Your Logo
Will Be
Placed Here

SYSTEM SECURITY PLAN (SSP)

ACME Business Consulting, LLC

SCOPING:

- **Name of System**: [name of contractor's internal, unclassified information system the SSP addresses]
- **DUNS #**: [contractor's DUNS #]
- **Contract #**: [contractor's contract # or other type of agreement description]
- **CAGE Code #**: [contractors CAGE code #]

DISTRIBUTION: [list who this SSP is distributed to (e.g., contracting official, prime contractors, etc.)]

REVISION DATE: [list the date of the last revision]

SSP
System Security Plan

Table of Contents

INSTRUCTION ON FILLING OUT THE SSP TEMPLATE

It is important to understand that there is no officially-sanctioned format for a System Security Plan (SSP) to meet NIST 800-171 compliance requirements. This template is based on SSP requirements that are used for other US government compliance requirements for SSPs, but it is tailored to document the entire Controlled Unclassified Information (CUI) environment for an organization.

A key concept to keep in mind with the SSP is that it should be complete enough for a reasonable person to pick up, read through and understand the following information:

- What CUI is in regards to the company's operations.
- Where CUI is stored, transmitted or processed.
- What controls are in place to protect CUI as it is stored, transmitted and processed.
- Any deficiencies that exist in protecting CUI, if applicable.
- Remediation plans address known deficiencies, if applicable.

Steps to fill out the SSP include:

- ✓ Step 1 – Read through the SSP template to get an understanding of the content required to fill out the template.
- ✓ Step 2 – Start filling out the information you have available, using the examples as guidance, where applicable.
- ✓ Step 3 – Work with stakeholders to fill in missing information.
- ✓ Step 4 – Work through Annex 1 to provide evidence of how each of the applicable CUI and Non-Federal Organization (NFO) controls are being addressed.
- ✓ Step 5 – For any CUI or NFO control that is not addressed, add an entry in the accompanying Plan of Action & Milestones (POA&M) template

Documentation Notes:

- Text in BLACK are standard template text that are expected to be included in the SSP and should not be deleted unless necessary.
- Text in RED are helpful instructions that need to be deleted as sections are completed.
- Text in BLUE are examples that need to be deleted as sections are completed.

PREPARED BY

[Name]
[Email Address]
[Phone #]
[Department]

REVISION HISTORY

Version	Date	Pages Affected	Description
1.0	TBD	All	Initial publish of SSP.

OWNERSHIP & CYBERSECURITY OVERVIEW

The objective of the System Security Plan (SSP) document is to have a simple, easy-to-reference document that covers pertinent information about the Controlled Unclassified Information (CUI) environment. This is a "living document" that is meant to be updated as conditions change.

The goal of this document is simple - anyone not familiar with the CUI environment should be able to read it and gain a fundamental understanding of the systems involved, the risks, and the security controls required to maintain an acceptable level of security.

Essentially, this document provides a centralized repository for knowledge that is specific to the CUI environment and its applicable security controls. The SSP reflects input from those responsible for the systems that make up the CUI environment, including information owners, system operators, and other stakeholders.

CONTRACTS CONTAINING CUI

[list the applicable contracts that contain CUI protection requirements]

SYSTEM IDENTIFICATION - CUI OVERVIEW

[provide a descriptive narrative of how CUI is defined by the applicable contract(s). Include a description of the function/purpose of the internal unclassified information system(s)/network(s) that is(are) addressed in the plan.]

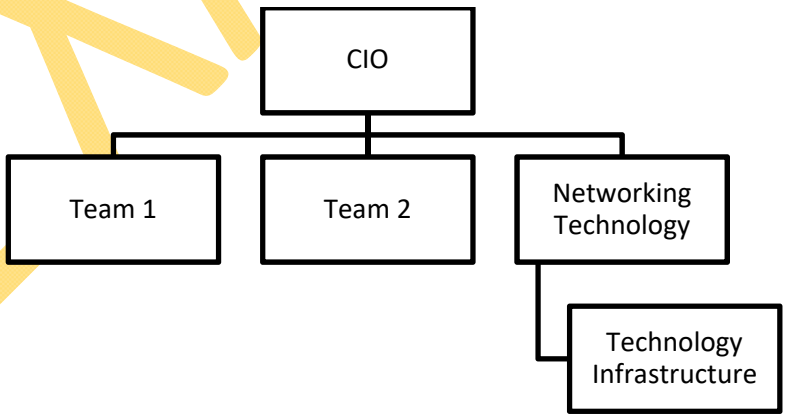
Example:
Contract XXXXXX defines CUI as schematic diagrams that are pertinent to the XYZ project.

KEY STAKEHOLDERS

CUI protection is a combined effort from the following stakeholders:

- Stakeholder 1, Position
- Stakeholder 2, Position
- Stakeholder 3, Position

Example:
It is sometimes worthwhile to include an organization chart, since this can assist with problem escalations.



Documentation Repository

Information security-related project and system documentation can be found at:

[add URL for network share, etc.]

Data Protection Considerations

The assets within the CUI environment are assessed, based on data sensitivity and mission criticality, in order to ensure the appropriate level of protection is applied.

Appendix A (Data Protection Considerations) provides the methodology for how data is classified in terms of data sensitivity and criticality to the CUI environment.

Additional Compliance Requirements

In addition to CUI protection requirements from the Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012), the following compliance requirements are also applicable, due to overlapping requirements for cybersecurity and privacy controls:

Statutory Requirements

[fill-in applicable statutory requirements]

Example statutory requirements include:

- *Cable Communications Policy Act (CCPA)*
- *Children's Internet Protection Act (CIPA)*
- *Children's Online Privacy Protection Act (COPPA)*
- *Computer Fraud and Abuse Act (CFAA)*
- *Consumer Credit Reporting Reform Act (CCRRA)*
- *Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)*
- *Electronic Communications Privacy Act (ECPA)*
- *Electronic Freedom of Information Act (E-FOIA)*
- *Electronic Funds Transfer Act (EFTA)*
- *Fair & Accurate Credit Transactions Act (FACTA)*
- *Fair Credit Reporting Act (FCRA)*
- *Family Education Rights and Privacy Act (FERPA)*
- *Federal Information Security Management Act (FISMA)*
- *Federal Trade Commission Act (FTCA)*
- *Gramm Leach Bliley Act (GLBA)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Privacy Act*
- *Right to Financial Privacy Act (RFPA)*
- *Sarbanes Oxley Act (SOX)*
- *Telecommunications Act*
- *Telephone Consumer Protection Act (TCPA)*
- *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)*
- *Video Privacy Protection Act (VPPA)*
- *US State - Massachusetts 201 CMR 17.00*
- *US State - Oregon Identity Theft Protection Act (ORS 646A)*
- *International - United Kingdom Data Protection Act (UK DPA)*

Regulatory Requirements

[fill-in applicable regulatory requirements]

Example regulatory requirements include:

- *Federal Acquisition Regulation (FAR 52.204-21)*
- *European Union General Data Protection Regulation (EU GDPR)*

System Environment

This section contains a detailed topology narrative and graphic shall that clearly depicts the system environment, including system boundaries, system interconnections, and key components.

Instruction: This does not require depicting every device, but would include an instance of operating systems in use, virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations, firewalls, routers, switches, copiers, printers, lab equipment, etc. If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram. Include or reference (e.g., to an inventory database or spreadsheet) a complete hardware and software inventory, including make/model/version and maintenance responsibility.

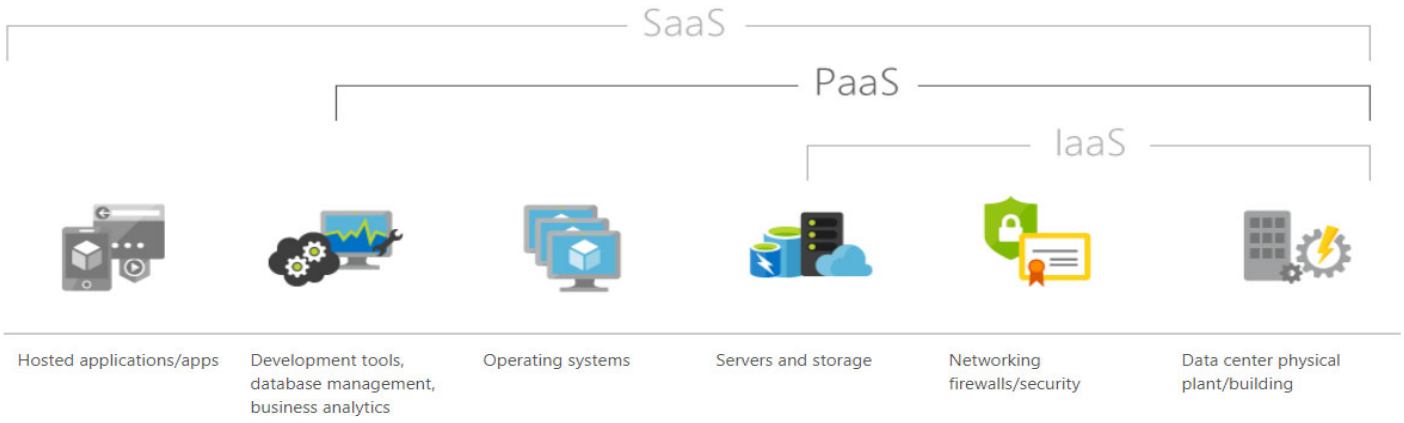
Delete this and all other instructions from your final version of this document.

Operating Model

Operating Environment Where CUI Exists (check all that apply)		
☐	Public Cloud	Cloud services and infrastructure supporting multiple organizations and clients
☐	Private Cloud	Cloud services and infrastructure dedicated to a specific organization and no other clients
☐	Data Center	Company-owned & operated datacenter.
☐	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data)
☐	Dispersed Endpoints	CUI can be found on workstations and other endpoints.
☐	Other	Explain:

High-Level Overview of Where CUI Is Stored, Transmitted or Processed (check all that apply)		
☐	End User Workstations	End user workstations (e.g., desktops & laptops)
☐	Mobile Devices	Mobile devices (e.g., tablets or smartphones)
☐	Industrial Control System (ICS)	Devices that control manufacturing processes
☐	Internal application/service	Internal application (e.g., ERM, SAP, ticket system, change control, etc.)
☐	Software as a Service (SaaS)	Web-based applications (e.g., Google Apps, Salesforce, GoToMeeting, WebEx)
☐	Platform as a Service (PaaS)	Web-based major applications (e.g., Azure Cloud Services)
☐	Infrastructure as a Service (IaaS)	Cloud environments (e.g., Azure, AWS, Rackspace)
☐	Other	Explain:

Example:



Interconnectivity Overview

[provide a descriptive narrative how systems within the CUI environment communicate – is it internal only? Does it communicate outside of the company's network?]

Appendix B (Hardware and Software Inventory), provides a breakdown of assets that comprise the CUI environment in both the production and development instances.

Appendix C (Interconnectivity Documentation), provides a detailed description of ports, protocols and services, in use within the CUI environment.

Identification & Authentication Overview

[provide a descriptive narrative of how the system handles identification & authentication]

Example:
Vendor accounts will be created in the ACME instance and pushed to the XXXXX instance. Only one account per vendor will be allowed. The vendor account will be inactivated when the vendor submits their documentation.

The two instances of XXXXX will use different methods for user identification and authentication, since the XXXXX-hosted instance will be externally accessible to vendors.

ACME Instance

- *User Names: AD integration*
- *Passwords: AD integration*
- *Account Reviews: Tied into AD*
- *Account Deactivation: Tied into AD*

XXXXX Instance

- *User Names:*
  - *ACME Users: Ping Federate (AD integration)*
  - *Non-ACME Users: Local XXXXX account (hosted instance only)*
- *Passwords:*
  - *ACME Users: Ping Federate (AD integration)*
  - *Non-ACME Users: TBD*
- *Account Reviews:*
  - *ACME Users: Ping Federate (AD integration)*
  - *Non-ACME Users: TBD*
- *Account Deactivation: Tied into AD*
  - *ACME Users: Ping Federate (AD integration)*
  - *Non-ACME Users: TBD*

System Components & Network Boundaries

[provide a descriptive narrative of what makes up the CUI operating environment, including defining the assets involved and the system boundaries]

Example:
XYZ is designed with two distinct instances, running in two different environments:

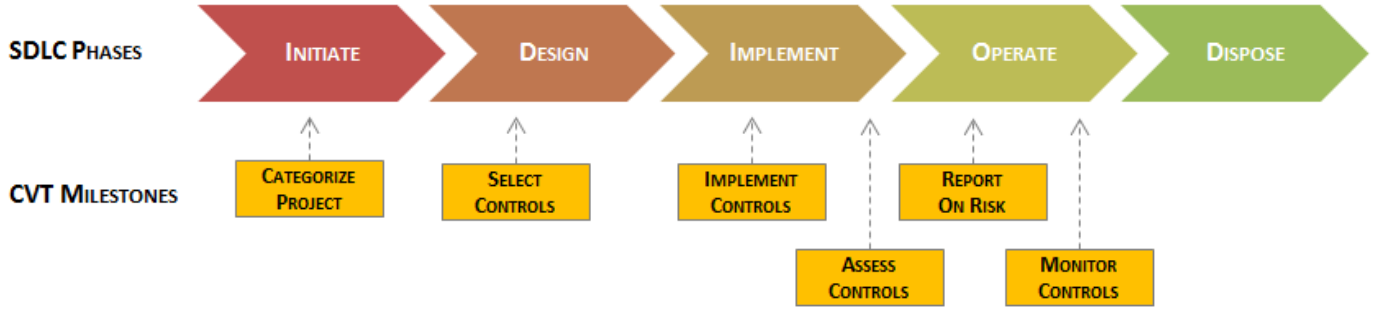
- *Internal XXXXX instance that is housed in ACME's datacenter (Datacenter 1); and*
- *Hosted XXXXX instance in Microsoft's Azure private cloud.*

OPERATIONAL PHASE

The CUI environment is currently:

Operational Status		
☐	Operational	CUI is being used by systems in a production environment.
☐	Under Development	CUI is being used by systems in a developmental / testing environment.
☐	Major Modification	CUI systems are undergoing a major change, development, or transition.
☐	Other	Explain:

The dates planned and dates reached for each phase of the System Development Lifecycle (SDLC) and Control Validation Testing (CVT) milestones:



Traditional SDLC Phase	Date Planned	Date Reached
Initiate	?	?
Develop / Design / Acquire	?	?
Implement	?	?
Operate & Maintain	?	?
Dispose	?	?

MILESTONES

[Enter a narrative about the planned milestones planned for the life of the systems that make up the CUI environment]

Example:
XYZ is currently in the operate phase. Updates and changes to XYZ is expected throughout the fiscal year. There are currently no envisioned alterations to XYZ that would severely affect its operational status during updates and changes to the system environment. XYZ will be undergoing major modification during the course of FY2018, including network engineering, security engineering, and systems engineering

INSTRUCTIONS: All milestones about operational status should be stated. If the system is about to go through a major revision, all milestones along the way should be listed as well.

Delete this and all other instructions from your final version of this document.

ANNEX 1 – SECURITY REQUIREMENTS (NIST 800-171 CUI & NFO CONTROLS)

The SSP consists of the applicable NIST 800-53 rev4 controls, as mapped in Appendix D (CUI controls) and Appendix E (NFO controls) of NIST 800-171 rev1.

NIST 800-171 APPENDIX D - 3.1 ACCESS CONTROL

These controls are associated with access control:

3.1.1 LIMIT SYSTEM ACCESS TO AUTHORIZED USERS, PROCESSES ACTING ON BEHALF OF AUTHORIZED USERS, OR DEVICES (INCLUDING OTHER SYSTEMS).
3.1.2 LIMIT SYSTEM ACCESS TO THE TYPES OF TRANSACTIONS AND FUNCTIONS THAT AUTHORIZED USERS ARE PERMITTED TO EXECUTE.

AC-2 ACCOUNT MANAGEMENT

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

AC-3 ACCESS ENFORCEMENT

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation:

Summary of Control Implementation
[describe the solution and how it is implemented]

AC-17 Remote Access

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

3.1.3 Control the flow of CUI in accordance with approved authorizations.

AC-4 Information Flow Enforcement

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

AC-5 Separation of Duties

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

AC-6 Least Privilege

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

AC-6(1) Least Privilege | Authorize Access To Security Functions

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled)

Summary of Control Implementation
☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

AC-6(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: [describe the solution and how it is implemented]

3.1.6 USE NON-PRIVILEGED ACCOUNTS OR ROLES WHEN ACCESSING NON-SECURITY FUNCTIONS.

AC-6(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS

Summary of Control Implementation
Implementation Status (check all that apply): ☐ Implemented (internally controlled) ☐ Implemented (outsourced execution of control) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)*