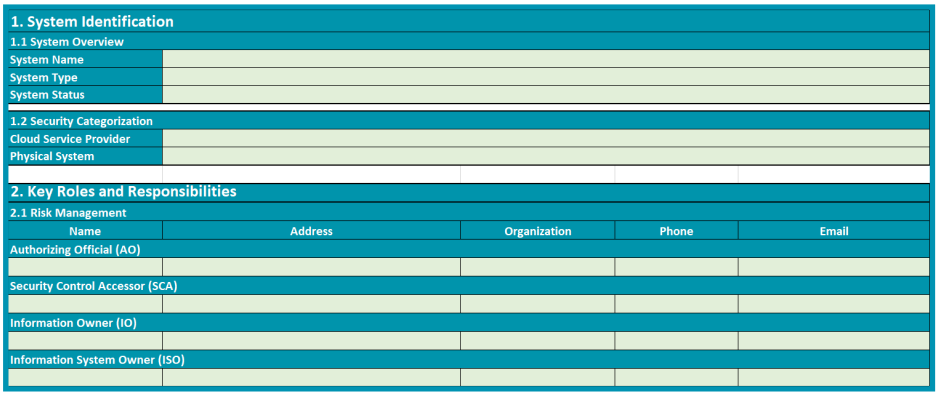
Ascolta CMMC Documentation Templates are designed to fully document your environment and easily assist CMMC assessors during your certification process.

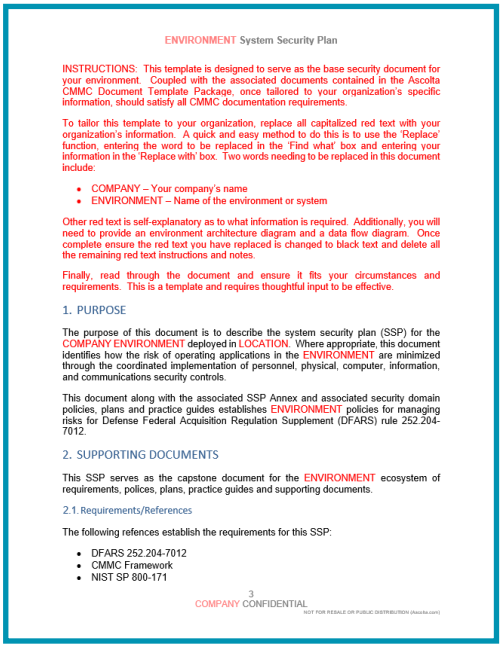
SYSTEM SECURITY PLAN

It all starts with the System Security Plan

The System Security Plan (SSP) describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. In particular, the system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.



1. System Identification				
1.1 System Overview				
System Name				
System Type				
System Status				
1.2 Security Categorization				
Cloud Service Provider				
Physical System				
2. Key Roles and Responsibilities				
2.1 Risk Management				
Name	Address	Organization	Phone	Email
Authorizing Official (AO)				
Security Control Accessor (SCA)				
Information Owner (IO)				
Information System Owner (ISO)				



ENVIRONMENT System Security Plan

INSTRUCTIONS: This template is designed to serve as the base security document for your environment. Coupled with the associated documents contained in the Ascolta CMMC Document Template Package, once tailored to your organization's specific information, should satisfy all CMMC documentation requirements.

To tailor this template to your organization, replace all capitalized red text with your organization's information. A quick and easy method to do this is to use the 'Replace' function, entering the word to be replaced in the 'Find what' box and entering your information in the 'Replace with' box. Two words needing to be replaced in this document include:

- COMPANY – Your company's name
- ENVIRONMENT – Name of the environment or system

Other red text is self-explanatory as to what information is required. Additionally, you will need to provide an environment architecture diagram and a data flow diagram. Once complete ensure the red text you have replaced is changed to black text and delete all the remaining red text instructions and notes.

Finally, read through the document and ensure it fits your circumstances and requirements. This is a template and requires thoughtful input to be effective.

1. PURPOSE

The purpose of this document is to describe the system security plan (SSP) for the COMPANY ENVIRONMENT deployed in LOCATION. Where appropriate, this document identifies how the risk of operating applications in the ENVIRONMENT are minimized through the coordinated implementation of personnel, physical, computer, information, and communications security controls.

This document along with the associated SSP Annex and associated security domain policies, plans and practice guides establishes ENVIRONMENT policies for managing risks for Defense Federal Acquisition Regulation Supplement (DFARS) rule 252.204-7012.

2. SUPPORTING DOCUMENTS

This SSP serves as the capstone document for the ENVIRONMENT ecosystem of requirements, polices, plans, practice guides and supporting documents.

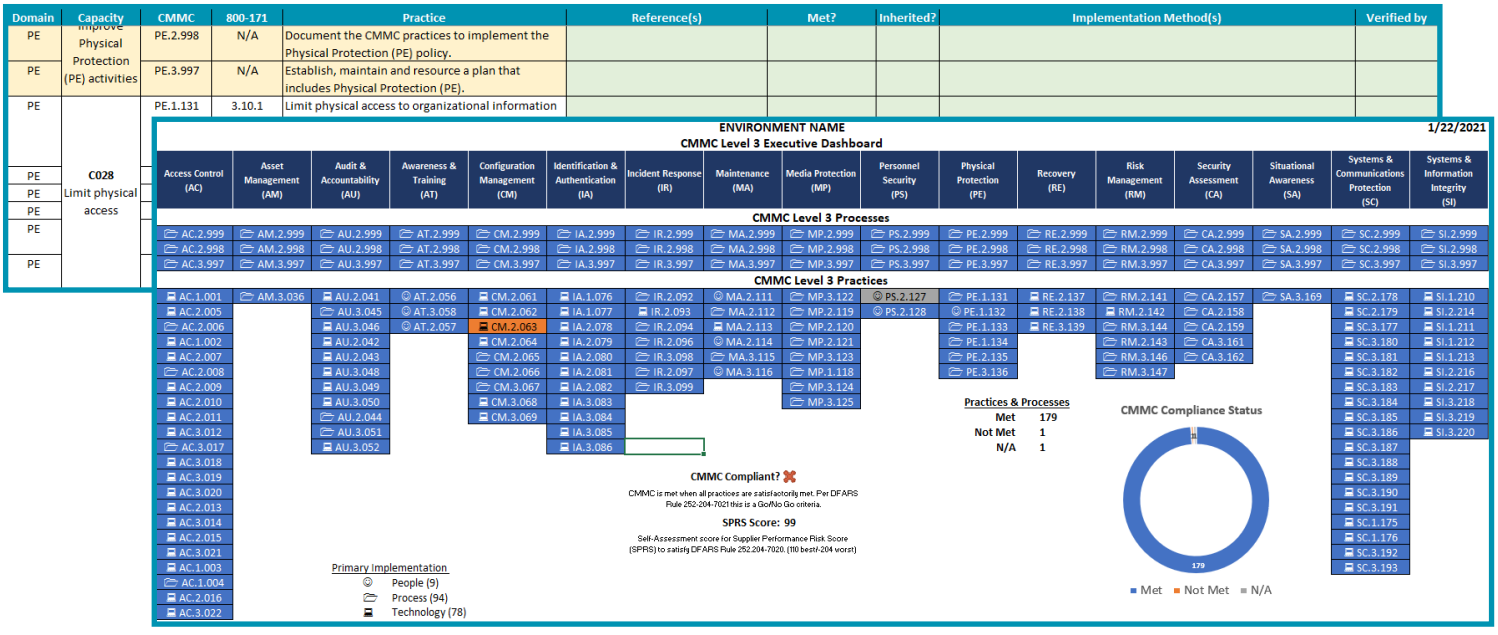
2.1. Requirements/References

The following refences establish the requirements for this SSP:

- DFARS 252.204-7012
- CMMC Framework
- NIST SP 800-171

3
COMPANY CONFIDENTIAL

The editable SSP Excel spreadsheet captures information in an easy to use format that generates auditable documents for the assessor. Coupled with the other provided templates you'll have everything needed to fully document your system or environment.



Domain	Capacity	CMMC	800-171	Practice	Reference(s)	Met?	Inherited?	Implementation Method(s)	Verified by
PE	Improve Physical Protection (PE) activities	PE.2.998	N/A	Document the CMMC practices to implement the Physical Protection (PE) policy.					
PE		PE.3.997	N/A	Establish, maintain and resource a plan that includes Physical Protection (PE).					
PE	C028 Limit physical access	PE.1.131	3.10.1	Limit physical access to organizational information					
PE									
PE									
PE									

ENVIRONMENT NAME — 1/22/2021

CMMC Level 3 Executive Dashboard

Access Control (AC)	Asset Management (AM)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)	Systems & Communications Protection (SC)	Systems & Information Integrity (SI)
CMMC Level 3 Processes																
AC.2.999	AM.2.999	AU.2.999	AT.2.999	CM.2.999	IA.2.999	IR.2.999	MA.2.999	MP.2.999	PS.2.999	PE.2.999	RE.2.999	RM.2.999	CA.2.999	SA.2.999	SC.2.999	SI.2.999
AC.2.998	AM.2.998	AU.2.998	AT.2.998	CM.2.998	IA.2.998	IR.2.998	MA.2.998	MP.2.998	PS.2.998	PE.2.998	RE.2.998	RM.2.998	CA.2.998	SA.2.998	SC.2.998	SI.2.998
AC.3.997	AM.3.997	AU.3.997	AT.3.997	CM.3.997	IA.3.997	IR.3.997	MA.3.997	MP.3.997	PS.3.997	PE.3.997	RE.3.997	RM.3.997	CA.3.997	SA.3.997	SC.3.997	SI.3.997
CMMC Level 3 Practices																
AC.1.001	AM.3.036	AU.2.041	AT.2.056	CM.2.061	IA.1.076	IR.2.092	MA.2.111	MP.3.122	PS.2.127	PE.1.131	RE.2.137	RM.2.141	CA.2.157	SA.3.169	SC.2.178	SI.1.210
AC.2.005		AU.3.045	AT.3.058	CM.2.062	IA.1.077	IR.2.093	MA.2.112	MP.2.119	PS.2.128	PE.1.132	RE.2.138	RM.2.142	CA.2.158		SC.2.179	SI.2.214
AC.2.006		AU.3.046	AT.2.057	CM.2.063	IA.2.078	IR.2.094	MA.2.113	MP.2.120		PE.1.133	RE.3.139	RM.3.144	CA.2.159		SC.3.177	SI.1.211
AC.1.002		AU.2.042		CM.2.064	IA.2.079	IR.2.096	MA.2.114	MP.2.121		PE.1.134		RM.2.143	CA.3.161		SC.3.180	SI.1.212
AC.2.007		AU.2.043		CM.2.065	IA.2.080	IR.3.098	MA.3.115	MP.3.123		PE.2.135		RM.3.146	CA.3.162		SC.3.181	SI.1.213
AC.2.008		AU.3.048		CM.2.066	IA.2.081	IR.2.097	MA.3.116	MP.1.118		PE.3.136		RM.3.147			SC.3.182	SI.2.216
AC.2.009		AU.3.049		CM.3.067	IA.2.082	IR.3.099		MP.3.124							SC.3.183	SI.2.217
AC.2.010		AU.3.050		CM.3.068	IA.3.083			MP.3.125							SC.3.184	SI.3.218
AC.2.011		AU.2.044		CM.3.069	IA.3.084										SC.3.185	SI.3.219
AC.3.012		AU.3.051			IA.3.085										SC.3.186	SI.3.220
AC.3.017		AU.3.052			IA.3.086										SC.3.187	
AC.3.018															SC.3.188	
AC.3.019															SC.3.189	
AC.3.020															SC.3.190	
AC.2.013															SC.3.191	
AC.3.014															SC.1.175	
AC.2.015															SC.1.176	
AC.3.021															SC.3.192	
AC.1.003															SC.3.193	
AC.1.004																
AC.2.016																
AC.3.022																

CMMC Compliant? ✖

CMMC is met when all practices are satisfactorily met. Per DFARS Rule 252-204-7021 this is a Go/No Go criteria.

SPRS Score: 99

Self-Assessment score for Supplier Performance Risk Score (SPRS) to satisfy DFARS Rule 252.204-7020. (110 best/-204 worst)

Practices & Processes

Met	179
Not Met	1
N/A	1

CMMC Compliance Status

Primary Implementation

People	(9)
Process	(94)
Technology	(78)

Our Executive Dashboard provides a quick reference tool to brief senior leadership and to manage continuous monitoring efforts. It also calculates your SPRS score for DFARS 252.204-7020 compliance.

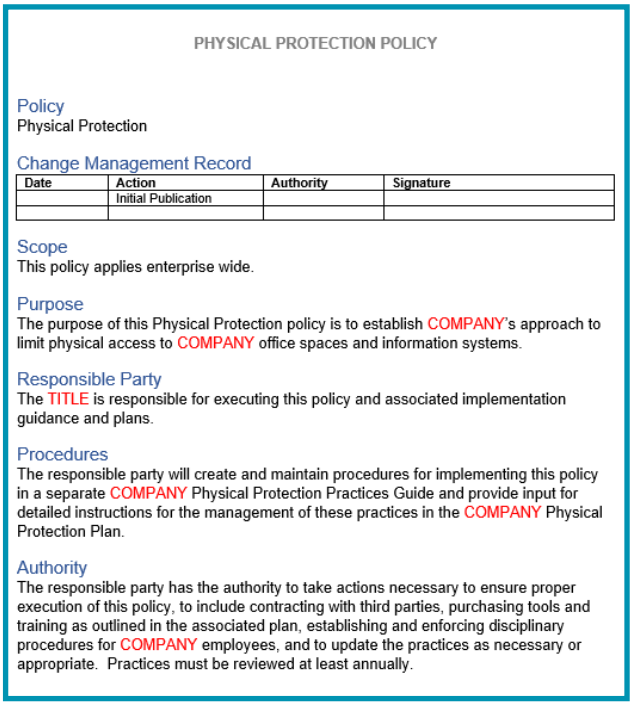
POLICIES

Establish a Policy for Each Security Domain

CMMC Level 3 require that for each security domain the:

- Purpose of the policy is clearly stated
- Scope of the policy is defined (e.g., enterprise-wide, department-wide, or information-system specific)
- Roles and responsibilities of the activities covered by this policy are defined; (i.e., the responsibility, authority, and ownership of Asset Management activities)
- Policy establishes or directs the establishment of procedures to carry out and meet the intent of the policy
- Any regulatory guidelines that this policy addresses are included
- Policy is endorsed by management and disseminated to appropriate stakeholders
- Policy is periodically reviewed and updated

You will receive fully editable Microsoft Word templates for each of the seventeen domains.



PHYSICAL PROTECTION POLICY

Policy
Physical Protection

Change Management Record

Date	Action	Authority	Signature
	Initial Publication		

Scope
This policy applies enterprise wide.

Purpose
The purpose of this Physical Protection policy is to establish COMPANY's approach to limit physical access to COMPANY office spaces and information systems.

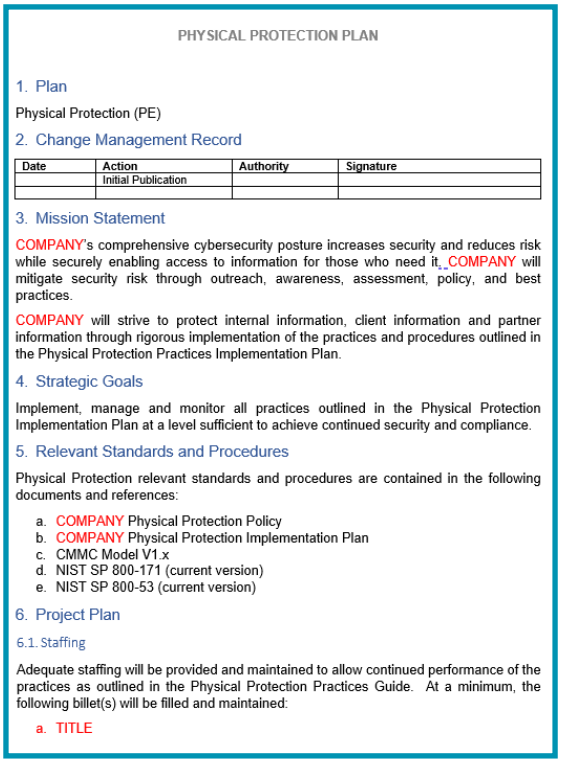
Responsible Party
The TITLE is responsible for executing this policy and associated implementation guidance and plans.

Procedures
The responsible party will create and maintain procedures for implementing this policy in a separate COMPANY Physical Protection Practices Guide and provide input for detailed instructions for the management of these practices in the COMPANY Physical Protection Plan.

Authority
The responsible party has the authority to take actions necessary to ensure proper execution of this policy, to include contracting with third parties, purchasing tools and training as outlined in the associated plan, establishing and enforcing disciplinary procedures for COMPANY employees, and to update the practices as necessary or appropriate. Practices must be reviewed at least annually.

PLANS

Establish, Maintain, and Resource Domain Plans



PHYSICAL PROTECTION PLAN

1. Plan

Physical Protection (PE)

2. Change Management Record

Date	Action	Authority	Signature
	Initial Publication		

3. Mission Statement

COMPANY's comprehensive cybersecurity posture increases security and reduces risk while securely enabling access to information for those who need it. COMPANY will mitigate security risk through outreach, awareness, assessment, policy, and best practices.

COMPANY will strive to protect internal information, client information and partner information through rigorous implementation of the practices and procedures outlined in the Physical Protection Practices Implementation Plan.

4. Strategic Goals

Implement, manage and monitor all practices outlined in the Physical Protection Implementation Plan at a level sufficient to achieve continued security and compliance.

5. Relevant Standards and Procedures

Physical Protection relevant standards and procedures are contained in the following documents and references:

a. COMPANY Physical Protection Policy
b. COMPANY Physical Protection Implementation Plan
c. CMMC Model V1.x
d. NIST SP 800-171 (current version)
e. NIST SP 800-53 (current version)

6. Project Plan

6.1. Staffing

Adequate staffing will be provided and maintained to allow continued performance of the practices as outlined in the Physical Protection Practices Guide. At a minimum, the following billet(s) will be filled and maintained:

a. TITLE

Additionally you will receive plans for each Domain to:

- Establish and maintain a plan that provides oversight for implementing the policies
- Plans includes a mission and/or vision statement, strategic goals/objectives, relevant standards and procedures and documents the activities, due dates, and resources assigned to implement and manage the policies
- People resources are assigned to support implementing the policies and staff members have the appropriate knowledge, skills, and abilities to carry out their duties
- Funding resources are defined and assigned to fully execute implementing the policies to include proper oversight, execution, and maintenance
- Specific tools required to implement the policies are provided and people resources are adequately trained to use these tools
- Relevant stakeholders are involved in resourcing activities

PRACTICE IMPLEMENTATION

Document the CMMC Practices to Implement Policies

How your organization implements each of the CMMC practices is the focus of an assessors evaluation and the key to a secure and compliant environment.

We provide a Practice Implementation Plan for each security domain that contains:

- Procedures to implement each practice and the documentation to be followed to implement the policy for each domain
- Procedures specifying the activities required to carry out the domain policy
- Procedures to be reviewed and updated periodically to ensure they meet Domain policy

Each Practice Implementation Plan contains instructions for each practice covered in the seventeen security domains. For practices that are non-environment specific, sample implementation methods are included.

7.1. Limit Physical Access (PE.1.131)

Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.

Objectives:

- Authorized individuals allowed physical access are identified;
- Physical access to organizational systems is limited to authorized individuals;
- Physical access to equipment is limited to authorized individuals; and
- Physical access to operating environments is limited to authorized individuals.

7.1.1. Implementation

Physical access to facilities and information system distribution and transmission lines within organizational facilities will be controlled by:

- Locking facilities doors and requiring swipe access for entry
- Locking server rooms and wiring closets
- Disconnecting or locking spare jacks

The TITLE will develop, approve, and maintain a list of individuals with authorized access to COMPANY facilities where CUI information resides and issue authorization credentials for facilities access. The list will be reviewed monthly, when access is no longer required, individual access will be removed.

Physical access to information system output devices will be controlled to prevent unauthorized individuals from obtaining the output by:

- Placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only
- Placing output devices in locations that can be monitored by organizational personnel
- Computing devices, external disk drives, networking devices, monitors, copiers, scanners, facsimile machines, and audio devices will be safeguarded.

7.1.2. Verification

EDIT THE LIST OF VERIFICATION METHODS LISTED BELOW FOR YOUR PARTICULAR CIRCUMSTANCES AND ENVIRONMENT. WHICHEVER METHODS YOU SELECT ENSURE THEY ARE AVAILABLE, UP TO DATE AND ACCURATE. CMMC ASSESSORS WILL REQUIRE A MINIMUM OF TWO MEANS OF VERIFICATION.

- Examine
  - Access lists
  - Physical inspection of equipment, locks, badges and swipe mechanisms
  - Physical Protection Practice Implementation Procedures
  - Procedures addressing physical access authorizations
  - System security plan
  - Authorized personnel access list
  - Authorization credentials
  - Physical access list reviews
  - Physical access termination records and associated documentation
- Interview
  - Facility Security Officer
  - Information System Security Manager
  - Personnel with physical access authorization responsibilities
  - Personnel with physical access to system facility
  - Personnel with information security responsibilities
- Test
  - Organizational processes for physical access authorizations
  - Mechanisms supporting or implementing physical access authorizations

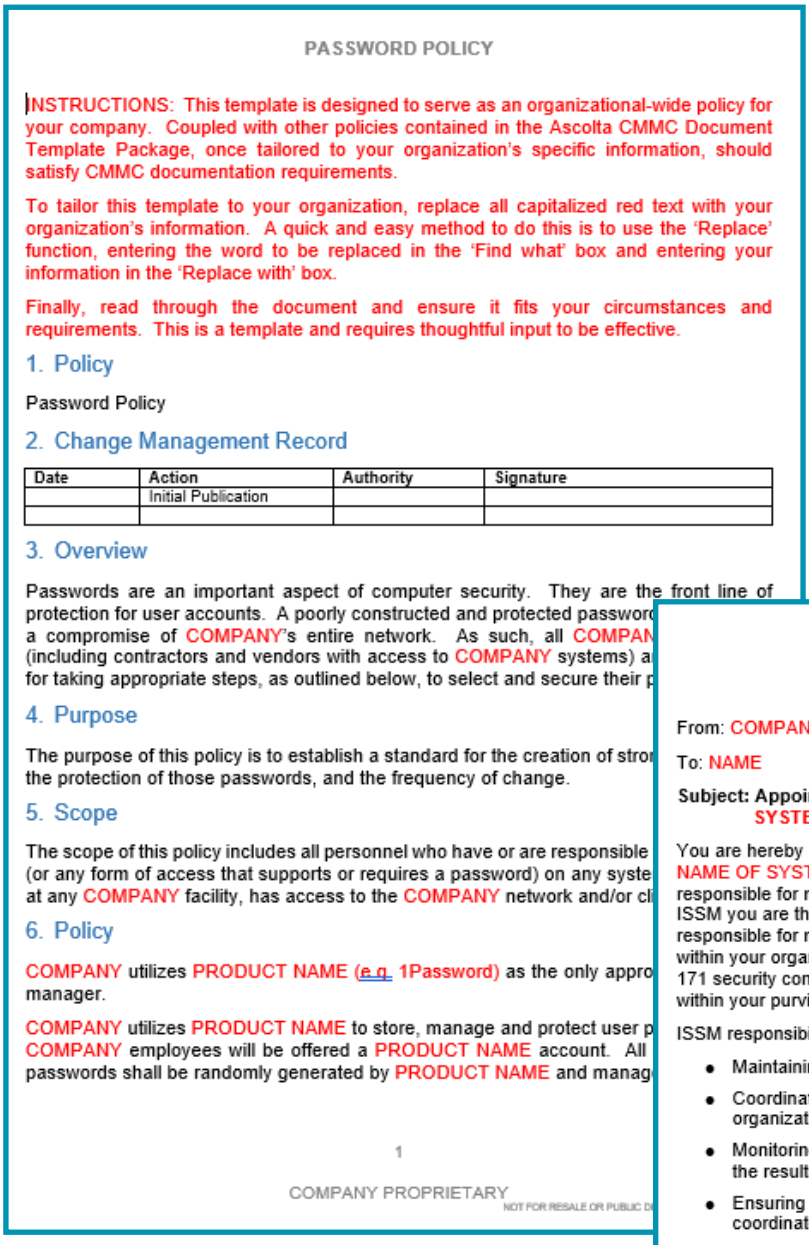
ascolta®

Additionally, we provide suggested verification methods to be utilized for each practice. This ensures you have a verifiable method to monitor compliance and it assists your assessor to rapidly determine if the practice is met or not met.

Each practice contains suggested list of artifacts to examine, lists of people to interview, and procedures and/or mechanisms to test.

POLICIES & TEMPLATES

Additional Helpful Policies and Templates Included



PASSWORD POLICY

INSTRUCTIONS: This template is designed to serve as an organizational-wide policy for your company. Coupled with other policies contained in the Ascolta CMMC Document Template Package, once tailored to your organization's specific information, should satisfy CMMC documentation requirements.

To tailor this template to your organization, replace all capitalized red text with your organization's information. A quick and easy method to do this is to use the 'Replace' function, entering the word to be replaced in the 'Find what' box and entering your information in the 'Replace with' box.

Finally, read through the document and ensure it fits your circumstances and requirements. This is a template and requires thoughtful input to be effective.

1. Policy

Password Policy

2. Change Management Record

Date	Action	Authority	Signature
	Initial Publication		

3. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly constructed and protected passwor
a compromise of COMPANY's entire network. As such, all COMPAN
(including contractors and vendors with access to COMPANY systems) a
for taking appropriate steps, as outlined below, to select and secure their p

4. Purpose

The purpose of this policy is to establish a standard for the creation of stro
the protection of those passwords, and the frequency of change.

5. Scope

The scope of this policy includes all personnel who have or are responsible
(or any form of access that supports or requires a password) on any syste
at any COMPANY facility, has access to the COMPANY network and/or cl

6. Policy

COMPANY utilizes PRODUCT NAME (e.g. 1Password) as the only appro
manager.

COMPANY utilizes PRODUCT NAME to store, manage and protect user p
COMPANY employees will be offered a PRODUCT NAME account. All
passwords shall be randomly generated by PRODUCT NAME and manag

1

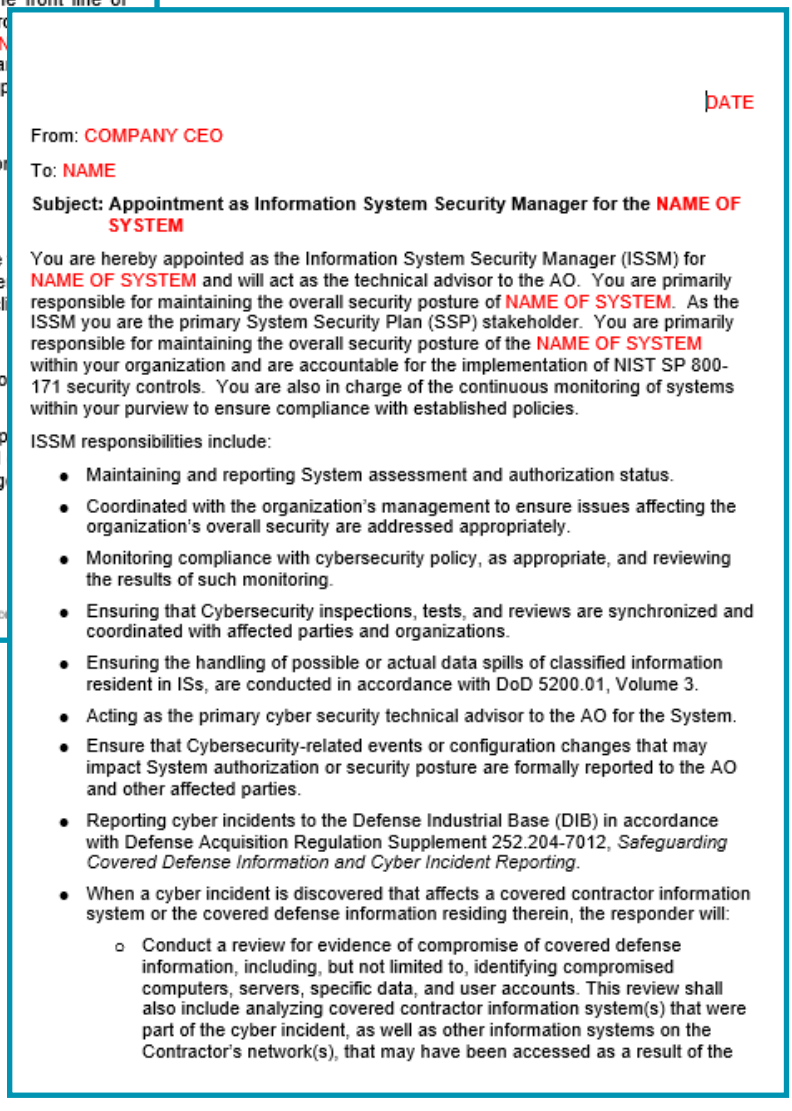
COMPANY PROPRIETARY

NOT FOR RESALE OR PUBLIC D

You'll also receive additional organizational policy templates for the following:

- Acceptable Use Policy
- Asset Management Policy
- Configuration & Change Control Policy
- Cyber Incident Response Policy
- Data Handling & Storage Policy
- Encryption Policy
- Mobile Device Policy
- Password Policy
- Risk Management Policy

All fully editable via Microsoft Word



DATE

From: COMPANY CEO

To: NAME

Subject: Appointment as Information System Security Manager for the NAME OF SYSTEM

You are hereby appointed as the Information System Security Manager (ISSM) for NAME OF SYSTEM and will act as the technical advisor to the AO. You are primarily responsible for maintaining the overall security posture of NAME OF SYSTEM. As the ISSM you are the primary System Security Plan (SSP) stakeholder. You are primarily responsible for maintaining the overall security posture of the NAME OF SYSTEM within your organization and are accountable for the implementation of NIST SP 800-171 security controls. You are also in charge of the continuous monitoring of systems within your purview to ensure compliance with established policies.

ISSM responsibilities include:

- Maintaining and reporting System assessment and authorization status.
- Coordinated with the organization's management to ensure issues affecting the organization's overall security are addressed appropriately.
- Monitoring compliance with cybersecurity policy, as appropriate, and reviewing the results of such monitoring.
- Ensuring that Cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations.
- Ensuring the handling of possible or actual data spills of classified information resident in ISs, are conducted in accordance with DoD 5200.01, Volume 3.
- Acting as the primary cyber security technical advisor to the AO for the System.
- Ensure that Cybersecurity-related events or configuration changes that may impact System authorization or security posture are formally reported to the AO and other affected parties.
- Reporting cyber incidents to the Defense Industrial Base (DIB) in accordance with Defense Acquisition Regulation Supplement 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting.*
- When a cyber incident is discovered that affects a covered contractor information system or the covered defense information residing therein, the responder will:
  - Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the

Finally, you'll receive many other documents in the form of appointment letters, Nondisclosure Agreements and other assorted useful templates.

Over seventy documents in all consisting of over 350 pages of timesaving material.

ascolta®