System/Network Security Plan Template

(derived from template used by the U.S. Department of Defense for Classified Systems)

Bar Biszick-Lockwood, cisa, cissp, csqa

QualityIT

DOCUMENT HISTORY

Revision:

Date Revised:

Filename:

Path hyperlink

Revision History

Author	Date	Comments

Responsible Parties

Name	Email

Other Interested Parties

Document Overview

This document describes the scope and approach, and resources required to assure the security of the {system name} system. Maintenance of this document is the sole responsibility of {enter title/division} The execution of the guidelines included herein are the responsibility of {list the titles/divisions of all responsible parties} The testing, certification and inspection of this system and its component parts is the sole responsibility of {name the test group and auditing division}.

Standards Compliance: This system achieves corporate security standards and complies with all relevant corporate and industry security policies unless otherwise specified.

System Purpose: The purpose of this application is to {high level description}

System Boundaries: {Describe the boundaries of the system and all components contained within it, or on which it is dependent, whose security requirements will be addressed in this document}

Scope Limitations: This Security Plan addresses only {describe the boundaries addressed in this document.}

SYSTEM SECURITY PLAN

1. OVERVIEW

System Security Plans are prepared by [unit/department name] as the basic system Security document and as evidence that the proposed system, or update to the existing system, meets the appropriate company Security Program requirements. This System Security Plan is used throughout the certification and accreditation process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The System Security Plan also serves as the basis for inspections of the system. Each system owner shall maintain the copy of record of the System Security Plan and associated documents for each system or network component under their control. Each Network Administrator shall (at a minimum) maintain a current list of the secure systems on his/her site or facility. A separate, designated authority [Data Architecture Administrator] will maintain accreditation documentation for each of the secure system he/she has accredited.

Each component contained by the system that processes company information such as a standalone mainframe, minicomputer, personal workstation, Unified Network, or Interconnected Network, will be covered by a separate Security Plan. Two or more similar plans may be combined under a consolidated Security Plan document.

Note: If a Security Plan is determined to contain classified information, the plan shall be appropriately marked and protected.

2. DEFINITIONS

For the purposes of this document, the following definitions will be used

- System Definition {describe in detail the component parts of the system, their relevance to the system and any extra system dependencies that must be considered in the plan}
- {Enter any other definitions that would not be commonly known to a member of the Company’s legal department or Business management}

3. ASSUMPTIONS

Describe known risks and assumptions.

4. COMMON DOCUMENTS

Information common to several systems or networks will be available at a common site or information contained in other documents may be attached to or referenced in the Security Plan.

5. SYSTEM SECURITY DOCUMENT

The Security Plan formally documents the operation of this system, and the measures that are used to control access and protect the protected system and its information. To make appropriate accreditation decisions, responsible parties need to understand the complete classified environment. Therefore, at a minimum, this Security Plan will contain the following information:

A. Introduction.

1) The identification and location of the system/network.
2) A brief narrative description of the system/network including its mission or purpose.

B. Security Requirements Specification

The Security Requirements Specification is a unique sub-set of the Security Plan that defines the secure operating environment of this system. A schematic diagram of the system should be attached. The Security Requirements Specification will be developed as an attachment to the Classified Security Plan for use if the classified system is to become part of an interconnected network. If at any time it is necessary or desirable to link a classified into a network, the information in the Security Requirements Specification will be used to determine any necessary changes in or additions to protections or countermeasures.

Security Personnel

The name, location, and contact information of the responsible System Owner, Architect, Administrator, Maintenance Facilitator and the Data/ Application Owner (if appropriate),including emergency contact numbers.

Secure Operating Environment

Brief description of the secure operating environment of the system.

Data Sensitivity Classification

(i.e., Internal Only, Confidential, Sensitive, Private Customer) and categories (i.e., Restricted Data, Formerly Restricted Data, etc.) of the data, and the percentages of each, to be processed, stored, transferred, or accessed;

Highly Sensitive or Unclassified data

Cite the presence of highly sensitive or unclassified data, and provide the physical system location by drive/file. Include the Security classification for each level of data on the system. (e.g., Privacy, Proprietary, Unclassified, Controlled, etc.) as required.

External system dependencies

Describe any special access programs required to access the data and reference them as defined in other technical or administrative documents

Access authorization

(e.g., Access to Special Access Programs);

Special handling instructions or caveats

(e.g., NO CONTRACT, WNINTEL);

Need to Know Policy

Information sharing restrictions on all persons connected with the development, maintenance, architecture, administration and use of the system, or system directly connected to the system.

Personnel Security.

State the range of security clearance levels, the set of formal access approvals, and the need-to-know status of users.

Mode of operation/Protection index

if system security levels have been pre-defined.

Physical Protection

The documentation of any special physical protection requirements unique to the system.

Security Contracts

A copy of any security contracts (memoranda of understanding, emails or other tangible proofs) with other persons, departments, companies or external entities and a list of all security contracts associated with the system.

Approved Waivers, Variances and Exceptions

A descriptive list and a copy of the approval documentation of any approved waivers, variances, or exceptions.

Special Security Countermeasures

The details of any special security countermeasures in use on the system, or externally imposed on the system.

System Description Details

A brief description of the system including all hardware components, showing the organization, interconnections, and interfaces of these components (block diagrams may be used to satisfy this requirement).

Configuration Management Program.

A brief description of, or reference to, the Configuration Management Program used for the system.

Identified Risks and Vulnerabilities.

- ***An itemized list of Identified vulnerabilities***

  A statement about the risk assessment of any unique vulnerabilities or threats to the system will document or reference threats unique to the site, the information, or threats unique to the classified itself.

If there are no unique threats or vulnerabilities, a statement to that effect will be entered.

- ***Mitigating Countermeasures***

Another statement will document will describe the countermeasures that will be used to mitigate identified vulnerabilities.

C. Security Policy Compliance

A description of how company Security requirements have been met will be provided. This description will specifically address:

Personnel Security.

Describe, attach, or reference the personnel procedures implemented.

Physical Security.

Provide a brief description of the physical security environment, e.g., type of Security Area, minimum security clearance level allowed (reference any Site Safeguards and or other Security Plan.

Telecommunications Security

Include or reference any Protected Distribution System documentation and its provisions.

Administrative Security

Describe or reference procedures for administration, if passwords are used for authentication of system access control.

Password Security

Describe the protection requirements and procedures for all authenticators including passwords.

Scavenging Security

Describe or reference procedures to protect against scavenging.

Hardening Methods

Describe the tools and techniques that will be used to insure risk to the system is minimized.

Privacy Protection Approach

Describe the methods and procedures used to sanitize the system between user sessions and when changes to user access levels are made.

Site Markings/Naming Conventions

Describe or reference the site marking procedures, and naming conventions used.

Technical Security

a. Describe or reference the auditing procedures to be followed

b. Describe the Shut down procedures when a failure of the real time auditing capability is detected.

c. Define the time lockout interval of inactivity in interactive sessions

d. Describe the restart requirements

Evaluated Product Dependencies

List products or justification for alternatives methods, hardware, or software.

Certification Process

Describe the application software certification process including most recent historical trending and security test results.

Waste, fraud and abuse protection

Describe the management controls established to deter and detect waste, fraud, and abuse.

Network Requirements

If the classified is implemented as a network, the Classified Security Plan will also address the following items:

(a) Overview of the Network.

(b) Include descriptions of the sub-networks, servers, hosts.

(c) Communications Protocols

(d) Briefly describe all protocols used in the network.

Security Support Structure

Briefly describe the Security Support Structure including all controlled interfaces and guards, their interconnection criteria, and their security requirements. Also, describe any encryption methods used to provide discretionary/nondiscretionary controls and the communications security devices that protect intranetwork communications.

Security Policies

Describe or reference the network security policies and procedures. If referenced, include a brief synopsis of the referenced policies and procedures, including:

(a) Network Access control policies.

(b) Network Authorization and authentication policies.

Network Audit policies

Describe the audit policies that will be applied, including the schedule for test certification and auditing inspections.

Remote Maintenance/Diagnostics

If approved remote diagnostic or maintenance services are to be used, specify the methods of connection, disconnection, and security measures.

Performance Test Plan

Describe the plan for ongoing security performance testing and the frequency of such testing.

Security Incident Reporting

Attach or reference the procedures to be used by the personnel for reporting any Security incidents to appropriate management. These procedures will include the actions to be taken to secure during reporting of a security-related incident, and how the incident information will be maintained for post-incident analysis purposes.

Continuity of Operations

Describe the Continuity of Operations Plan, if available.

- If the decision was made to have a continuity of operations plan, reference the plan, and include a short abstract of the plan. Include the documentation of the frequency and cost to exercise the plan, any approval documentation, and provide or reference a list of the applications on the system that require a continuity of operations plan.
- In the absence of a Continuity of Operations Plan, describe the process used to protect the current backup copies of software, data, applications, and the documentation judged to be essential to the continued operation of the system.

Potential Addendum Attachments:

- ***System Graphic***
- ***Emergency Contact List***
- ***Position in Network Graphic***
- ***Network Security Policy***
- ***Schedule of Performance Certification Testing & Results***
- ***Schedule of Audit Inspections & Results***
- ***Enterprise Interconnected Systems Security Plan***

A Network operating as part of an Enterprise Interconnected networks system, the Enterprise Network Security Plan should be referenced in the System Security Plan. Relevant references should include:

(a) Designates the individuals responsible for the secure operation of the Interconnected Network;

(b) Describe the secure operating environment and protections of the Network Security Support Structure including a description of the operation of any Controlled Interfaces;

(c) Identify any special security responsibilities of the users of the Interconnected Network

(d) Lists the networks (Interconnected or Unified) and systems that comprise the Interconnected Network

(e) Include a copy of the Security Contract for each separately accredited network or and a copy of their relevant Security Requirements Specifications, provided as attachments.