SAMPLE: Copyright 2016 Imprimis, Inc.

Company XYZ

System Security Plan

Full templates available at ...
www.i2ComplianceTools .com

Company XYZ
9-15-2016

Copyright © 2016 by Company XYZ
All rights reserved.

This document may be internally used by the purchaser for the creation and maintenance of an internal system security plan.

No portions of this document may be distributed or used in any other than the intended manner without the express written permission of Company XYZ

SAMPLE: Copyright 2016 Imprimis, Inc.

Version Control

Date	Author	Version

Contents

SAMPLE: Copyright 2016 Imprimis, Inc.

SAMPLE: Copyright 2016 Imprimis, Inc.

1.0 Introduction

This System Security Plan (SSP) provides an overview of the security requirements for the XYZ Network and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the XYZ system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the XYZ information systems (IS).

The security safeguards implemented for the XYZ systems meet the policy and control requirements set forth in this SSP. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

This SSP shall be reviewed and updated at last annually based on changes to organizational and system risks, system structure, and company policies and procedures.

2.0 System Description and Characterization

Provide a name, status, and primary responsible parties for the system in question. It is important to properly scope the network in question and define the boundaries to it. The system covered in this SSP may be the entirety of all networks the company possesses, or it may be a very specific portion of the network with specific ownership, data sensitivity, or connectivity. Ensure that the boundaries of the system are clearly defined and understood.

It is often prudent to have a hierarchy of SSPs, one for the primary network infrastructure, then many additional SSPs for individual enclaves or systems that have unique security requirements or configurations.

System Name: The system name is the XYZ Network
System Status: XYZ Network is operational

The following is contact information for XYZ Network System Steward and Approval Authority:

Table 1: System Steward and Approval Authority

	System Steward	Approval Authority
Name	Joe IT	Head Honcho
Title	IT Manager	CIO
Address		
Phone		
E-mail		

2.1 General Description / Purpose

Describe the system composition, primary use, types of data processes, and explanation of diagrams

Provide detailed system diagrams at Appendix A. For a network of any complexity, this may require several diagrams with different levels of detail and, possibly, different focus. For example, you might have one top-level

diagram and then several detailing subordinate portions of the network. You might also have some diagrams that depict a logical view of the network while others provide a more physical/technical view. Attach as many diagrams as are necessary to properly depict the system in Appendix A and explain briefly here.

The XYZ network supports all administrative and operational functions of Company XYZ and is essential to business operations. The diagrams in Appendix A convey the general structure and content of the XYZ network.

The first diagram is the top-level, inter-site connectivity diagram. It depicts the multiple locations (A, B, and C) with nodes of the XYZ network and conveys some aspects of the connectivity between sites.

The subsequent 6 diagrams (AL, AP, BL, BP, CL, and CP) provide logical and physical views of the networks at sites A, B, and C respectively.

2.2 System Interconnection / Information Sharing

Describe permanent or intermittent interconnections with other internal/external systems.
Provide detailed interconnection diagrams at Appendix B and explain here. The explanation should include a discussion of how these connections are limited or secured. Describe major flows of information to/from other systems. The diagrams and descriptions should include connections to cloud services.

As shown in Appendix B, XYZ Network has several defined system interconnections. These are listed in Table 2.

Table 2: System Interconnection/Information Sharing

System Name	Responsible Organization	Type (e.g.,TCP/IP)	SLA / MOU / MOA	Date	Approving Authority
Network Z	**Company Z**	**IP VPN**	**MOU**	**15 Jun 15**	**CIO Yanis**
Q Network	**Company Q**	**IP VPN**	**MOA**	**14 Dec 14**	**CIO Xerxes**

The Network Z connection is permanently active and allows Company Z contractors, working in Company XYZ's facilities to connect directly to Network Z to access mandatory company services and proprietary information. The connection is controlled in a secure VPN and can only be accessed from Company Z-owned equipment. All Network Z users within Company XYZ's facilities are also recognized users of the XYZ Network, and are regularly trained on its security requirements.

The Q Network connection specifically supports the Quip project and is only activated during specified project phases (development, testing, fielding, etc.). The Quip project manager is responsible for direction, activation, and termination of the connection. The VPN connection allows several IP-specified servers to share data with several other IP-specified servers within Company Q's facilities to support the joint development and maintenance of Quip-related systems.

2.3 System Dependencies / Inheritance

List system specific dependencies. A dependency is a telecommunication or information technology interconnection or resource on which the system under review relies for processing, transport, or storage. The relationship between

SAMPLE: Copyright 2016 Imprimis, Inc.

the system in question and the dependencies can directly affect the confidentiality, integrity, or availability of the system or its data. Whenever a system has a dependency, the system inherits the intrinsic risks of the dependent asset.

Inheritance is an important concept, especially with a large, complex network. As noted above, in a complex network, it is often best to have a hierarchy of SSPs with a clear demarcation between them. If done properly, subordinate systems can then inherit many of the security controls of the systems on which they reside. For instance you might have an SSP for the overall administrative network and then have SSPs for specialized systems supporting Human Resources, Engineering, etc. These latter SSPs might be able to inherit a lot from the administrative network SSP.

XYZ Network uses ISP X for external connectivity. As noted in Appendix A, ISP X maintains at least one access point in each XYZ facility. ISP X access to these access points is coordinated by the IT Department and all ISP X personnel are escorted during access. ISP X services are detailed in the 15 Apr 15 ISP X SLA, on file with the Contracts Department.

Company XYZ uses MegaCloud for cloud storage and processing. It is accessed via a secure Web Login with a connection that will terminate after several hours of non-use. The Megacloud SLA was negotiated to ensure that data in MegaCloud is protected at a level at least on par with that in XYZ Network. Details of MegaCloud service and security are detailed in the 16 Mar 16 MegaCloud SLA, on file with the Contracts Department.

2.4 System Inventory

In order for an organization to effectively defend their IS, they must first kn
must have an inventory of IS components. Such an inventory allows t
devices are given access and that unauthorized devices attemptin
Similarly, an inventory of authorized software allows the organiza
unauthorized software and dramatically reduces options for att
IS (including hardware and software) is recommended and is
standards. Such an inventory also often supports various

As with the system diagrams discussed in Section 2.1, IS
differing levels of detail. Attach inventories at Appendix

Company XYZ tracks IS inventory using locally develo
hardware components authorized to connect to the n

3.0 Governance

Provide an overview of the personnel and orgar
the development, approval, operations, or ma

Following are primary system securit
cyber policies. This

SAMPLE: Copyright 2016 Imprimis, Inc.