

---

# Creating and Implementing an Effective IT Security Policy

*Why you need one, what it should cover, and how to implement it*

**By InstantSecurityPolicy.com**

---

## Table of Contents

<b>1. Introduction</b>	<b>3</b>
<b>2. What is a Security Policy?</b>	<b>3</b>
<b>3. Why do I Need a Security Policy?</b>	<b>4</b>
<b>4. The Security Policy Problem</b>	<b>5</b>
<b>5. What a Policy Should Cover</b>	<b>5</b>
<b>6. Types of Policies</b>	<b>6</b>
<b>7. Policy Content</b>	<b>6</b>
<b>8. Policy Implementation</b>	<b>7</b>
<b>9. Policy Review</b>	<b>8</b>
<b>10. Summary</b>	<b>9</b>
<b>11. About InstantSecurityPolicy.com</b>	<b>9</b>

---

## 1. **Introduction**

There is no right or wrong way to begin the process of developing a security policy. No single policy or security strategy will work for every organization. Contrary to what is advertised on the Internet, there is no generic template that will meet every need. A fantastic policy for Company A might be useless to Company B. A security policy must be a custom document that reflects your company's environment, and meets its specific security needs.

In fact, *a useless Security policy is worse than no policy*. Companies that boast of Security Policies thicker than a ream of paper are often the ones that have no idea what those policies say. The false sense of security provided by an ineffective policy is dangerous. The point of a Security policy is not to create "shelfware" that will look good in a binder, but rather to create an actionable and realistic policy that your company can use to manage its security practices.

*Note: This document is organized into sections, which may or may not be applicable depending on where you are in your security policy development process. Feel free to skip ahead to the section that applies best to you.*

## 2. **What is a Security Policy?**

A security policy is a strategy for how your company will implement Information Security principles and technologies. It is essentially a business plan that applies only to the Information Security aspects of a business.

A security policy is different from security procedures, in that a policy will provide both high level and specific guidelines on how your company is to protect its data, but will not specify exactly how that is to be accomplished. This provides leeway to choose which security devices and methods are best for your company and budget. A security policy is technology and vendor independent – its intent is to set policy only, which you can then implement in any manner that accomplishes the specified goals.

A security policy should cover all your company's electronic systems and data. As a general rule, a security policy would not cover hard copies of company data but occasionally some overlap is inevitable. Where the security policy applies to hard copies of information, this must be specifically stated in the applicable policy.

A security policy must specifically accomplish three objectives:

- 1) It must allow for the confidentiality and privacy of your company's information.
- 2) It must provide protection for the integrity of your company's information.

---

3) It must provide for the availability of your company's information.

This is commonly referred to as the "CIA Triad" of Confidentiality, Integrity, and Availability, an approach which is shared by all major security regulations and standards.

### **3. Why do I Need a Security Policy?**

It is generally impossible to accomplish a complex task without a detailed plan for doing so. A security policy is that plan, and provides for the consistent application of security principles throughout your company. After implementation, it becomes a reference guide when matters of security arise.

A security policy indicates senior management's commitment to maintaining a secure network, which allows the IT Staff to do a more effective job of securing the company's information assets. Ultimately, a security policy will reduce your risk of a damaging security incident.

A security policy can provide legal protection to your company. By specifying to your users exactly how they can and cannot use the network, how they should treat confidential information, and the proper use of encryption, you are reducing your liability and exposure in the event of an incident. Further, a security policy provides a written record of your company's policies if there is ever a question about what is and is not an approved act.

Security policies are often required by third parties as part of their due diligence process. Some examples of these might be auditors, customers, partners, and investors. Companies that do business with your company, particularly those that will be sharing confidential data or connectivity to electronic systems, will be concerned about your security policy.

Lastly, one of the most common reasons why companies create security policies today is to fulfill regulations and standards that relate to security of digital information. A few of the more commonly encountered are:

- The PCI Data Security Standard (DSS)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes-Oxley Act (SOX)
- Massachusetts 201 CMR 17.00
- The ISO family of security standards
- The Graham-Leach-Bliley Act (GLBA)

All these require, in some form, a written IT security policy.

---

#### **4. The Security Policy Problem**

The process of getting a security policy is difficult, time-consuming, and expensive. You typically have two choices:

- 1) Hire a security professional to write a custom policy for your organization.
- 2) Try to write your own using resources found on the Internet or purchased guides.

Number one is an expensive proposition – it can cost tens of thousands of dollars, depending on the complexity and number of policies, and take a great deal of time. Number two is impractical – it would take weeks, if not months, of painstaking work to cobble together a policy that will likely not be appropriate for your company. These two reasons deter most security policy projects before they start.

The process of getting a security policy is confusing. As an example, leading security policy experts recommend that a policy have the following components: standards, guidelines, position statements, guiding principles, rules, procedures, and lastly, policies. This jumble of “consultant-speak” is confusing at best, and does not result in a useful management tool.

To be effective, a security policy must be clear and consistent. As important, a security policy should fit into your existing business structure and not mandate a complete, ground-up change to how your business operates.

#### **5. What a Policy Should Cover**

A security policy should be written so that it can be understood by its target audience (which should be clearly identified in the document). For example, technical policies can by nature be more technical than policies intended for users, which should be written in everyday language. At no point should a security policy use confusing or obscure legal terms.

A security policy should not allow room for misunderstanding so that there is universal understanding of the policy and consistent application of security principles across the company.

A Security policy should have, at minimum, the following sections.

- Overview: Provides background information on the issue that the policy will address.
- Purpose: Specifies why the policy is needed.

- 
- Scope: Lays out exactly who and what the policy covers.
  - Target Audience: Advises for whom the policy is intended.
  - Policies: This is the main section of the document, and provides statements on each aspect of the policy. For example, an Acceptable Use Policy might have individual policy statements relating to Internet use, email use, software installation, network access from home computers, etc.
  - Definitions: For clarity, any technical terms should be defined.
  - Version: To ensure consistent use and application of the policy, include a version number that changes with any changes to the policy.

## 6. Types of Policies

Different companies will need different policies for effective security management. Below is a list of standard policies that would make up an organization's security policy. Some companies may need all these policies, while others need only a handful.

That said, certain policies can reasonably be considered "essential" to security management and are applicable to most every company. These are denoted below with an asterisk.

Acceptable Use Policy*	Network Access Policy*
Authentication Policy*	Network Security policy*
Backup Policy*	Outsourcing Policy
Confidential Data Policy*	Password Policy*
Data Classification Policy	Physical Security policy
Encryption	Remote Access Policy
Email Policy	Retention Policy
Policy	Third Party Connection Policy
Guest Access Policy	VPN Policy
Incident Response Policy*	Wireless Access Policy
Mobile Device Policy	

## 7. Policy Content

When developing content, many go about creating a policy exactly the wrong way. The goal is not to create hundreds of pages of impressive-looking information, but rather to create an actionable security plan. The following guidelines apply to the content of successful IT security policies.

- 
- A security policy should be no longer than is absolutely necessary. Some believe that policies are more impressive when they fill enormous binders, or contain hundreds or thousands of policies. In fact the sheer amount of information in those policies is what makes them useless. Brevity is of the utmost importance.
  - A security policy should be written in “plain English.” While, by nature, technical topics will be covered, it is important that the policy be clear and understood by the target audience for that particular policy. There is never room for “consultant-speak” in a security policy. If there is a doubt, the policy should be written so that more people can understand it rather than fewer.
  - A security policy must be consistent with applicable laws and regulations. In some cases there are laws that apply to a company’s security practices, such as those covering encryption. Some states have specific disclosure laws and some industries have specific regulations. Research and become familiar with any regulations or laws that apply to your company’s security controls.
  - A security policy should be reasonable. The point of this process is to create a policy that you can actually use rather than one that makes your company secure on paper but is impossible to implement. Find a middle ground in the balance between security and usability that will work for you.
  - A security policy must be enforceable. A policy should clearly state what actions are permitted and what actions are in violation of the policy. Further, the policy should spell out enforcement options when non-compliance or violations are discovered.

## **8. Policy Implementation**

Once you’ve created your policy, you need to roll it out to your organization. Too many well-intentioned projects lose steam in this phase, so this step must be well planned and undertaken thoughtfully.

First, and perhaps most importantly, a security policy must be backed by your company’s senior management team. Without their support, the cooperation needed across departments will likely doom the implementation. Department heads must be involved, and specifically, Human Resources and Legal Services must play an integral part.

If the position doesn’t already exist, an Information Security Officer should be designated at your company who is responsible for implementing and managing the

---

security policy. This is sometimes not practical at smaller companies, but regardless, one person, who has the authority to make executive decisions, needs to own and be accountable for your company's security policy.

Remember that your security policy must be officially adopted as company policy. It should be signed off on and recorded in the same way your company makes any major decision, including full management approval.

Go through each policy and think about how it will be applied within the organization. Make sure that the tools are in place to conform to the policy. For example, if the policy specifies that a certain network be monitored, make sure that monitoring capabilities exist on that network segment. If a policy specifies that visitors must agree to the Acceptable Use Policy before using the network, make sure that there is a process in place to provide visitors with the Acceptable Use Policy.

User education is critical to a successful security policy implementation. A training session should be held to go over the specific policies that will impact users, as well as provide basic information security awareness training. Often, users create security issues because they simply don't understand that what they are doing is risky or not permitted.

Users must be provided any user-level policies, and must acknowledge in writing that they have read and will adhere to the policies. If possible, coordinate this with Human Resources so that the policies can be included with any other HR documents that require a user signature.

No matter how well thought out, no policy will be 100% applicable for every scenario, and exceptions will need to be granted. Exceptions, however, must be granted only in writing and must be well documented. It should be made clear from the outset that the policy is the official company standard, and an exception will only be granted when there is an overwhelming business need to do so.

## **9. Policy Review**

After the security policy has been in place for some period of time, the company's information security controls should be audited against the applicable policies. Make sure that each policy is both A) being followed, and B) still appropriate to the situation.

Regularly review the security policy to ensure that it still meets your company's requirements. Create a process so that the policy is periodically reviewed by the appropriate persons. This should occur both at certain intervals (i.e., once per year), and when certain business changes occur (i.e., the company opens a new location). This will ensure that the policy does not get "stale" and will continue to be a useful management tool for years to come.

---

## 10. Summary

The most useful security policies share two characteristics: 1) they are an accurate reflection of a company's security strategy and, 2) they provide realistic and attainable security goals. A security policy should never simply be dictated by a downloaded template – it needs to be specific to your company. The challenging part is often finding a way to accomplish these goals without devoting a huge amount of time and/or money to the effort.

Recognize that a Security policy should not be created and then shelved for eternity, but rather actively consulted throughout your company's organization. By incorporating your custom Security policy into your company's management process, it is possible to both meet applicable regulations; and enjoy risk reduction for years to come.

Visit [www.InstantSecurityPolicy.com](http://www.InstantSecurityPolicy.com) for more information on how to obtain a professional, custom security policy in minutes. Policies that you develop at [www.InstantSecurityPolicy.com](http://www.InstantSecurityPolicy.com) were created according to all the principles found in this document.

### **About InstantSecurityPolicy.com**

InstantSecurityPolicy.com is the only provider of online, customized, instant IT security policies in the world. Since its launch in 2008, the site has helped hundreds of companies from across the globe to cost effectively address their security policy needs. Policies developed by InstantSecurityPolicy.com assist a diverse customer base to fulfill industry regulations, provide security documentation for audits, and act as a security handbook to set company policy.



InstantSecurityPolicy.com  
100 Capitola Drive, Suite 302  
Durham, NC 27713

888-764-4610 **toll free**  
919-998-8383 **international**  
[info@InstantSecurityPolicy.com](mailto:info@InstantSecurityPolicy.com)