electronic mail in person discussions with members of the Center Staff.

Intentional infractions (i.e., sharing accounts or passwords, harassment, repeated minor infractions, etc.) may result in the temporary loss or modification of Center access privileges, and formal notification of the employee's supervisor and/or department manager for applicable corrective action.

Intentional serious infractions (i.e., unauthorized use; attempts to steal passwords, data, or licensed software; viola-

tions of BC policies; repeated instances of "intentional infractions," etc.) will definitely result in permanent loss of Center access privileges, and will involve corrective action as deemed appropriate by the employee's management.

## 7.4 University Computer Use Policy

ABC University provides and maintains computing and telecommunications technologies to support the education, research and work of its faculty, staff, and students. ABC's computing and telecommunications technologies are collectively referred to as ABCnet. By connecting thousands of computers at ABC with each other and with national and international computer networks, ABCnet provides many educational benefits.

The purpose of this policy is to define responsible and ethical behavior of ABCnet users in order to preserve the health, availability, and integrity of ABCnet resources. This policy is purposely silent on matters covered by other policies such as sexual harassment and honor code violations, and by federal and state laws on privacy and computer abuse. This policy applies to all users of ABCnet resources.

The priorities for use of ABCnet resources are:

- HIGHEST: All education, research, and administrative purposes of ABC.
- MEDIUM: Other uses indirectly related to ABC purposes with education or research benefit, including personal communications.
- LOWEST: Recreation, including game-playing.
- FORBIDDEN: Selling ABC resources, commercial activities not sanctioned by the Provost's office, intentionally denying or interfering with service, unauthorized use or access, reading or modifying files without proper authorization, using the technology to impersonate another, violations of laws or other ABC policies.

Because it is impossible to anticipate all the ways in which individuals can harm or misuse ABCnet facilities, this policy

focuses on a few simple rules. These rules generally indicate actions that should be avoided.

If you observe someone violating this policy, or another ABC policy using ABCnet resources, you can report it by email to [. . .].

## Rules of use

ABC treats access to ABCnet resources as a privilege that is granted on a presumption that every member of the university community will exercise it responsibly. The following rules are not complete – just because an action is not explicitly proscribed does not necessarily mean that it is acceptable. You should read these rules for the principles behind them and stick to the principles.

### Use ABCnet Consistently With the Stated Priorities

The low priority uses of ABCnet should be avoided during the times of peak demand, typically the mid afternoon to late evening hours. During peak periods, other users may be prevented from doing their high priority work if you are doing something of low priority. Those users are likely to complain to you or to [. . . ] if they observe you interfering with their work.

Certain activities such as chain letters or broadcast email to very large distributions will consume large amounts of resources; avoid them.

### Don't Allow Anyone to Use Your Account for Illegitimate Purposes

Your ABCnet username identifies you to the entire international Internet user community. Another person using your account, whether or not you have given permission, will be acting in your name. Anyone who knows your password can use your account. You are responsible for that person's actions in your account. If that person violates any policies, his or her actions will be traced back to your username and you may be held responsible. The easiest way to protect yourself is to not give away your password. If you need to

give someone access, give it on a temporary basis, and change your password after that person finishes using your account. You should also not give your password to anyone you do not trust.

If someone else offers you use of an account for which you are not authorized, decline. If you discover someone's password, don't use it; report the access to the password to the owner or to <stopit>.

**Honor the Privacy of Other Users**

ABC treats the contents of all files, email, and communications as private, and will strive to protect the privacy of all users. Many aspects of privacy of files and communications are also protected by [local] laws. Examples:

- Don't access the files or directories of another user without explicit authorization from that user. Typically, authorization is signalled by the other user's setting file access permissions to allow public or group reading of files. Since some systems by default make all files readable to all users and some users don't know this, the file permissions are not reliable. It is always best to ask.
- Don't intercept or monitor any network communications not explicitly meant for you.
- Don't use the systems or transmit personal or private information about individuals unless you have explicit authorization from the individuals affected. Don't distribute such information unless you have permission from those individuals.
- Don't create programs that secretly collect information about users. Software on ABCnet is subject to the same guidelines for protecting privacy as any other information-gathering project at ABC. You may not user ABC computer and telecommunication systems to collect information about individual users without their consent. Note that some system utilities log user information (ftp, mosaic, login, etc.). This is considered normal system administration functions.

**Don't Impersonate Any Other Person.**

Using ABCnet resources to impersonate someone else is improper. If you use someone else's account, you may be committing acts of fraud because the account owner's name will be attached to the transactions you have performed.

If you send anonymous mail or postings, you should realize that it is customarily considered polite to identify that your message is anonymous or is signed by pseudonym. You should be aware that most people will give less credence to anonymous communication than to signed communication.

**Don't Use ABCnet To Violate Other Policies or Laws.**

Computer networks offer new ways to commit actions that violate laws or policies that are covered elsewhere. Here are reminders of typical other policies:

- Don't copy copyrighted documents. Many programs and their documentation are owned by individual users or third parties and are protected by copyright and other laws, licenses, and contractual agreements. You must abide by these restrictions; to do otherwise may be a crime.
- Don't use ABCnet to threaten or harass anyone. Various types of harassment, including sexual or racial, are proscribed by ABC policies.
- Don't use ABCnet to violate the Honor Code.
- Don't use ABCnet to launch viruses, worms, trojan horses, or other attacks on computers here or elsewhere.

## Schools, Institutes, Centers, and Departments

Organizational units on the campus operate computers and networks to support their missions. The principles of this policy apply to all ABC organizational units, and any computers connected to ABCnet. Units may set additional local policies and expectations that are consistent with this policy.

## Privacy

All users of ABCnet enjoy a right of privacy. No other user, system administrator, or official may read email, files, or communications without the consent of their owners.

Only in rare and exceptional cases where a severe threat is present and there is no alternative to ameliorating the threat may the Security Review Panel authorize the reading of email, files, or communications. No system administrator or official may do this without the authorization of the Panel.

**System Administrators (SAs)**

The system administrators of various computers around campus have special responsibilities. They should exercise their extraordinary powers to override or alter access controls, accounts, configurations, and passwords with great care and integrity. SAs manage computers and administrate policies, but they do not create policies. Their actions are constrained by this policy and by the policies of local administrative units. In particular, local units should set policies concerning accounts on their machines, and SAs must follow these policies.

[. . .} maintains a set of guidelines and standards for all SAs and will offer help for new SAs. Managers of ABC units who employ SAs are responsible for ensuring that the SAs comply with and enforce the requirements of this policy in the systems for which they are responsible. SAs who violate this policy or any local policy, or who misuse their powers, will face disciplinary action.

If an SA observes someone engaging in activities that would seriously compromise the health or integrity of a system or network – e.g., someone launching a virus attack or attempting to gain root access – the SA may take immediate action to stop the threat or minimize damage. This may include termination of processes, disconnection from a network, or temporary suspension of an account. Account suspensions must be reported immediately to the Security Review Panel. Only in exceptional cases, authorized by the Security Review Panel (described below) as part of an investigation, may personal files or communications be inspected without the knowledge of the owner. Thus, SAs may not read email, files, or communications as part of an investigation without explicit authorization from the Security Review Panel.

**Security Review Panel (SRP)**

This policy establishes a Security Review Panel consisting of three faculty members, two student members, one non-[. . .] system administrator, and one [. . .] staff member. Its chair will be one of the faculty members and will be appointed by the Provost. SAs will report all violations and their responses to this panel immediately. Any member of the community can report a violation to the panel via [. . .]. On receipt of a complaint from a user or an SA, the panel chair will assign one of the members as the panel's "case worker" for that complaint. The process within which the panel operates is described in a companion document.

If a user's account is disabled as a result of a suspected violation, the user has a right to a resolution and reactivation of the account in the case of a mistake within 2 working days.

The panel is also responsible for reviewing these policies periodically and recommending improvements and clarifications as needed.

## About the Series

This is the second in a series of booklets that SAGE is presenting to the system administration community. They are intended to fill a void in the current information structure, presenting topics in a thorough, refereed fashion, but staying small enough and flexible enough to grow with the community. Therefore, these booklets will be "living documents" that are updated as needed.

#1: Job Descriptions for System Administrators
Edited by Tina Darmohray

#2: A Guide to Developing Computing Policy Documents
Edited by Barbara L. Dijker

## About SAGE and USENIX

SAGE, The System Administrators Guild answers the widely felt need for an organization dedicated to advancing the profession of systems administration. SAGE brings together system administrators to:

- recruit talented individuals to the profession,
- share technical problems and solutions,
- establish standards of professional excellence while providing recognition for those who attain them,
- promote work that advances the state-of-the-art or propagates knowledge of good practice in the profession

USENIX is the UNIX and advanced computing systems technical and professional association.

The USENIX Association and its members are dedicated to:

- problem-solving with a practical bias,
- fostering innovation and research that works,
- communicating rapidly the results of both research and innovation,
- providing a neutral forum for the exercise of critical thought and the airing of technical issues.

## About the Editor

Barbara L. Dijker (*barb@usenix.org*) is a consultant with her own business, Labyrinth Computer Services. She is co-founder and Excutive Director of the Colorado Internet Cooperative Association as well as NeTrack, a commercial Internet Service Provider. Barb also serves as treasurer on the SAGE Board and is saver of USENIX faces.