



flex-protection

We Can Help!

Protect Your Company / Organization

From Cyber Attack or Data Loss



Sensible Measures to Reduce Risk



Our Portfolio of Services and Flexible Tools

	<p>Free Written Information Security Policy Utilize our flexible Information Security Policy (ISP) for a high-level roadmap to a more secure environment. Use it as-is or customize it to more precisely match your operations. Already have an ISP? Let us review it with you on a confidential basis.</p>
	<p>Data Defender Program Take advantage of the 7 Best Practices and the 5 Easiest Ways to make a difference. We'll help you understand and implement these improvements as needed. The Data Defender program provides a basic cost-effective framework designed to improve your security.</p>
	<p>Risk Assistant Cloud-Based Application Identify threats to your organization and deploy corresponding defensive measures. Quantify and track your overall risk situation on an ongoing basis. Risks may be categorized as Technical, Physical, and Administrative.</p>
	<p>User Security Awareness Training (SAT) Security training for system users reduces the chances of a successful attack or security breach. A course for the non-technical will include basic concepts, password management, email risks, and encryption fundamentals.</p>
	<p>High-Level Assessment A review of your current operations, infrastructure, data stores and defenses in place. We'll look for danger spots and opportunities for improvement, without disrupting your business. The assessment can be as detailed or summarized as you need.</p>

The Five Easiest Steps

There are steps you can take to protect yourself without breaking your budget. Our list is prepared from the perspective of a mid-market business or nonprofit with limited resources.

Don't look here for technical, complex operations like deep vulnerability scanning, script-based penetration testing, code-based exploits, red teams and blue teams and so forth. These are all very useful activities and strategies, but they are beyond our scope here.

An outline of our 5 Easiest Steps:

1. Create a comprehensive but simplified Data Security Policy
2. Make an inventory of your critical data, and how it is protected.
3. Arrange user awareness training and knowledge tests.
4. Establish Defense in Depth.
5. Understand what else is available.

The 5 Easiest Steps: Documents and Details may be downloaded from www.flex-protection.com.

Top 7 Best Practices

1. Automate Your Daily Backups.
2. Spend the most resources on protecting the crown jewels.
3. Place a high priority on user education.
4. Hire a Penetration Tester.
5. Separate computers, networks, and servers when possible.
6. Get cost-effective help.
7. Stay with it.

Top 7 Best Practices: Documents and Details may be downloaded from www.flex-protection.com.

Information Security Policy

Purpose

The purpose of an Information Security Policy (ISP) is to provide a broad framework of guidelines and defensive measures for the protection of company and customer information assets.

Its goal is to reduce the chances of a data breach, system hack, or privacy violation by assigning responsibility for better practices, processes, monitoring and user education. Adopting these policies demonstrates to customers, employees and stakeholders that the company takes data security and privacy seriously. It provides a road map of how behaviors, procedures, protections and technology are used as added security measures.

The ISP provides a high-level view of common threats and defensive measures, and the steps needed to better control risk. It strongly encourages the designation of specific staff or management to be responsible for certain tasks.

This policy document is considered effective when signed and dated by management, and should be revised, reviewed, and signed off on periodically in the future. This policy document should be updated at least quarterly, to ensure that the information is current. Verify that the correct individuals are still properly assigned to each area of responsibility, and that the identified responsibilities are being carried out.

Executive Summary

No security policy is 100% guaranteed to prevent a data breach or cyber incident. The threat landscape is constantly changing, and a dedicated team of hackers can eventually disrupt or gain access to operations and confidential data. What an ISP will do is act to reduce the risks, and to do so cost-effectively.

Economics must be considered when implementing an Information Security Policy. The mostly elaborate defenses can be very costly. Focus on those defensive measures which will provide the most impact at the least effort and cost. The “low hanging fruit” items will be addressed before more complex measures are considered.

Internal cyber threats have proven to be a greater risk than external threats. It is common to experience a data breach resulting from a bad actor guessing someone’s password, or simply asking for it. Less common is the hooded hacker in a dark room delivering a complex technical exploit onto your network, although this does happen.

Therefore, policies and guidelines involving Account and Password Management and User Education are paramount, along with a current prioritized Data Inventory.

Policy statements and guidelines herein generally conform to the widely accepted NIST Cybersecurity Framework (National Institute of Standards and Technology).

Further steps which may bring additional security, albeit at an increased cost, are identified below under “Additional Steps”.

The fully customizable Information Security Policy may be downloaded from www.flex-protection.com.

The Data Defender Program

Data Defender is an annual subscription that provides a basic level of protection.

It provides simple guidelines and measures that are universally recognized as ways to prevent attacks and data breaches. The subscription includes:

- The 5 Easiest Steps
- 7 Best Practices
- Data Inventory template
- Security Questionnaire
- A customizable Information Security Policy document.

Data Defender also includes a one-time vulnerability scan of your network and website, with a written report.

Details about the Basic Defender and Enterprise Defender programs are available at www.flex-protection.com/defender.aspx

Risk Assistant Application

Show your management or clients that you are taking action to reduce cybersecurity risks, and to improve your security posture. Risk Assistant is a management application, not a technical tool.

Use your private cloud-based Risk Assistant tool to import common risks and add additional threats you may face. Deploy effective defensive measures to reduce and track overall risk. Use your personal dashboard to manage your exposure and your flexible preventative measures.

While the Risk Assistant will make suggestions, you are the final authority on which risks will be tracked and measured and which defensive measures will be deployed.

Here are selected screen images from the Risk Assistant application.

Risk Assistant - Managing Cybersecurity Risk

Cyber Risk – Defensive Measures = **Reduced Risk**



Security Risks
Security Measures

Risk Assistant provides direct evidence of your organization's good faith efforts to manage cybersecurity risks.

Continue

Dashboard
Risks
Measures
Matching
Dashboard

Totals across all risks and measures:

Number Defined Risks: 23

Type of Risk

- Technical: 8
- Physical: 4
- Administrative: 11

Number Defined Measures: 35

Type of Measure

- Preventive: 3
- Detective: 5
- Corrective: 7

Matching Risks and Measures

Risks With Measures Assigned

- Assigned: 2
- Unassigned: 21

[Work With Risks](#)

[Work With Measures](#)

[Analytics](#)

Reduction in expected cybersecurity losses credited to defensive measures:

Single Loss Expectancy

Raw: 70,000
With Measures: 45,000

Annual Rate of Occurrence

Raw: 6
With Measures: 4

Annual Loss Expectancy

Raw: 420,000
With Measures: 180,000

Reduction in Annual Loss Expectancy(ALE)

420,000
-180,000
=====

240,000

Risk Assistant
Dashboard Help
Archive Current Values
Logout

View a short demo of the user-friendly Risk Assistant application at www.flex-protection.com/ra.mp4

Security Awareness Training

The best cybersecurity investment you can make is better training.

According to the Harvard Business Review, the major sources of cyberthreats aren't technological. They're found in the human brain, in the form of curiosity, ignorance, apathy, and hubris. These human forms of malware can be present in any organization and are every bit as dangerous as threats delivered through malicious code. Employees are the weak link in corporate cybersecurity, but also the best defense, if they are given policies that are easy to follow and not too numerous.

Arrange for an online Security Awareness course for your users and management.

Purpose:

- Reduce the chances of a successful attack or security breach.
- Promote awareness of good security design and habits.

Course Outline:

- Cyber Threats
- Types of Attacks
- Malware - Types and Damage
- Social Engineering
- Phishing Attacks
- People and Roles
- Physical Security
- Password Management
- Safe Browsing
- Outside Devices and BYOD
- Documents and Policies
- Best Practices

High Level Security Assessment

Do ANY of these apply to you?

- We need to have a brief “discovery” conversation to identify options.
- We could use help developing or reviewing a formal data security policy.
- No one knows exactly what data stores are being backed up.
- We are looking for scanning and testing to identify possible exposures.
- We need to get our arms around the most critical risks and how to reduce them.
- We want to reduce risks by providing Best Practices education for our end users.
- It would be good to know what tools and systems are available for protection.

Basic Data Security Check-Up

- Review and suggest improvements to your Data Security Policy.
- Review/develop your Security Testing Plan.
- Perform vulnerability scans of your network and/or web applications.
- Provide tips for "hardening" your devices, applications, and data storage.
- Provide an online "Security Awareness" course highlighting end-user best practices.
- Identify additional steps to improve overall security without disrupting operations.

A high-level security assessment starts with a questionnaire such as the following:

Information Security - **Confidential** Discovery Survey

(Use the TAB key to move from field to field)

Date: _____

Company / Organization: _____

Contact Name: _____ Position: _____

E-mail: _____ Phone: _____

Employees: 1-100 101-1000 Over 1000

Approximate number of Information Technology staff? _____

Do you have a public web site?

Web site address? _____

Where is it hosted? _____

Other public-facing applications: _____

Is your web site encrypted (HTTPS)?

Internal Email server or cloud email? _____

Sensitive files on laptops / tablets? In cloud-based services?

Is there a written password policy? Is it enforced?

Regular data security training for staff? How often? _____

What topics are covered in end-user security training?

Do you have a formal Information Security Policy?

Do you have a formal Security Testing Plan?

Do you have a dedicated CISO (Security Officer)?

Name & Contact info: _____

Computers & Servers on Windows? Unix/Linux? Mac?

Have you had an outside resource review your policies and planning? Who?

Have you experienced a data breach recently? Please describe:

Copyright National Training Systems, Inc. All rights reserved. www.Flex-Protection.com