YOUR LOGO GOES HERE

SYSTEM SECURITY PLAN (SSP)

NIST 800-171 R2 / CMMC 2.0

ACME Consultants, LLP

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 #**: [contractor's 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]

SENSITIVE

Access Limited to Authorized Personnel

Table of Contents

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.

GENERAL DESCRIPTION / PURPOSE

[provide a high-level description of the purpose of the system/application/service that is in scope]

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.]

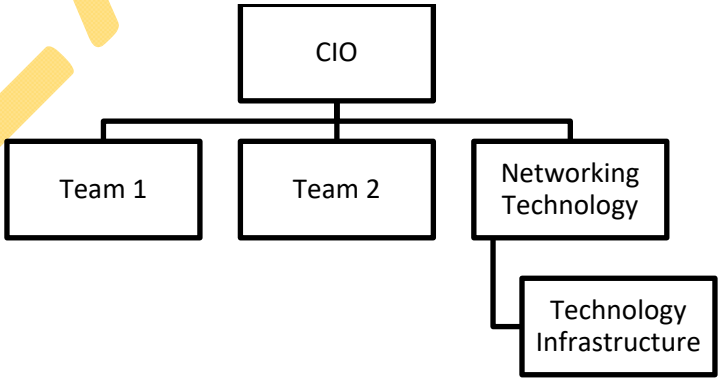
Example:
Contract XXXXXX defines CUI as schematic diagrams that are pertinent to the XYZ project.

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)*

- *Financial Industry Regulatory Authority (FINRA)*
- *National Industrial Security Program Operating Manual (NISPOM)*
- *Department of Defense Information Assurance Risk Management Framework (DIARMF) (DoDI 8510.01)*
- *Federal Risk and Authorization Management Program (FedRAMP)*
- *New York Department of Financial Services (NY DFS) 23 NYCCRR 500*
- *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)*

CONTRACTUAL REQUIREMENTS

[fill-in applicable contractual requirements]

Example contractual requirements include:

- *Payment Card Industry Data Security Standard (PCI DSS)*
- *Generally Accepted Privacy Principles (GAPP)*
- *American Institute of CPAs Service Organization Control (AICPA SOC2)*
- *Center for Internet Security Critical Security Controls (CIS CSC)*
- *Cloud Security Alliance Cloud Controls Matrix (CSA CCM)*

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.

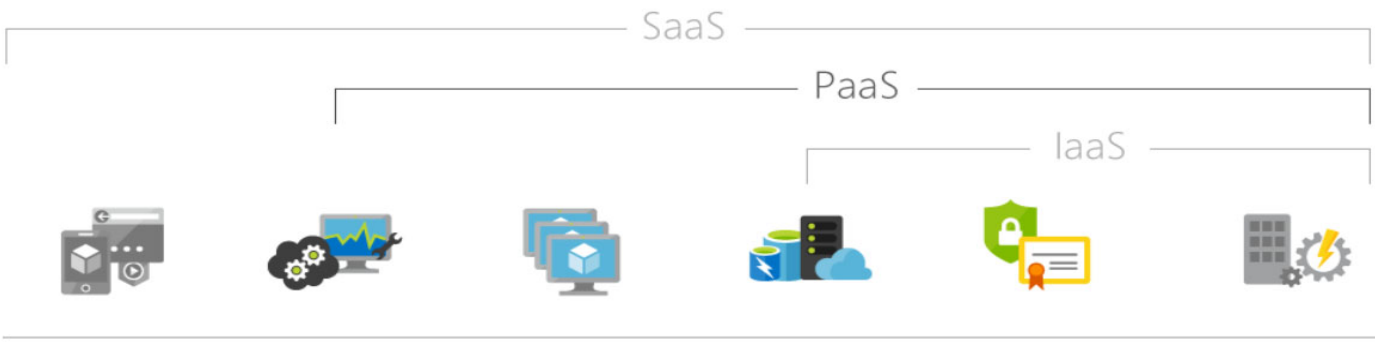
Delete this and all other instructions from your final version of this document.

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]
[describe how many users are involved. Also describe how many administrators are involved]

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

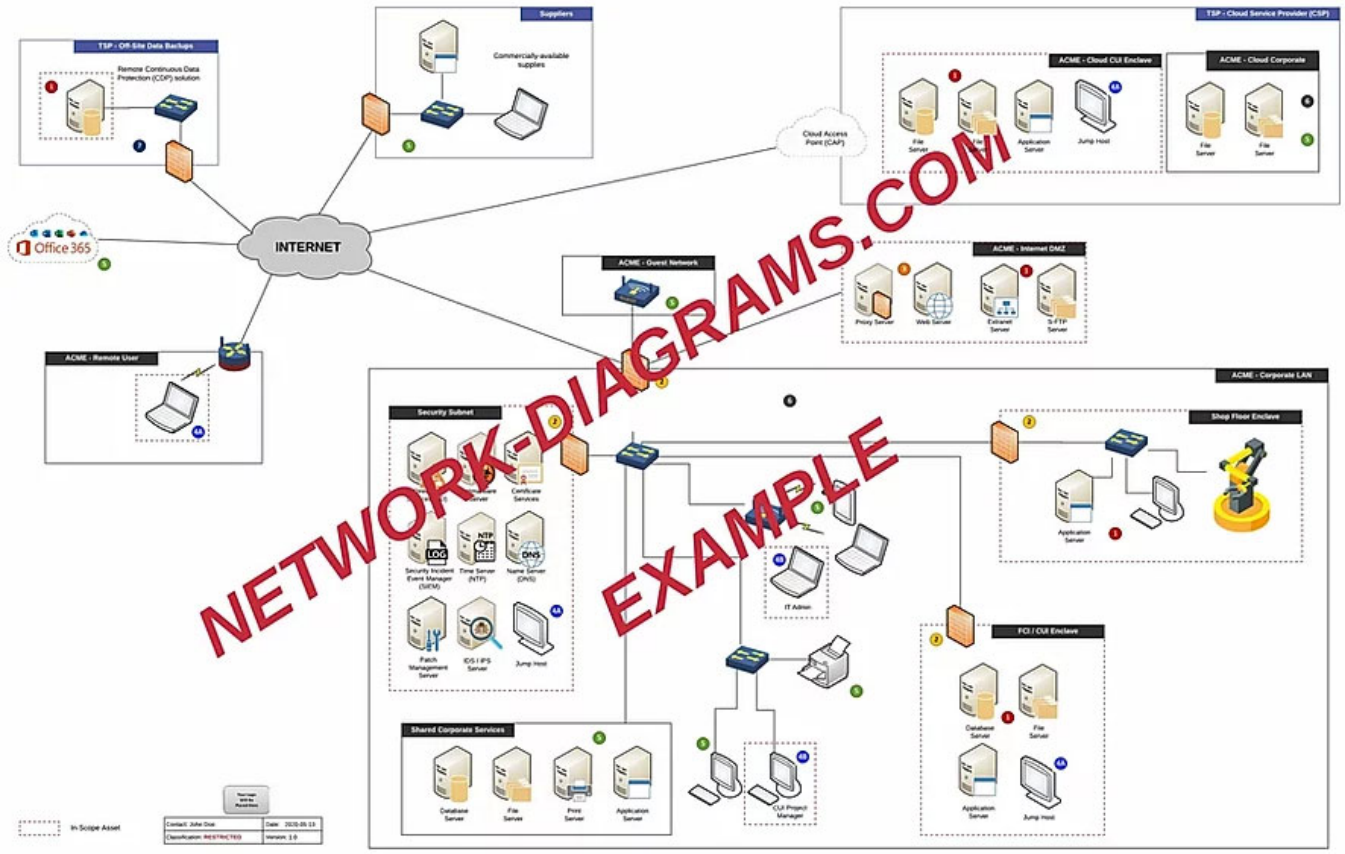
[provide a descriptive narrative of what makes up the CUI operating environment, including defining the assets involved and the system boundaries]

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.*

HIGH-LEVEL NETWORK DIAGRAM

[add network diagram here - if you do not have a network diagram, you can work with https://www.network-diagrams.comto obtain a quality network diagram and data flow diagram for your CUI environment (see below for an example)]



Instruction: Useful tools to create a high-level network diagram include:
- Microsoft Visio (network diagram templates) or
- Department of Homeland Security's free tool, the Cyber Security Evaluation Tool (CSET) -
https://www.cisa.gov/downloading-and-installing-cset

Provide a diagram that portrays the system boundaries and all applicable connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system.

Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

Formal names of components as they are known by the project team in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions
If necessary, include multiple network diagrams.

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

DATA FLOW DIAGRAM

[add data flow diagram here]

Instruction: Useful tools to create a data flow diagram include:
- Microsoft Visio (network diagram templates) or
- Department of Homeland Security's free tool, the Cyber Security Evaluation Tool (CSET) - https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf

In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. If necessary, include multiple data flow diagrams.

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

ROLES & PRIVILEGES

Cybersecurity roles and responsibilities are based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, as described in NIST Special Publication 800-181. Appendix F (Cybersecurity Roles and Responsibilities)lists the types of roles and responsibilities that are applicable to the CUI environment.

[specific to handling CUI, identify the roles and associated privileges of those roles]

Role	Internal or External	Privileged (P) Non-Privileged (NP) or No Logical Access (NLA)	Authorized Privileges	Functions Performed

Example:

Role	Internal or External	Privileged (P) Non-Privileged (NP) or No Logical Access (NLA)	Authorized Privileges	Functions Performed
UNIX sysadmin	*Internal*	*P*	*Full Access (root)*	*Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups*
Client administrator	*Internal*	*NP*	*Portal administration*	*Add/remote client users. Create, modify and delete client applications*
Program director	*Internal*	*NLA*	*None*	*Reviews, approves and enforces policy*

Instruction: This table must include all roles including systems administrators and database administrators as a role types. This includes web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact CUI.

This table must also include whether these roles are fulfilled by foreign nationals or roles that exist outside the United States, since that may impact compliance obligations.

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

SUPPLY CHAIN OVERVIEW

[provide a descriptive narrative of how vendors are involved in supporting how CUI is stored, processed or transmitted, if applicable]

Example:
There is currently only one (1) vendor involved in the supply chain for the CUI environment:

- *Vendor: VENDOR1*
- *Contract #: (123) 456-7890*
- *Support Contact: Jim Somebody*
- *Services Purchased: Platinum Support (contract #123456789) 24x7x365 support*

ONGOING MAINTENANCE & SUPPORT PLAN

[provide a descriptive narrative of how maintenance operations are conducted. This includes patch management and vulnerability remediation from ongoing vulnerability management scans]

Example:
VENDOR1 is currently providing Professional Services (PS) support for the initial configuration and integration of the tool. Once Technology Infrastructure has its XYZ administrator fully integrated, the amount of external support from XYZ, will decrease. Professional Services (PS) engagements will be on a case-by-case basis to augment CS Governance's organic capabilities.

XYZ System
Asset Owner: John Doe, SOC Director & contact #
Asset Custodian(s):

- *Primary XXXXX, Role & contact #*
- *Secondary XXXXX, Role & contact #*

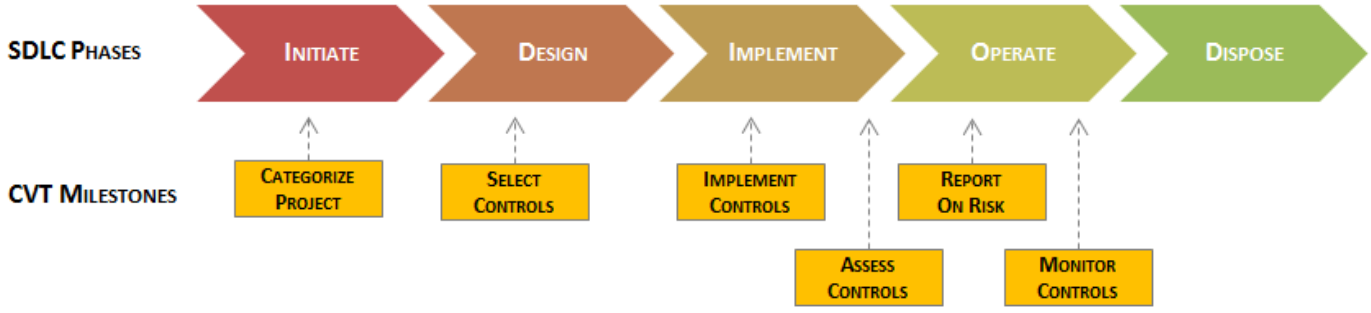
Patching is conducted in accordance with the Vulnerability & Patch Management Program (VPMP).

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 SP 800-171 CUI & NFO CONTROLS / CMMC PRACTICES)

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

NIST SP 800-171 APPENDIX D: 3.1 ACCESS CONTROL

These controls are associated with access control:

3.1.1 (AC.L1-3.1.1) LIMIT SYSTEM ACCESS TO AUTHORIZED USERS, PROCESSES ACTING ON BEHALF OF AUTHORIZED USERS, OR DEVICES (INCLUDING OTHER SYSTEMS).

Summary of NIST SP 800-171 & CMMC Controls Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ 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: Supporting policy(es): Identification & Authentication (IAC) & Third-Party Management (TPM) Supporting standard(s): IAC-15, IAC-20, TPM-05 & TPM-05.2 Supporting procedure(s): P-IAC-25, P-IAC-20, P-TPM-05 & P-TPM-05.2 [briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement] **Assessment Objectives (AOs) - Determine if:** **3.1.3[a] - information flow control policies are defined.** [briefly describe how this AO is implemented] **3.1.3[b] - methods and enforcement mechanisms for controlling the flow of CUI are defined.** [briefly describe how this AO is implemented] **3.1.3[c] - designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.** [briefly describe how this AO is implemented] **3.1.3[d] - authorizations for controlling the flow of CUI are defined.** [briefly describe how this AO is implemented] **3.1.3[e] - approved authorizations for controlling the flow of CUI are enforced.** [briefly describe how this AO is implemented]

Summary of NIST SP 800-171 & CMMC Controls Implementation

3.1.2 (AC.L1-3.1.2) LIMIT SYSTEM ACCESS TO THE TYPES OF TRANSACTIONS AND FUNCTIONS THAT AUTHORIZED USERS ARE PERMITTED TO EXECUTE.

Summary of NIST SP 800-171 & CMMC Controls Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ 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: Supporting policy(es): Identification & Authentication (IAC) Supporting standard(s): IAC-15 Supporting procedure(s): P-IAC-15 [briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement] **Assessment Objectives (AOs) - Determine if:** **3.1.2[a] - the types of transactions and functions that authorized users are permitted to execute are defined.** [briefly describe how this AO is implemented] **3.1.2[b] - system access is limited to the defined types of transactions and functions for authorized users.** [briefly describe how this AO is implemented]

3.1.3 (AC.L2-3.1.3) CONTROL THE FLOW OF CUI IN ACCORDANCE WITH APPROVED AUTHORIZATIONS.

Summary of NIST SP 800-171 & CMMC Controls Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable

Summary of NIST SP 800-171 & CMMC Controls Implementation
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: Supporting policy(es): Data Classification & Handling (DCH), Identification & Authentication (IAC) & Network Security (NET) Supporting standard(s): DCH-03, IAC-08, NET-04 & NET-18 Supporting procedure(s): P-DCH-03, P-IAC-08, P-NET-04 & P-NET-18 [briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement] **Assessment Objectives (AOs) - Determine if:** **3.1.3[a] - information flow control policies are defined.** [briefly describe how this AO is implemented] **3.1.3[b] - methods and enforcement mechanisms for controlling the flow of CUI are defined.** [briefly describe how this AO is implemented] **3.1.3[c] - designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.** [briefly describe how this AO is implemented] **3.1.3[d] - authorizations for controlling the flow of CUI are defined.** [briefly describe how this AO is implemented] **3.1.3[e] - approved authorizations for controlling the flow of CUI are enforced.** [briefly describe how this AO is implemented]

3.1.4 (AC.L2-3.1.4) SEPARATE THE DUTIES OF INDIVIDUALS TO REDUCE THE RISK OF MALEVOLENT ACTIVITY WITHOUT COLLUSION.

Summary of NIST SP 800-171 & CMMC Controls Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ 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]

Summary of NIST SP 800-171 & CMMC Controls Implementation
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: Supporting policy(es): Human Resources Security (HRS) Supporting standard(s): HRS-11 Supporting procedure(s): P-HRS-11 [briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement] **Assessment Objectives (AOs) - Determine if:** **3.1.4[a] - the duties of individuals requiring separation are defined.** [briefly describe how this AO is implemented] **3.1.4[b] - responsibilities for duties that require separation are assigned to separate individuals.** [briefly describe how this AO is implemented] **3.1.4[c] - access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.** [briefly describe how this AO is implemented]

3.1.5 (AC.L2-3.1.5) EMPLOY THE PRINCIPLE OF LEAST PRIVILEGE, INCLUDING FOR SPECIFIC SECURITY FUNCTIONS AND PRIVILEGED ACCOUNTS.

Summary of NIST SP 800-171 & CMMC Controls Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ 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: Supporting policy(es): Identification & Authentication (IAC) Supporting standard(s): IAC-16, IAC-16.1, IAC-21, IAC-21.1 & IAC-21.3 Supporting procedure(s): P-IAC-16, P-IAC-16.1, P-IAC-21, P-IAC-21.1 & P-IAC-21.3