

INFORMATION SECURITY POLICY TEMPLATE

Version 1.0, Last Revised 7/12/10

SAMPLE

How to use the Policy Template

This template is meant as a guide for creating an information security policy specifically tailored to your organization. Much of the content is written in a general manner that conveys the concepts of what should be addressed. This policy template is not meant to be all encompassing, but rather meant to guide and highlight areas that need to be covered. You may find areas in your organization that are specific and not addressed in the template. Therefore, as you proceed to examine your organization and its processes you need to identify all areas that need high-level executive direction to handling your information in a secure manner.

First, executive management should designate and charge a group or individual with the specific responsibility of creating, maintaining, and enforcing the information security policy. In situations where a group of individuals is charged as a body, one person should be designated with the responsibility of coordinating the activities of this group. In either situation, this designation should be clearly communicated to the entire organization by executive level management. This will ensure the cooperation and continued success of the challenge ahead of the individual or group.

Throughout the document you will see the designation of an "information security officer". Your organization's designation should be substituted if you wish to use a different title. It is critical that throughout the document this designation references an individual person that is responsible for this role versus a group of people. In any case, you will want to avoid designating a person by name and all references should be made by title and designation (i.e. Information Security Officer vs. John Smith). This will avoid unnecessary updating of the policy when personnel changes occur. In the following pages of the policy, you will find **<angle brackets in red>** designating a substitution of your organization's name or other required fields that should be replaced with the appropriate information that is specific to your organization.

Again, this is a template for creating your own policy. It is vitally important that this policy be applicable to your organization and that the policy be effective in your organization. The policy should be structured and worded in a way that the policy can be the foundation of your security.

Table of Contents

Policy Applicability	1
Introduction	1
Purpose and Scope.....	1
Sanctions and Violations.....	1
Revisions and Updating Schedule	1
Contact Information.....	2
Roles and Responsibilities	2
Owners	2
Custodians.....	2
Users	2
Designation	2
Information Release and Disclosure	2
Acceptable Use.....	3
Definitions.....	3
Networks	5
1.0 Purpose	5
2.0 Scope	5
3.0 Policy	5
3.1 Firewall	5
3.2 DMZ	5
3.3 Internal	5
3.4 External	5
3.5 Wireless	6
3.6 Moves, Adds, Changes	6
3.7 Vulnerability Scanning	6
3.8 Penetration Testing	6
3.9 Encryption.....	6
3.10 Remote Access.....	6
3.11 System Logs	6
Information Systems	7
1.0 Purpose	7
2.0 Scope	7
3.0 Policy	7
3.1 Information Systems.....	7
3.2 Vulnerability Management	7
3.3 Moves, Adds, Changes	7

3.4 File Integrity Monitoring.....	8
3.5 System Logs	8
3.6 Encryption.....	8
3.7 Remote Access.....	8
3.8 Backup/Recovery	8
3.9 Administrative Access.....	8
Data	8
1.0 Purpose	8
2.0 Scope.....	8
3.0 Policy	8
3.1 Approvals	8
3.2 Least Privilege (Need to Know).....	8
3.3 Encryption.....	9
3.4 Classification	9
3.5 Storage.....	9
3.6 Handling.....	9
3.7 Shipping	9
3.8 Printing / Copies	9
3.9 Removal / Destruction / Disposal	9
3.10 Remote Access.....	9
3.11 Backup and Recovery.....	10
3.12 System Logs	10
3.13 Mobile Devices	10
Vulnerability Management.....	10
1.0 Purpose	10
2.0 Scope.....	10
3.0 Policy	10
3.1 Operating System Updates	10
3.2 Common Software	10
3.3 Anti-Malware	10
3.4 Personal Firewall.....	11
3.5 Vulnerability Scanning	11
3.6 Penetration Testing	11
3.7 Notification	11
Physical Security.....	11
1.0 Purpose	11
2.0 Scope.....	11
3.0 Policy	11
3.1 Controls.....	11

3.2 Access	12
3.3 Approval.....	12
3.4 Third-Parties	12
3.5 Employees.....	12
3.6 Unauthorized Access	12
Remote Access	12
1.0 Purpose	12
2.0 Scope.....	13
3.0 Policy	13
3.1 General	13
3.2 Requirements	13
Accounts and Passwords	14
1.0 Purpose	14
2.0 Scope.....	14
3.0 Policy	14
3.1 General	14
3.2 Guidelines	14
Change Control.....	16
1.0 Purpose	16
2.0 Scope.....	16
3.0 Policy	16
3.1 Approval.....	16
3.2 Process.....	16
3.3 Documentation.....	16
Monitoring and Testing.....	16
1.0 Purpose	16
2.0 Scope.....	17
3.0 Policy	17
3.1 Information Security Policy.....	17
3.2 File Integrity Monitoring.....	17
3.3 Logs and Alerts.....	17
3.4 Change Control	17
3.5 Vulnerability Testing	17
3.6 Penetration Testing	17
3.7 System Logs	17
3.8 Access Rights.....	18
Mobile Systems.....	18
1.0 Purpose	18
2.0 Scope.....	18

3.0 Policy	18
3.1 Configuration	18
3.2 Secure	18
3.3 Data Storage	18
Incident Response	18
1.0 Purpose	18
2.0 Scope	19
3.0 Policy	19
3.1 Roles and Responsibilities	19
3.2 Notification	19
3.3 Incident Specific	19
3.4 Testing	19
Employee Training and Security Awareness	19
1.0 Purpose	19
2.0 Scope	19
3.0 Policy	19
3.1 General	19

SAMPLE

Policy Applicability

Introduction

Every day information increases in value; those with ill intent are highly motivated to obtain this information in an ever-expanding matrix of methods. Therefore, we must be diligent and be on guard. As a company we hold and create valuable information; this information must be properly handled to protect our customers and our brand.

It is important to remember that effective security is a team effort involving the participation and support of every <Company Name> employee and affiliate who deals with information and/or information systems. Therefore, it is the responsibility of each individual to know these guidelines and to conduct their activities accordingly.

Purpose and Scope

The policy will serve as the governing mandate from executive management on how information must be stored, processed, and transmitted. All entities (employees, vendors, contractors, temporary, etc) must adhere and comply with the Information Security Policy (ISP) at all times. This policy applies to all information that the company stores, creates, and processes; regardless of media, medium, or system.

Sanctions and Violations

Any entity found in violation of any part of the ISP will be subject to disciplinary action, up to and including termination. Additionally, as there are federal, state, and local laws governing information security; deliberate violations can result in criminal and/or civil legal action.

Revisions and Updating Schedule

This policy must be reviewed for applicability, effectiveness, and enforcement every 12 months. If there is found to be an error or gap in the policy, it must be immediately updated and disseminated. The policy should have a clearly noted effective date and version assignment. The person designated as the Information Security Officer will have the responsibility for review, update, and dissemination.

Date	Version	Section	Changes