**Security Policy**

*What is a Security Policy and Why Have One?*

The security-related decisions you make, or fail to make, as administrator largely determines how secure or insecure your network is, how much functionality your network offers, and how easy your network is to use. However, you cannot make good decisions about security without first determining what your security goals are.

Until you determine what your security goals are, you cannot make effective use of any collection of security tools because you simply will not know what to check for and what restrictions to impose. For example, your goals will probably be very different from the goals of a product vendor. Vendors are trying to make configuration and operation of their products as simple as possible, which implies that the default configurations will often be as open (i.e., insecure) as possible.

While this does make it easier to install new products, it also leaves access to those systems, and other systems through them, open to any user who wanders by.

Your goals will be largely determined by the following key tradeoffs:

**1. services offered versus security provided -**

Each service offered to users carries its own security risks. For some services the risk outweighs the benefit of the service and the administrator may choose to eliminate the service rather

than try to secure it.

**2. ease of use versus security -**

The easiest system to use would allow access to any user and require no passwords; that is, there would be no security.

Requiring passwords makes the system a little less convenient, but more secure. Requiring device-generated one-time passwords makes the system even more difficult to use, but much more secure.

**3. cost of security versus risk of loss -**

There are many different costs to security: monetary (i.e., the cost of purchasing security hardware and software like firewalls and one-time password generators), performance (i.e., encryption and decryption take time), and ease of use (as mentioned above).

There are also many levels of risk: loss of privacy (i.e., the reading of information by unauthorized individuals), loss of data (i.e., the corruption or erasure of information), and the loss of service (e.g., the filling of data storage space, usage of computational resources, and denial of network access). Each type of cost must be weighed against each type of loss.

Your goals should be communicated to all users, operations staff, and managers through a set of security rules, called a "security policy." We are using this term, rather than the narrower "computer security policy" since the scope includes all types of information technology and the information stored and manipulated by the technology.

*Definition of a Security Policy*

A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

*Purposes of a Security Policy*

The main purpose of a security policy is to:

* Inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met.
* Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.
* Another major use of an AUP is to spell out, exactly, the corporate position on privacy issues and intellectual property issues. In some countries, if the company does not explicitly state that e-mail is not secure, it is considered to be so and any breach could cause privacy and confidentiality liabilities. It is very important to spell out what is and is not acceptable in intellectual transfers and storage and what the corporate privacy policies are to prevent litigation about same.
* An Appropriate Use Policy (AUP) may also be part of a security policy. It should spell out what users shall and shall not do on the various components of the system, including the type of traffic allowed on the networks.
* The AUP should be as explicit as possible to avoid ambiguity or misunderstanding. For example, an AUP might list any prohibited USENET newsgroups. (Note: Appropriate Use Policy is referred to as Acceptable Use Policy by some sites.)

*Who Should be Involved When Forming Policy?*

In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. It is especially important that corporate management fully support the security policy process otherwise there is little chance that they will have the intended impact. The following is a list of individuals who should be involved in the creation and review of security policy documents:

· site security administrator

· information technology technical staff (e.g., staff from computing center)

· administrators of large user groups within the organization (e.g., business divisions, computer science department within a university, etc.)

· security incident response team

· representatives of the user groups affected by the security policy

· responsible management

· legal counsel (if appropriate)

The list above is representative of many organizations, but is not necessarily comprehensive. The idea is to bring in representation from key stakeholders, management who have budget and policy authority, technical staff who know what can and cannot be supported, and legal counsel who know the legal ramifications of various policy choices. In some organizations, it may be appropriate to include EDP audit personnel. Involving this group is important if resulting policy statements are to reach the broadest possible acceptance. It is also relevant to mention that the role of legal counsel will also vary from country to country.

*What Makes a Good Security Policy?*

The characteristics of a good security policy are:

1. It must be implementable through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.

2. It must be enforceable with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.

3. It must clearly define the areas of responsibility for the users, administrators, and management.

**The components of a good security policy include:**

1. **Computer Technology Purchasing Guidelines** which specify required, or preferred, security features. These should supplement existing purchasing policies and guidelines.

2. **A Privacy Policy** which defines reasonable expectations of privacy regarding such issues as monitoring of electronic mail, logging of keystrokes, and access to users' files.

3**. An Access Policy** which defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to a network, and adding new software to systems. It should also specify any required notification messages (e.g., connect messages should provide warnings about authorized usage and line monitoring, and not simply say "Welcome").

4. **An Accountability** Policy which defines the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident handling guidelines

(i.e., what to do and who to contact if a possible intrusion is detected).

5. **An Authentication Policy** which establishes trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices (e.g., one-time passwords and the devices that generate them).

6. **An Availability statement** which sets users' expectations for the availability of resources. It should address redundancy and recovery issues, as well as specify operating hours and

maintenance downtime periods. It should also include contact information for reporting system and network failures.

**7.An Information Technology System & Network Maintenance** Policy which describes how both internal and external maintenance people are allowed to handle and access technology. One

important topic to be addressed here is whether remote maintenance is allowed and how such access is controlled.

Another area for consideration here is outsourcing and how it is managed.

**8. A Violations Reporting** Policy that indicates which types of violations (e.g., privacy and security, internal and external) must be reported and to whom the reports are made. A nonthreatening atmosphere and the possibility of anonymous reporting will result in a greater probability that a violation will be reported if it is detected.

9. **Supporting Information** which provides users, staff, and management with contact information for each type of policy violation; guidelines on how to handle outside queries about a security incident, or information which may be considered confidential or proprietary; and cross-references to security procedures and related information, such as company policies and governmental laws and regulations.

There may be regulatory requirements that affect some aspects of your security policy (e.g., line monitoring). The creators of the security policy should consider seeking legal assistance in the creation of the policy. At a minimum, the policy should be reviewed by legal counsel.

Once your security policy has been established it should be clearly communicated to users, staff, and management. Having all personnel sign a statement indicating that they have read, understood, and agreed to abide by the policy is an important part of the process. Finally, your policy should be reviewed on a regular basis to see if it is successfully supporting your security needs.