

---

[**Editor's Note:** The following excerpt is from Chapter 5 of the free eBook *The Definitive Guide to Windows Desktop Administration* (Realtimepublishers.com) written by Bob Kelly and available at <http://www.scriptlogic.com>.]

## Written Security Policy

A written security policy is the documentation used to define the rules for the use of computer systems in your organization. Without established, clearly written, and readily available documentation, ignorance will prevail as the reason for all security violations. A written security policy is often overlooked until the damage has been done. To protect your organization from data loss through misuse or from a lawsuit as the result of license violations or administrative action, it is important that a written security policy be defined and enforced.

Keeping in mind that desktop security is only a part of an organization's overall security policy and that the level of restrictions imposed is often based on a user's job, it is unlikely that you should be drafting this policy yourself. There should be several people from management in various departments involved in the creation and review of your organization's security policy.

### Defining Your Security Policy

We will discuss the benefits and drawbacks that come with written security restrictions later in this chapter. For now, I'll summarize considerations to keep in mind when establishing this documentation.

- Keep it realistic—In some government networks or other environments in which data is very sensitive, extreme security measures are understandably a necessity. However, too strong a security policy can impede users' effectiveness and might add complexity to desktop administration. This management concept is called *convergence*, when multiple management goals, such as productivity and security begin to conflict. You will need to determine what is important to your business, then use that definition as your middle ground. When it comes to security, it is important to find a middle ground from which you can protect your data and systems without putting an unnecessary burden on those forced to abide by these rules.



Are the rules being laid down enforceable? We will discuss many of the tools available to enforce your security policy. However, you must also keep in mind that enforcement and backing by management are vital to a security policy that is of any value. There must be a means of ensuring that the policy is followed and consequences result if they are not.

- Keep it simple—Can those who must read and abide by the security policy understand it? As a technical person, it is easy to assume an unrealistic level of technical knowledge and to use terms that not everyone will understand. Everyone must understand the security policy, and although it is painful to dumb things down to the lowest common denominator, in the case of a document such as this, it is necessary to do so.
- Keep it available—To establish a policy that people do not read defeats the purpose of creating one in the first place. Provide employees with a copy and have them sign a statement that they have read and understand it. Provide an electronic copy of the policy on your network for easy reference—a link from an intranet home page is ideal.




---

## Enforcing Your Security Policy

With your realistic, simple security policy as common knowledge, ensure that all users know how you will be aware of violations and what you will do about them. It is difficult to enforce a rule to which there is no consequence for a failure to comply.

- Employing restrictions—A majority of this chapter will focus on the technologies and tools available to enforce your security policy. If users aren't allowed to introduce media to the network, restrict their ability to do so. If users aren't allowed to install unauthorized software, restrict their ability to do so. And if users are not allowed to save data to their local systems, restrict their ability to do so. See a trend here?
- Monitoring violations—With the right tools and a little persistence, most any restriction imposed can be bypassed. Computer cases can be opened, users might bring in Plug and Play—PnP—storage devices, and users might attempt to guess passwords or access data to which they are not allowed. When you understand the weaknesses in your ability to restrict such behavior, you've reached step two of security policy enforcement—monitoring.
- Imposing penalties—Odds are that you will be the one to point the finger, but not the one to punish offenders. It is, however, important for everyone to understand the consequences of security policy violation. The sensitivity and attention given to security in your organization will dictate the severity of these consequences.

 Get it in writing! Just as if an employee were regularly late for work, if a user has repeatedly violated security policy and a move is made to penalize the user, documented reprimands are imperative. An employee might choose to fight whatever penalty is being imposed, making it difficult to enforce without proper documentation. When a user violates security, the user should be made to sign and date a document clearly stating the violation in order to confirm that the user understands what he or she has done and to establish a trend in the event that repeated violations should arise.

[**Editor's Note:** This content was excerpted from the free eBook *The Definitive Guide to Windows Desktop Administration* (Realtimepublishers.com) written by Bob Kelly and available at <http://www.scriptlogic.com>.]