4.6. Example: Academic Computer Security Policy

Security policies can have few details, or many. The explicitness of a security policy depends on the environment in which it exists. A research lab or office environment may have an unwritten policy. A bank needs a very explicit policy. In practice, policies begin as generic statements of constraints on the members of the organization. These statements are derived from an analysis of threats, as described in Chapter 1, "An Overview of Computer Security." As questions (or incidents) arise, the policy is refined to cover specifics. As an example, we present an academic security policy. The full policy is presented in Chapter 35, "Example Academic Security Policy."

4.6.1. General University Policy

This policy is an "Acceptable Use Policy" (AUP) for the Davis campus of the University of California. Because computing services vary from campus unit to campus unit, the policy does not dictate how the specific resources can be used. Instead, it presents generic constraints that the individual units can tighten.

The policy first presents the goals of campus computing: to provide access to resources and to allow the users to communicate with others throughout the world. It then states the responsibilities associated with the privilege of using campus computers. All users must "respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations."[1]

[1] See Section 35.2.1.2.

The policy states the intent underlying the rules, and notes that the system managers and users must abide by the law (for example, "Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws").[2]

[2] See Section 35.2.1.2.

The enforcement mechanisms in this policy are procedural. For minor violations, either the unit itself resolves the problem (for example, by asking the offender not to do it again) or formal warnings are given. For more serious infractions, the administration may take stronger action such as denying access to campus computer systems. In very serious cases, the university may invoke disciplinary action. The Office of Student Judicial Affairs hears such cases and determines appropriate consequences.

The policy then enumerates specific examples of actions that are considered to be irresponsible use. Among these are illicitly monitoring others, spamming, and locating and exploiting security vulnerabilities. These are examples; they are not exhaustive. The policy concludes with references to other documents of interest.

This is a typical AUP. It is written informally and is aimed at the user community that is to abide by it. The electronic mail policy presents an interesting contrast to the AUP, probably because the AUP is for UC Davis only, and the electronic mail policy applies to all nine University of California campuses.

4.6.2. Electronic Mail Policy

The university has several auxiliary policies, which are subordinate to the general university policy. The electronic mail policy describes the constraints imposed on access to, and use of, electronic mail. It conforms to the general university policy but details additional constraints on both users and system administrators.

The electronic mail policy consists of three parts. The first is a short summary intended for the general user community, much as the AUP for UC Davis is intended for the general user community. The second part is the full policy for all university campuses and is written as precisely as possible. The last document describes how the Davis campus implements the general university electronic mail policy.

4.6.2.1. The Electronic Mail Policy Summary

The summary first warns users that their electronic mail is not private. It may be read accidentally, in the course of normal system maintenance, or in other ways stated in the full policy. It also warns users that electronic mail can be forged or altered as well as forwarded (and that forwarded messages may be altered). This section is interesting because policies rarely alert users to the threats they face; policies usually focus on the remedial techniques.

The next two sections are lists of what users should, and should not, do. They may be summarized as “think before you send; be courteous and respectful of others; and don't interfere with others' use of electronic mail.” They emphasize that supervisors have the right to examine employees' electronic mail that relates to the job. Surprisingly, the university does not ban personal use of electronic mail, probably in the recognition that enforcement would demoralize people and that the overhead of carrying personal mail is minimal in a university environment. The policy does require that users not use personal mail to such an extent that it interferes with their work or causes the university to incur extra expense.

Finally, the policy concludes with a statement about its application. In a private company, this would be unnecessary, but the University of California is a quasi-governmental institution and as such is bound to respect parts of the United States Constitution and the California Constitution that private companies are not bound to respect. Also, as an educational institution, the university takes the issues surrounding freedom of expression and inquiry very seriously. Would a visitor to campus be bound by these policies? The final section says yes. Would an employee of Lawrence Livermore National Laboratories, run for the Department of Energy by the University of California, also be bound by these policies? Here, the summary suggests that they would be, but whether the employees of the lab are Department of Energy employees or University of California employees could affect this. So we turn to the full policy.

4.6.2.2. The Full Policy

The full policy also begins with a description of the context of the policy, as well as its purpose and scope. The scope here is far more explicit than that in the summary. For example, the full policy does not apply to e-mail services of the Department of Energy laboratories run by the university, such as Lawrence Livermore National Laboratories. Moreover, this policy does not apply to printed copies of e-mail, because other university policies apply to such copies.

The general provisions follow. They state that e-mail services and infrastructure are university property, and that all who use them are expected to abide by the law and by university policies. Failure to do so may result in access to e-mail being revoked. The policy reiterates that the university will apply principles of academic freedom and freedom of speech in its handling of e-mail, and so will seek access to e-mail without the holder's permission only under extreme circumstances, which are enumerated, and only with the approval of a campus vice chancellor or a university vice president (essentially, the second ranking officer of a campus or of the university system). If this is infeasible, the e-mail may be read only as is needed to resolve the emergency, and then authorization must be secured after the fact.

The next section discusses legitimate and illegitimate use of the university's email. The policy allows anonymity to senders provided that it does not violate laws or other policies. It disallows using mail to interfere with others, such as by sending spam or letter bombs. It also expressly permits the use of university facilities for sending personal e-mail, provided that doing so does not interfere with university business; and it cautions that such personal e-mail may be treated as a "University record" subject to disclosure.

The discussion of security and confidentiality emphasizes that, although the university will not go out of its way to read e-mail, it can do so for legitimate business purposes and to keep e-mail service robust and reliable. The section on archiving and retention says that people may be able to recover e-mail from end systems where it may be archived as part of a regular backup.

The last three sections discuss the consequences of violations and direct the chancellor of each campus to develop procedures to implement the policy.

An interesting sidelight occurs in Appendix A, "Definitions." The definition of "E-mail" includes any computer records viewed with e-mail systems or services, and the "transactional information associated with such records [E-mail], such as headers, summaries, addresses, and addressees." This appears to encompass the network packets used to carry the e-mail from one host to another. This ambiguity illustrates the problem with policies. The language is imprecise. This motivates the use of more mathematical languages, such as DTEL, for specifying policies.

4.6.2.3. Implementation at UC Davis

This interpretation of the policy simply specifies those points delegated to the campus. Specifically, "incidental personal use" is not allowed if that personal use benefits a non-university organization, with a few specific exceptions enumerated in the policy. Then procedures for inspecting, monitoring, and disclosing the contents of email are given, as are appeal procedures. The section on backups states that the campus does not archive all e-mail, and even if e-mail is backed up incidental to usual backup practices, it need not be made available to the employee.

This interpretation adds campus-specific requirements and procedures to the university's policy. The local augmentation amplifies the system policy; it does not contradict it or limit it. Indeed, what would happen if the campus policy conflicted with the system's policy? In general, the higher (system-wide) policy would prevail. The advantage of leaving implementation to the campuses is that they can take into account local variations and customs, as well as any peculiarities in the way the administration and the Academic Senate govern that campus.