**Security Policy Template**

This Information Security Policy Template is free for you to copy and use on your project

and within your organization. We hope that you find this template useful and

welcome your comments. Public distribution of this document is only permitted

from the Project Management Docs official website at:

[ProjectManagementDocs.com](http://www.projectmanagementdocs.com/)

**Security Policy**

**<Project Name>**

**Company Name**

**Street Address**

**City, State Zip Code**

**Date**

**Table of Contents**

[1. Introduction 3](#_Toc395177655)

[1.1. Purpose 3](#_Toc395177656)

[1.2. Scope 3](#_Toc395177657)

[1.3. History 3](#_Toc395177658)

[1.4. Responsibilities 4](#_Toc395177659)

[1.5. General Policy Definitions 4](#_Toc395177660)

[2. IT Assets Policy 5](#_Toc395177661)

[2.1. Purpose 5](#_Toc395177662)

[2.2. Scope 5](#_Toc395177663)

[2.3. Policy Definitions 5](#_Toc395177664)

[3. Access Control Policy 7](#_Toc395177665)

[3.1. Purpose 7](#_Toc395177666)

[3.2. Scope 7](#_Toc395177667)

[3.3. Policy Definitions 7](#_Toc395177668)

[4. Password Control Policy 8](#_Toc395177669)

[4.1. Purpose 8](#_Toc395177670)

[4.2. Scope 8](#_Toc395177671)

[4.3. Policy Definitions 8](#_Toc395177672)

[5. Email Policy 9](#_Toc395177673)

[5.1. Purpose 9](#_Toc395177674)

[5.2. Scope 10](#_Toc395177675)

[5.3. Policy Definitions 10](#_Toc395177676)

[6. Internet Policy 11](#_Toc395177677)

[6.1. Purpose 11](#_Toc395177678)

[6.2. Scope 11](#_Toc395177679)

[6.3. Policy Definitions 12](#_Toc395177680)

[7. Antivirus Policy 12](#_Toc395177681)

[7.1. Purpose 13](#_Toc395177682)

[7.2. Scope 13](#_Toc395177683)

[7.3. Policy Definitions 13](#_Toc395177684)

[8. Information Classification Policy 14](#_Toc395177685)

[8.1. Purpose 14](#_Toc395177686)

[8.2. Scope 14](#_Toc395177687)

[8.3. Policy Definitions 14](#_Toc395177688)

[9. Remote Access Policy 15](#_Toc395177689)

[9.1. Purpose 15](#_Toc395177690)

[9.2. Scope 15](#_Toc395177691)

[9.3. Policy Definitions 16](#_Toc395177692)

[10. Outsourcing Policy 16](#_Toc395177693)

[10.1. Purpose 16](#_Toc395177694)

[10.2. Scope 16](#_Toc395177695)

[10.3. Policy Definitions 17](#_Toc395177696)

[11. Annex 17](#_Toc395177697)

[11.1. Glossary 17](#_Toc395177698)

Introduction

The Information Security Policy states the types and levels of security over the information technology resources and capabilities that must be established and operated in order for those items to be considered secure. The information can be gathered in one or more documents.

You can structure policies in as many sections as you identify as valid in your organization. In the example below, sections have been selected according to best practices and our experience. You may include more sections as far as you detect more technologies in your company to be addressed with specific policies. Sections have been written all together in one document. You may as well separate them into independent policy documents for easier managing, e.g. one for Email policies, other for Internet policies and so on.

## Purpose

Specify the intention of the entire Security Policy.

This Security Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in the Organization. Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

## Scope

Define here the scope where policies in the whole document apply.

This document applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

## History

This section of the Security Policy is aimed to check the life time of a specific version of the whole document. In case you separate into several policy documents, ensure there is a version history for each one of them. Policies must be reviewed and eventually updated periodically to keep up with changes in risks, technologies and regulations.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Description** | **From** | **To** | **Author** |
| 1.0 | Initial version | 8/1/20xx | 7/1/20xx | John Doe |
|  |  |  |  |  |

## Responsibilities

Identify all the roles involved and their responsibilities in the enforcement of the policies in this document.

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| Chief Information Officer | * Accountable for all aspects of the Organization’s information security. |
| Information Security Officer | * Responsible for the security of the IT infrastructure. * Plan against security threats, vulnerabilities, and risks. * Implement and maintain Security Policy documents. * Ensure security training programs. * Ensure IT infrastructure supports Security Policies. * Respond to information security incidents. * Help in disaster recovery plans. |
| Information Owners | * Help with the security requirements for their specific area. * Determine the privileges and access rights to the resources within their areas. |
| IT Security Team | * Implements and operates IT security. * Implements the privileges and access rights to the resources. * Supports Security Policies. |
| Users | * Meet Security Policies. * Report any attempted security breaches. |

## General Policy Definitions

List here all the security policies that are global to the whole document and not belonging to a specific section. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
2. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.
3. All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.
4. Infractions of the policies in this document may lead to disciplinary actions. In some serious cases they could even led to prosecution.

# IT Assets Policy

This section of the Security Policy lists policies for the secure handling of the IT assets.

## Purpose

Specify what the intention of this policy section is.

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in the Organization.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

## Policy Definitions

List here all the IT Asset policies you have identified as necessary to regulate in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the Security Policy document.

1. IT assets must only be used in connection with the business activities they are assigned and / or authorized.
2. All the IT assets must be classified into one of the categories in the Organization’s security categories; according to the current business function they are assigned to.
3. Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
4. All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
5. Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
6. Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.
7. All personnel interacting with the IT assets must have the proper training.
8. Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.
9. Access to assets in the Organization location must be restricted and properly authorized, including those accessing remotely. Company’s laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
10. The IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
11. Special care must be taken for protecting laptops, PDAs and other portable assets from being stolen. Be aware of extreme temperatures, magnetic fields and falls.
12. When travelling by plane, portable equipment like laptops and PDAs must remain in possession of the user as hand luggage.
13. Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
14. Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the Information Security Officer.
15. Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

# Access Control Policy

This section of the Security Policy lists policies for securing access control.

## Purpose

Specify what the intention of this policy section is.

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in the Organization.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

## Policy Definitions

List here all the access control policies you have identified as necessary to regulate in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Any system that handles confidential information must be protected by a two factor -based access control system.
3. Discretionary access control list must be in place to control the access to resources for different groups of users.
4. Mandatory access controls should be in place to regulate access by process operating on behalf of users.
5. Access to resources should be granted on a per-group basis rather than on a per-user basis.
6. Access shall be granted under the principle of “less privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
7. Whenever possible, access should be granted to centrally defined and centrally managed identities.
8. Users should refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.
9. Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.

# Password Control Policy

This section of the Security Policy lists policies for securing password control.

## Purpose

Specify what the intention of this policy section is.

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in the Organization.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

## Policy Definitions

List here all the Password Control policies you have identified as necessary to regulate in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Every user must have a separate, private identity for accessing IT network services.
3. Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
4. Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
5. Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.
6. Password for some special identities will not expire. In those cases, password must be at least 15 characters long.
7. Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two set of credentials: one for administrative work and the other for common work.
8. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
9. Whenever a password is deemed compromised, it must be changed immediately.
10. For critical applications, digital certificates and multiple factor authentication using smart cards should be used whenever possible.
11. Identities must be locked if password guessing is suspected on the account.

# Email Policy

This section of the Security Policy lists policies for the secure handling of electronic mail.

## Purpose

Specify what the intention of this policy section is.

The Email Policy section defines the requirements for the proper and secure use of electronic mail in the Organization.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

## Policy Definitions

List here all the policies you have identified as necessary to regulate email in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the Organization. Occasional use of personal email address on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in the Organization system resources and the productivity of the work is not affected.
2. Use of the Organization resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the Organization business is strictly forbidden.
3. In no way may the email resources be used to reveal confidential or sensitive information from the Organization outside the authorized recipients for this information.
4. Using the email resources of the Organization for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
5. Use of the Organization email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
6. Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriated.
7. Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the Information Security Officer may approve the interception and disclosure of messages.
8. Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the company’s procedures for managing identities. Sharing of passwords is discouraged. Users should not impersonate another user.
9. Outbound messages from corporate users should have approved signatures at the foot of the message.
10. Attachments must be limited in size according to the specific procedures of the Organization. Whenever possible, restrictions should be automatically enforced.
11. Whenever possible, the use of Digital Rights technologies is encouraged for the protection of contents.
12. Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
13. Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.
14. Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management.

# Internet Policy

This section of the Security Policy lists policies for the secure access to Internet.

## Purpose

Specify what the intention of this policy section is.

The Internet Policy section defines the requirements for the proper and secure access to Internet.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

## Policy Definitions

List here all the policies you have identified as necessary to regulate Internet access in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. Limited access to Internet is permitted for all users.
2. The use of Messenger service is permitted for business purposes.
3. Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged.
4. Downloading is a privilege assigned to some users. It can be requested as a service.
5. Internet access is mainly for business purpose. –some limited personal navigation is permitted if in doing so there is no perceptible consumption of the Organization system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
6. Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
7. In accessing Internet, users must behave in a way compatible with the prestige of the Organization. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
8. Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Officer.
9. Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

# Antivirus Policy

This section of the Security Policy lists policies for the implementation of anti-virus and other forms of protection.

## Purpose

Specify what the intention of this policy section is.

The Antivirus Policy section defines the requirements for the proper implementation of antivirus and other forms of protection in the Organization.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to servers, workstations and equipment in the Organization, including portable devices like laptops and PDA that may travel outside of the Organization facilities. Some policies apply to external computers and devices accessing the resources of the Organization.

## Policy Definitions

List here all the policies you have identified as necessary to regulate the antivirus environment in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. All computers and devices with access to the Organization network must have an antivirus client installed, with real-time protection.
2. All servers and workstations owned by the Organization or permanently in use in the Organization facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to the Organization network or that can be managed via secure channels through Internet.
3. Organization’s computers permanently working in other Organization’s network may be exempted from the previous rule if required by the Security Policies of the other Organization, provided those computers will be protected too.
4. Traveling computers from the Organization that seldom connect to the Organization network may have installed an approved antivirus independently managed.
5. All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
6. Visitors computers and all computers that connect to the Organization’s network are required to stay “healthy”, i.e. with a valid, updated antivirus installed.

# Information Classification Policy

This section of the Security Policy defines a framework for the classification and use of the information according to the importance and risk.

## Purpose

Specify what the intention of this policy section is.

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the Organization information.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to all the information created, owned or managed by the Organization, including those stored in electronic or magnetic forms and those printed in paper.

## Policy Definitions

List here all the policies you have identified as necessary to regulate information classification in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. Information owners must ensure the security of their information and the systems that support it.
2. Information Security Management is responsible for ensuring the confidentiality, integrity and availability of the Organization’s assets, information, data and IT services.
3. Any breach must be reported immediately to the Information Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
4. Information in the Organization is classified according to its security impact. The current categories are: confidential, sensitive, shareable, public and private.
5. Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
6. Information defined as sensitive must be handled by a greater number of persons. It is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.
7. Information defined as shareable can be shared outside of the limits of the Organization, for those clients, organizations, regulators, etc. who acquire or should get access to it.
8. Information defined as public can be shared as public records, e.g. content published in the company’s public Web Site.
9. Information deemed as private belongs to individuals who are responsible for the maintenance and backup.
10. Information is classified jointly by the Information Security Officer and the Information Owner.

# Remote Access Policy

This section of the Security Policy lists policies for the secure remote access to the organization’s internal resources.

## Purpose

Specify what the intention of this policy section is.

The Remote Access Policy section defines the requirements for the secure remote access to the Organization’s internal resources.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to the users and devices that need access the Organization’s internal resources from remote locations.

## Policy Definitions

List here all the policies you have identified as necessary to regulate remote access in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. To gaining access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
2. Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
3. Remote access to confidential information should not be allowed. Exception to this rule may only be authorized in cases where is strictly needed.
4. Users must not connect from public computers unless the access is for viewing public content.

# Outsourcing Policy

This section of the Security Policy lists policies for the outsourcing of IT services, functions and processes.

## Purpose

Specify what the intention of this policy section is.

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes.

## Scope

Write here whom this policy is aimed to. In doing so you are facilitating the distribution of policies to the target groups of users.

This policy applies to the Organization; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

## Policy Definitions

List here all the policies you have identified as being necessary to regulate outsourcing in your organization. Formulate them in direct, understandable terms, avoiding language that can be too technical or to legal for the common user. Avoid been too specific in procedures or too attached to technology. Concentrate instead in formulating the policy itself.

You may structure the policies inside this section in subcategories if you think it contributes to the clarity of the document.

1. Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
2. Whenever possible, a bidding process should be followed to select between several service providers.
3. In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
4. Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If the Organization has not enough knowledge and resources, a specialized company should be hired to do the auditing.
5. A service contract and defined service levels must be agreed between the Organization and the service provider.
6. The service provider must get authorization from the Organization if it intends to hire a third party to support the outsourced service, function or process.

# Annex

Insert here anything you may like to attach to support the document.

## Glossary

This section of the Security Policy provides the definitions of terms, acronyms, and abbreviations required to understand this document.

| **Term** | **Definition** |
| --- | --- |
| Access Management | The process responsible for allowing users to make use of IT services, data or other assets. |
| Asset | Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service. |
| Audit | Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met. |
| Confidentiality | A security principle that requires that data should only be accessed by authorized people. |
| External Service Provider | An IT service provider that is part of a different organization from its customer. |
| Identity | A unique name that is used to identify a user, person or role. |
| Information Security Policy | The policy that governs the organization’s approach to information security management |
| Outsourcing | Using an external service provider to manage IT services. |
| Policy | Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc. |
| Risk | A possible event that could cause harm or loss, or affect the ability to achieve objectives. |
| Service Level | Measured and reported achievement against one or more service level targets. |
| Warranty | Assurance that a product or service will meet agreed requirements. |

Table 1. Glossary.

Sponsor Acceptance

Approved by the Project Sponsor:

Date:

<Project Sponsor>

<Project Sponsor Title>

This free Information Security Policy Template is brought to you by [www.ProjectManagementDocs.com](http://www.ProjectManagementDocs.com)