January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Purpose of the System Security Plan 3](#_Toc4567572)

[II. Overview of the System Security Plan 3](#_Toc4567573)

[III. Security Policy 4](#_Toc4567574)

[IV. Risk Assessment 5](#_Toc4567575)

[V. Risk Analysis 7](#_Toc4567576)

[VI. Risk Response 8](#_Toc4567577)

[Appendix A – Distribution List 9](#_Toc4567578)

[Appendix B – Receipt and Acknowledgement 10](#_Toc4567579)

# I. Purpose of the System Security Plan

The purpose of the System Security Plan (Plan) is to provide an overview of the security requirements of ABC Company’s Information Resources. This Plan also describes the controls necessary to ensure information availability, confidentiality, and integrity.

# II. Overview of the System Security Plan

The System Security Plan documents our structured process of planning adequate and cost-effective security protection. It reflects input from managers and asset owners, the IT Department, and ABC Company’s Chief Security Officer (CSO).

ABC Company’s System Security Plan leverages our existing security policies, procedures, and plans including:

* Risk Assessment
* Risk Assessment Policy
* Risk Management Policy
* Risk Task List
* Risk Treatment Plan
* Security Controls Review Policy
* Security Policy

# III. Security Policy

ABC Company’s Security Policy provides overall guidance and direction for information security and related activities.

Security plans are no longer a luxury, but an essential element of ABC Company’s risk management program. The decision to invest in security is required by legislation, third parties (e.g., insurers), and the realistic view that management must minimize the impact of security incidents on business operations.

ABC Company’s Security Policy is in place to protect ABC Company and its information assets. Risk Assessments and Risk Treatment Plans ensure that risks are identified and the appropriate mitigating technologies are in place.

An up-to-date Security Plan creates a competitive advantage out of its ability to respond to rapid changes in the environment. ABC Company can then move from simple firewalls and anti-virus solutions to experiencing the benefits associated with the continuing of business operations that are in line with the corporate strategy of facilitating growth and profitability.

# IV. Risk Assessment

ABC Company is committed to protecting its business operations, investments by its stakeholders, and assets of the organization. Risks assessments are used as a tool to help identify and mitigate risks to assets.

ABC Company management defines and selects the risk assessment methodology and approach considering internal and external risk assessment resources. A significant amount of risk assessment, planning, and knowledge of security controls is required. This ensures that the proper level of security is designed and implemented properly.

The purpose of the risk assessment is to determine areas of vulnerability and minimize risks to the organization. These risk assessments are concentrated on business processes and related assets that are of a high priority and importance to the organization.

While preparing and conducting a risk assessment, the following best practices or approaches should be considered.

A. Assets

One of the first steps is to identify important assets. This includes facilities, network infrastructure components, customer data, intellectual property, etc. Without a complete and accurate inventory of IT assets, criticality and impact on the organization cannot be determined.

Depending on the accuracy and availability of inventory documentation and asset valuation data, ABC Company may need to conduct an asset valuation or asset criticality (importance) assessment to prioritize and determine those network infrastructure components and assets that are most important to the organization.

B. Threats

Once the assets are inventories, the risk assessment identifies general and specific threats to the assets. Threats can include both unintentional and intentional threats including:

* Natural threats (acts of God)
* Accidental or unintentional threats (staff error, equipment failure, etc.)
* Intentional threats such as asset theft and asset tampering (malicious damage)

C. Vulnerabilities

Threats identify realistic events with a potential harm to the organization. The risk assessment identifies vulnerabilities or weaknesses that allow a threat to be exploited. For example, an imposter posing as an employee is a threat and related vulnerabilities can include physical access to systems, lack of employee security related education, etc.

D. Impact

Once assets, threats, and vulnerabilities are identified, the risk assessment will evaluate the potential impact or loss on our organization. Examples included the impact on our ability to perform services and meet deadlines. It also includes a negative impact on revenue, damage to our image and reputation, etc.

# V. Risk Analysis

Once the risk assessment identifies our assets, threats, and vulnerabilities, a risk analysis determines the potential impact on our organization. Each asset includes the following information:

* Asset class – major asset grouping (e.g. Information Technology).
* Asset – specific asset (e.g. Servers).
* Threat – potential to cause harm to an asset (e.g. unsecured data center)
* Vulnerability –a weakness that could be used to exploit a threat (e.g. theft)
* Impact – loss (e.g. customer data exposed results in lost revenues)

Risk reduction is the process of identifying measures and controls to safeguard against the above risks and impact on our organization. Risk reduction evaluates potential risks and safeguards:

* Physical risks - we determine the vulnerability of the data center and the impact of environmental hazards on the computer, related equipment, and contents.
* Communication risks - we evaluate the system for threats to the privacy and authenticity of telecommunications.
* Hardware - we review the system’s current or proposed hardware configurations.
* Software - we review operating and application software for security risks and potential vulnerabilities.
* Personnel - we describe staffing and third-party risks and potential vulnerabilities.

We then identify various risk treatment safeguards and controls for appropriateness, cost efficiency, and effectiveness. Risk reduction strategies include safeguards and controls to:

* Mitigate – implement controls to reduce risks to an acceptable level
* Transfer – transfer risks to another entity
* Eliminate – change the business model to avoid or eliminate the risk if the risk cannot be reduced to an acceptable level or transferred to another entity
* Monitor – acknowledge the risk and monitor to ensure the risk remains within acceptable limits

# VI. Risk Response

In most instances, ABC Company reduces risks through the use of mitigating controls and safeguards. For each applicable risk, we implement safeguards to enhance the effectiveness of our controls to prevent and minimize the threat or vulnerability. In some instances, insurance transfers the risk to an outside entity.

It should be noted that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk.

A separate Risk Treatment Plan describes how we manage risks. It defines roles and responsibilities for participants in the risk processes, the risk reduction activities, the schedule for risk management activities, and any techniques used.

The Risk Treatment Plan is updated on an on-going basis as tasks are completed and new risks are identified. The Risk Treatment Plan identifies how the Risk Task List is maintained and risk resolution status is reported to management.

# Appendix A – Distribution List

President

Chief Operating Officer

IT Director

IT security Staff

Chief Security Officer

# Appendix B – Receipt and Acknowledgement

I have read ABC Company’s (Company’s) System Security Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (Printed)