The IT Security Policy Guide

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

By: InstantSecurityPolicy.com

Table of Contents

1. Introduction

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.

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 living, custom document that reflects your company's environment and culture, 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 and reduce its risk of a security incident.

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 processes and 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 some overlap is inevitable, since hard copies invariably were soft copies at some point. 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. Additionally, this approach is consistent with generally-accepted industry best practices for security management.

3. Why is a Security Policy Necessary?

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. And in the event of a security incident, certain policies, such as an Incident Response Policy, may limit your company's exposure and reduce the scope of the 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 that do business with your company 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 meet 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 HITECH Act

- 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

Simply put, security policies are not easy to create. The process of getting a security policy is difficult, time-consuming, and expensive. Companies 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 completely appropriate for your company. These two reasons deter most security policy projects before they start.

Additionally, the process of getting a security policy is confusing. As an example, different 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. More information can be found in the Policy Implementation section of this guide.

5. What a Policy Should Cover

A security policy must 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 allow no room for misunderstanding. There must be a 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 is changed to reflect any changes/updates 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 considered "essential" to security management and are applicable to most every company. These are denoted below with an asterisk.

Acceptable Use Policy*
Authentication Policy*
Backup Policy*
Confidential Data Policy*
Data Classification Policy
Encryption Policy
Email Policy
Guest Access Policy
Incident Response Policy*
'Mobile Device Policy
Network Access Policy*
Network Security policy*
Outsourcing Policy
Password Policy*
Physical Security policy
Remote Access Policy

Retention Policy
Third Party Connection Policy
VPN Policy
Wireless Access 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 even thousands of policies. These types of policies overwhelm you with data, and are frequently advertised on the internet. But quantity does not equal quality, and it is the sheer amount of information in those policies that 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. Clarity must be a priority in security policies, so that a policy isn't misunderstood during a crisis, or otherwise misapplied, which could lead to a critical vulnerability.

- A security policy must be consistent with applicable laws and regulations. In some countries there are laws that apply to a company's security practices, such as those covering the use of encryption. Some states have specific disclosure laws or regulations governing the protection of citizens' personal information, and some industries have regulations governing security policies. It is recommended that you research and become familiar with any regulations or standards 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. Keep in mind that the more secure a policy is, the greater the burden it places on your users and IT staff to comply. 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, and must be consistent with applicable laws.

A security policy can be formatted to be consistent with your company's internal documentation; however certain information should be placed on each page of the policy. At a minimum, this information should include: policy name, creation date, target audience, and a clear designation that the policy is company confidential.

8. Policy Implementation

Once you've created your policy, perhaps the hardest part of the process is rolling 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 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. Make sure you have management buy-in before you get too far along in the process.

If the position doesn't already exist, an Information Security Officer or IT Security Program Manager should be designated at your company who is responsible for implementing and managing the security policy. This can be an existing manager. This designation 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 senior management approval.

Next, 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. In this phase, if you discover something impractical, create a plan to make appropriate changes to either the network or the policy.

Understand that policies differ from processes and procedures. You will need to carefully consider the necessary security processes and procedures after you have your policy finished. For example, the Backup Policy may detail the schedules for

backups and off-site rotation of backup media, however it won't say exactly how these tasks are to be accomplished.

Additionally, certain procedures must be created to support the policies. For example, how should your users respond if they suspect a security incident? How will you notify your users if they are noncompliant with a specific policy? How will exemptions to the policy be requested and approved? Work with the necessary departments within your company (Legal, IT, HR, etc.) to establish procedures to support your policies.

User education is critical to a successful security policy implementation. A training session should be held to go over the 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 against the security policy.

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 implemented, 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 - which can be anywhere from three months to a year, depending on your company - the company's information security controls should be audited against the applicable policies. Make sure that each policy is being followed as intended and is still appropriate to the situation. If discrepancies are found, or the policies are no longer applicable as written, they must be change to fit your company's current requirements.

After the initial review process, you should 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.

When changes need to be made, be sure to A) update the revision history section of the document to differentiate the new document from past versions; and B) distribute

any modified user-level policies to your users. Clearly communicate the policy changes to any affected parties.

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 what is pre-written in 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.

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.

Visit www.InstantSecurityPolicy.com for more information on how to obtain a professional, custom security policy in minutes.

InstantSecurityPolicy.com
100 Capitola Drive, Suite 250
Durham, NC 27713

888-764-4610 **toll free**
919-998-8383 **international**
info@InstantSecurityPolicy.com