Security Policy 101

Essential Information Security Policies Every Organization Must Have

By David Lineman

InformationShield

About Information Shield

Information Shield is a global provider of security policy, data privacy and security awareness solutions that enable organizations to effectively comply with international security and privacy regulations. Information Shield products are used by over 9000 customers in 60 countries worldwide.

Information Shield, Inc.
7549 Highmeadow Dr.
Houston, TX 77063
www.informationshield.com
sales@informationshield.com
P: 888.641.0500
F: 866.304.6704

Essential Security Policies that Every Organization Must Have

Many organizations are aware that they need information security policies. Perhaps they have been asked by a large customer to demonstrate that they are capable of protecting sensitive data. Or maybe the organization has to comply with one of several federal regulations that require policies. In any case, organizations often mistakenly refer to a single "policy" when they talk about information security. While all of the essential elements of protecting information can be in a single policy document – that is not advised or sufficient.

So what essential security policies do you need? We will answer by taking a quick walk through the essentials of protecting information and reducing the risk of data loss. These are the essentials that any auditor, regulator, customer or insurance provider will want to understand.

> *"A security policy is written set of rules the organization will follow to protect information."*

Why do we need information security policies?

An information security policy is simply a written set of rules the organization will follow in order to protect information. While simply defined, security policies play three critical roles in managing information security:

1. **Demonstrate** – Written policies demonstrate that management is serious about information security. If the organization does not take the time to develop written policies, it is a good sign that management is not performing due diligence in protecting customer and company data.

2. **Organize** –Security policies document what the organization is actually going to DO to protect information. Modern information systems are incredibly complex and store vast amounts of data. It is impossible to protect data on these systems without an organized plan. Written security policies define the "rules of the road" for how data and systems will be protected.

3. **Communicate** – Security policies formally communicate how the organization will protect data. People want to know if your organization is serious about security. Your customers want to know that you won't lose their data. Insurance companies want to know you won't cost them money with a breach. And Regulators want to know if you are complying with data protection laws. Security policies are a formal way to demonstrate to customers, auditors, regulators and business partners.

Can we demonstrate management support for information security?

Like an effort within an organization, those without management support are generally doomed to fail. Because information security is a cost to the organization, it is often slighted or overlooked completely. That is why all data protection laws require some evidence that the senior management of the organization is serious about information security.

Information Security Program Policy *– Defines the organizations overall approach to information security, including the developing of information security plans and written policies and procedures.*

> *"Security efforts without management support are generally doomed to fail."*

Information Security Roles and Responsibilities Policy *– Defines the key roles of information security organization, including the specific responsibilities of everyone in the organization.*

Do we know where sensitive data resides?

This seems obvious: before we can protect sensitive information, we need to understand *what* and *where* it is. Since information security can be a complex effort, the goal is to protect information according to how valuable or 'sensitive' it is within the organization. For example, the customer list or payroll list are almost always very valuable and would cause much harm if they were lost or stolen. On the other hand, a press release or research paper might actually be designed to be disclosed to the public. Examples of security policies that help you keep track of this information include:

Information Classification Policy *– Defines how information is classified and labeling, including which data is PUBLIC, CONFIDENTAL or SENSITVE.*

Asset Management Policy *– Defines how both information and technology assets are acquired and managed.*

Information Disposal Policy *– Defines how the organization will dispose of information and key technology that contains the information.*

Can we limit access to sensitive data?

Once we know the location and format of data we can protect it. One of the fundamentals of information security is limiting data access based on "the need to know." The concept is simple – only give people access to the information they need to perform their jobs. This access is controlled via personal authentication - userids and passwords. Examples of security policies that define personal access include:

Access Control Security Policy *– Defines who is authorized to access data and how systems are designed to protect sensitive data.*

Account Management Policy *– Defines how personal userids and passwords are issued and managed.*

Remote Access Security Policy *– Defines how employees and contractors can safely access data from remote locations.*

Can we safely transmit sensitive information?

Assuming that we understand what our sensitive is and where it resides, we need to protect it when it moves. Very few people are aware of just how much sensitive data moves around each day within their organization via email, networks, paper documents and phone calls. Examples of security policies that help protect data during transfer include:

> *"For effective security, we need to protect data both at rest and in motion."*

Information Exchange Security Policy *– Defines how sensitive information is safely transmitted in both digital and paper form.*

Third Party Security Policy *– Defines how any third party organization will safely access and process sensitive data.*

Network Security Policy *– Defines how the organization builds, manages and secures computer networks and network access, including firewalls.*

Can we protect physical access to sensitive data?

Information is only as secure as the container it resides in. All of the technical security in world will be limited if a thief can simply walk in and steal a server loaded with data. That is why every major data protection law requires some form of physical security. Examples of security policies that protect your physical surroundings include:

Physical Access Security Policy *– Defines how the organization will control physical access of employees and visitors, including badges, gates, and guards.*

IT Data center Security Policy *– Defines how the organization will protect the IT data center, including both physical access and protection from the environment – water, fire, wind and power outages.*

Can we manage our internal systems to protect data?

By definition, most electronic information sits somewhere on a piece of computer or networking gear. The most common examples are data servers, email servers, firewalls and backups. To be secure, these systems must have secure configurations. And all of these systems are ultimately managed by people. Thus it should be no surprise that the most common risks for any organization include those from poor configurations and accidental or incorrect changes. Examples of policies for managing internal systems include:

Change Management Policy *– Defines how patches and system updates are handled*

System Management Policy *– Defines how systems are securely configured and managed, including the proper configuration of operations systems and software.*

Malicious Software Policy *– Defines how the organization will protect against infestations of malicious software including Trojans, worms, keyloggers, rootkits and other malware*

Can we monitor the movements of sensitive data?

Most people never stop to think how much information flows through their organization on a daily basis in both digital and paper form. A typical organization may send hundreds of emails and visit thousands of web pages in a single day. In order for organization to protect data, they must be able to monitor activities that are relevant to security. Examples include internet traffic, which userids are logged into the network at any given time, and who is physically present within the company buildings. An example of such a policy:

Audit and Log Management Policy *– Defines how information systems will record events and manage the history of these events for proper record-keeping, security, privacy and disaster recovery.*

Can we safely use information technology to protect data?

Whenever humans use computers or other technology, there is the potential for mistakes. Examples include a customer service person accidentally emailing an attachment with the wrong customer data, or a laptop being left in a taxi with the entire customer database. Perhaps an employ clicks on a link which installs malicious software on your network? Each of these examples has already happened hundreds of times in the real world. Since most information today ends up in some digital form, we must define safe ways for employees to use computers, electronic email, the web, instant messaging and office systems. Examples of policies that define proper usage include:

Acceptable Use of Assets Policy *– Defines the ways that employees can safely use computers, email, internet, faxes, phones and other assets.*

Can we recover from an event or physical disaster?

There is no such thing as "perfect" security. No matter how much money or technology the organization uses, there will always be some security risk. That is why one of the essential elements of effective security is the ability to respond to and recover from events. In some cases, organizations have been completely destroyed by a fire or flood. In other cases, a virus infection has caused thousands of dollars worth of damage or disclosed banking information to criminals. The faster and better you can respond, the less risk the organization has. Examples include:

Data Backup Policy *– Defines how the organization will manage the backup and restoration of critical information, including the security of the backup media.*

Computer Incident Response Policy *– Defines how the organization reports and responds to security events, including possible data breaches.*

Business or Disaster Recovery Policy *– Defines how the organization will resume business in the event of a major disruption of business.*

So which policies do we need?

Well, we've got good news and bad news. First, the bad news – your organization needs all of these information security policies. These policies work together to form a data protection framework. Each one has limited impact if it used in isolation. (How can we backup sensitive data if we don't know where it resides?) Now the good news. Each of these documents can be fairly simple and straightforward, depending on the complexity of your organization.

> *"Quality information security policies are possible with the right templates and the right guidance."*

And now the REALLY good news. You don't have to start from scratch. Companies like Information Shield have created a group of security policy templates that cover each of these key areas and more. These templates not only save your organization time and money, but they are based on industry best practices that have been used of decades across many organizations.

The bottom line: Having quality written information security policies is something your organization can accomplish with the right guidance, the right start, and support from senior management.

About the Author

David J. Lineman is president and CEO of Information Shield, Inc. a global provider of information security policy and data privacy leading practices. He has 25 years of software, security and information technology management experience, and holds 3 patents on software technology. He is a frequent speaker and author on the topics of information security policy and regulatory compliance.

Mr. Lineman is also the editor of the *Security Policy Solutions Newsletter* and contributing author to the *Security Policy University Blog*. His has been featured in *SC Magazine, The Cutter IT Journal, Windows Security, CRM Magazine, Houston Business Journal, Texas CEO Magazine, Dell Solutions Magazine*. He has also spoken about information security topics on *KHOU TV in Houston* and *The Business Makers Radio Show*.

Sponsored by eRisk Hub®

This research paper is offered as a bonus for eRisk Hub® member companies and their clients. For more information visit our website at www.eriskhub.com.

Summary – Essential Information Security Policies

Acceptable Use of Assets Policy

Access Control Security Policy

Account Management Policy

Asset Management Policy

Audit and Log Management Policy

Business or Disaster Recovery Policy

Computer Incident Response Policy

Data Backup Policy

Information Classification Policy

Information Disposal Policy

Information Exchange Security Policy

Information Security Program Policy

Information Security Roles and Responsibilities Policy

IT Data center Security Policy

Network Security Policy

Physical Access Security Policy

Remote Access Security Policy

Third Party Security Policy