Template
Security and Privacy Policies

Provided by CSPO Tools - materials for the security and privacy officer

Highlights

Pre-written materials – ready for you to edit and use in your company.

Downloadable tools for self-assessment and compliance

Avoid the cost, and time, of building your materials from scratch.

Reduce your need for expensive consultants by using these materials

The cost? This document is free, and an annual subscription to our library of materials is only about equal to the cost of a book.

Stop by the CSPO Tools site to see what other materials we have available for you to use.

CSPO Tools, Inc.
Cary, NC
www.CSPOtools.com

Every regulation and industry standard states that you must have security and privacy policies.

But these regulations don't help you in actually writing your policies.
That's why CSPO Tools is providing this set of security and privacy policies.

Security policies are the top-level set of documents at your company. They document company decisions on the protection, sharing, and use of information in your company's care. A complete and appropriate set of policies will help you avoid liability and compliance problems late on.

You may also want to download our template security standards document, which sets out requirements at the detailed level for passwords, authentication, and similar topics. Some companies call that document a policy document – so take a look at both. Just stop by our website and download a copy.

You don't have to swim in circles, looking for security and privacy materials.

That's Delila, the company swan, in the picture at the top of the page. Some days, she prefers swimming in the kiddy pool rather than the lake – she actually likes going round and round, getting nowhere.

But, you don't have to go round and round, looking for examples of security and privacy materials. CSPO Tools has the materials you need already written, ready for you to download.

- Security and privacy policies – much more than what is in the free package
- Security and privacy standards for a company
- Awareness training materials, ready for use with your staff
- Roles and responsibilities definitions, job descriptions – even pre-written job postings
- Self-assessment and compliance scoring tools
- Information security and privacy procedures
- Emergency response plans
- Compliance tools for PCI DSS, HIPAA, ISO 27000 series, FISMA, and more

We're adding more all the time, with many items free of charge. We invite you to stop by and see what is available – www.CSPOtools.com.

This is the template version of basic Information Security and Privacy policies, provided by CSPO Tools, Inc.

How to use this document

Purpose

This is one of the standard documents which every organization needs to create. Since it is much easier to create this sort of document if you have an example in front of you, we are making this template version freely available to everyone.

In this document you'll find:

- a company security policy
- a privacy policy suitable for use with your employees
- a privacy policy suitable for use with your customers

You may want to put these policies into your employee handbooks, your annual training, new employee hiring process – and also to use them when presenting your company's core values to prospective customers.

By the way - stop by www.CSPOtools.com to check for updates and additions to this document, and for other items (many are free, as this one is).

License

Making this document suit your organization

Read through it, marking up the places where you need to make changes. For example:

- Are you a 'corporation', or do you call yourself a 'firm' or use another word? Just change it – we set this up to say 'corporation', since that is the most common.
- Do you call your employees 'associates', 'employees', or another word?
- Think carefully about the wording in the Employee and Customer policy sections. The wording in this template document will fit most companies, but you will have to be comfortable with the promises made (to your customers) and the rules imposed (on your employees).

Once you have worked out your updated version, make certain that all interested parties can agree to the new version. You will likely need to show this policy to the business owners, the representatives of the employees and investors, your trading partners (such as vendors who handle your information), and also to your legal department.

Implementing the policies

You will need to make each employee, vendor, contractor, and others aware of this policy once you have it customized and approved. One way to do this is to collect signatures from everyone once you have done the training program on the policy. We have put a signature page at the end of this document.

You may also need to update your contract terms and conditions to reflect this policy, and may need to update your employee handbooks also.

Materials for the training program are available at our site. These include Powerpoint slides, and scripts for you to follow.

The sales pitch

This document is a part of a basic toolkit, which includes other policies, standards, and awareness training materials needed to start up the security and privacy efforts at a company. Our library has much more for you to use.

Subscribers to our library of tools have access to the source documents, in Microsoft Office or other formats as appropriate (this makes it easier for you to edit things). Plus, there are a lot more things in the library than these policies.

For example: you may need slides and a script to follow when doing your awareness training for your employees… that sort of added tool is included in the library.

The cost is only about equal to a book – much less than the cost of hiring a consultant. Check in at our web site, and see what else is included in the library – we think you'll find there many more items which you can use.

■■■■

Please let us know if you need help, and what you would like to have added. We are at www.CSPOtools.com. And, remember – there's more free material on that site!

And now, onward to the template document…

Information Protection Policy

Background

Our company has many more assets that the physical world you see by looking around you. These assets are *information*, which is critical to doing business, keeping the trust of our customers, and keeping our future strong. This policy outlines our commitments to our employees, customers, and to our future regarding how we will handle this information.

Information can be sensitive by its nature, and can also be sensitive due to regulations and industry standards. The types of sensitive information can include:

- Customer information (both for customer companies and for people as individuals)
- Financial information, including credit cards, salaries, banking, transactions and more
- Medical information of all types
- Company patents, business plans, and other intellectual property
- Company business records and planning materials, including our customer list, marketing and sales efforts, product line plans, and more.
- Copyrighted materials, both which our company creates and those which we obtain under license from others

This information may reside on our computing systems or backup devices, may traverse the networks, be on paper, or be in people's minds. All locations must be properly controlled.

The rules by which information is handled are determined by the regulations, business requirements, and company commitments relating to that type of information. Put together, these are called the *significance* of the information.

Every employee, vendor, contractor, supplier or vendor, agent or representative of our company must be aware of the significance of the information being handled, and ensure that proper controls are applied to prevent copying, disclosure, or other misuse of the information.

This Information Protection policy is a part of the overall security and privacy effort of our company. Other policies and controls may also apply, as issued by the Human Resources and Security teams. These are available in the employee handbook, or on the company's intranet site.

Penalties for violating these policies may include disciplinary actions up to termination of employment, or termination of the business relationship with our company.

Our company relies upon employees and business partners to properly develop, maintain, and operate our systems, networks, and processes which keep our sensitive information safe and properly used. This means that every person and organization handling our information has the responsibility to keep the information safe, no matter where the information is located. This includes computing systems, networks, paper copies, business processes, and verbal transmission of information.

Our company's policy

- We will meet all applicable requirements in properly protecting the information, including:
  - Laws
  - Regulations
  - Industry standards
  - Contractual commitments

- The protections we apply to information assets will be in proportion to the value and sensitivity of the information, and will balance the sensitivity of the information against
  - The cost of controls
  - The impact of the controls on the effectiveness of business operations
  - The risks of disclosure, modification, destruction, or unauthorized use of the information

- We will protect all types of sensitive information, including but not limited to
  - Medical
  - Financial
  - Credit
  - Business transaction and planning
  - Personal information, both of our employees and of our customers

- We will ensure that these controls are accepted by all employees, vendors, service providers, representatives and associates of our company who may have access to our information. This includes ensuring that all personnel at all levels are aware of, and are held accountable for safeguarding information assets.

- We will ensure that access to information is controlled, and based upon, job function and need-to-know criteria.

- We will maintain proper business continuity and security procedures, including information systems, networks, resources, and business processes.

- We will report any suspected or actual breach of these policies, and will cooperate with investigative agencies.

- We will comply with other, related policies, including the Company's privacy policies.

Privacy Policy for Employees

Our company values each employee, and so has a commitment to protect the personal information which we handle on behalf of the employee.

It is our policy that:

- Our company will collect only that information about employees which is needed and relevant.
- Our company will strive to make certain that personal information about employees is kept accurate and up-to-date.
- Our company will use appropriate controls to ensure that this information is kept secure, and is only viewed or used by the proper personnel.
- Information about employees will not be disclosed to any external parties unless appropriate.
- Employees will be told how they can review information about them, make updates, and report problems.
- Our company will comply with applicable laws, regulations, and industry standards when protecting employee information.
- We hold our employees, vendors, contractors, suppliers, and trading partners to meet this same set of policies.

Privacy Policy for Customers

It is a part of our company's core values that we will properly value and protect any information entrusted to us about our customers. This policy describes how we will safeguard personal and company information, to ensure peace of mind when dealing with our company.

It is our policy that:

- Our company will collect only that information about customers which is needed and relevant.
- Our company will not disclose information to other parties unless customers have been properly notified of such a disclosure.
- Our company will strive to make certain that information about customers is kept accurate and up-to-date.
- Our company will use appropriate controls to ensure that this information is kept secure, and is only viewed or used by the proper personnel.
- Our company will comply with applicable laws, regulations, and industry standards when protecting employee information.
- We hold our employees, vendors, contractors, suppliers, and trading partners to meet this same set of policies.

I have read and understood the Company's security and privacy policies.

_____ _____

Signed Date