System Security Plan

CMMC Level 2 / NIST SP 800-171 Rev 2 Starter Template

Organization: _____

Program / Contract: _____

Plan Owner: _____

Date prepared: _____

Version: 1.0

How to use this template

This document is a starter template for the System Security Plan (SSP) required by NIST SP 800-171 Rev 2 § 3.12.4 and referenced by the CMMC 2.0 assessment process. It is opinionated about structure and conservative about content — fill in what's true for your environment.

> **Three things assessors look for in an SSP:**
> 1. The control implementation matches what's actually deployed (not aspirational).
> 2. Each implementation statement is specific (no copy-paste of the requirement back at itself).
> 3. Evidence references are concrete (procedure document, screenshot, config file).

What to fill in

For each control in Sections 2-15, replace the placeholder fields:

- **Implementation:** One to three sentences describing HOW your organization meets the requirement. Be specific to your tooling and process.
- **Evidence:** Pointers to where an assessor can verify the claim — document IDs, policy paragraph numbers, ticket IDs.

What not to do

- Do not restate the requirement text as your implementation. Auditors flag this immediately.
- Do not claim controls that are not in production. Document partial coverage on your POA&M instead.
- Do not skip the "out of scope" sections — assessors expect to see the boundary defined explicitly.

1. System Description

1.1 System name + identifier

NAME

_____

UNIQUE IDENTIFIER

_____

1.2 Authorization boundary

Describe the systems, network segments, and physical locations within the scope of this SSP. Reference an architecture diagram if one exists. The boundary should be tight — if a system does not touch CUI, exclude it explicitly.

1.3 CUI handling

What CUI categories does this system handle? Where does CUI originate, where is it stored, and where is it transmitted? List the data stores explicitly.

1.4 Connections to other systems

Document every external system connection (SaaS, partner network, internet). For each connection: purpose, data exchanged, protections in place.

1.5 Roles and responsibilities

SYSTEM OWNER

_____

SECURITY OFFICER / ISSO

_____

AUTHORIZING OFFICIAL

_____

2. Access Control (AC)

22 controls. Provide an implementation statement and evidence reference for each one.

3.1.1 L1

Limit system access to authorized users, processes acting on behalf of users, and devices.

Implementation: _____

Evidence: _____

3.1.2 L1

Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Implementation: _____

Evidence: _____

3.1.3 L2

Control the flow of CUI in accordance with approved authorizations.

Implementation: _____

Evidence: _____

3.1.4 L2

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

Implementation: _____

Evidence: _____

3.1.5 L2

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

Implementation: _____

Evidence: _____

3.1.6 L2

Use non-privileged accounts or roles when accessing nonsecurity functions.

Implementation: _____

Evidence: _____

3.1.7 L2

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Implementation: _____

Evidence: _____

3.1.8 L2

Limit unsuccessful logon attempts.

Implementation: _____

Evidence: _____

3.1.9 L2

Provide privacy and security notices consistent with applicable CUI rules.

Implementation: _____

Evidence: _____

3.1.10 L2

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Implementation: _____

Evidence: _____

3.1.11 L2

Terminate (automatically) a user session after a defined condition.

Implementation: _____

Evidence: _____

3.1.12 L2

Monitor and control remote access sessions.

Implementation: _____

Evidence: _____

3.1.13 L2

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Implementation: _____

Evidence: _____

3.1.14 L2

Route remote access via managed access control points.

Implementation: _____

Evidence: _____

3.1.15 L2

Authorize remote execution of privileged commands and remote access to security-relevant information.

Implementation: _____

Evidence: _____

3.1.16 L2

Authorize wireless access prior to allowing such connections.

Implementation: _____

Evidence: _____

3.1.17 L2

Protect wireless access using authentication and encryption.

Implementation: _____

Evidence: _____

3.1.18 L2

Control connection of mobile devices.

Implementation: _____

Evidence: _____

3.1.19 L2

Encrypt CUI on mobile devices and mobile computing platforms.

Implementation: _____

Evidence: _____

3.1.20 L1

Verify and control/limit connections to and use of external systems.

Implementation: _____

Evidence: _____

3.1.21 L2

Limit use of organizational portable storage devices on external systems.

Implementation: _____

Evidence: _____

3.1.22 L1

Control CUI posted or processed on publicly accessible systems.

Implementation: _____

Evidence: _____

3. Awareness and Training (AT)

3 controls. Provide an implementation statement and evidence reference for each one.

3.2.1 L2

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities.

Implementation: _____

Evidence: _____

3.2.2 L2

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Implementation: _____

Evidence: _____

3.2.3 L2

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Implementation: _____

Evidence: _____

4. Audit and Accountability (AU)

9 controls. Provide an implementation statement and evidence reference for each one.

3.3.1 L2

Create and retain system audit logs and records to enable monitoring, analysis, investigation, and reporting of unlawful or unauthorized activity.

Implementation: _____

Evidence: _____

3.3.2 L2

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Implementation: _____

Evidence: _____

3.3.3 L2

Review and update logged events.

Implementation: _____

Evidence: _____

3.3.4 L2

Alert in the event of an audit logging process failure.

Implementation: _____

Evidence: _____

3.3.5 L2

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Implementation: _____

Evidence: _____

3.3.6 L2

Provide audit record reduction and report generation to support on-demand analysis and reporting.

Implementation: _____

Evidence: _____

3.3.7 L2

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Implementation: _____

Evidence: _____

3.3.8 L2

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Implementation: _____

Evidence: _____

3.3.9 L2

Limit management of audit logging functionality to a subset of privileged users.

Implementation: _____

Evidence: _____

5. Configuration Management (CM)

9 controls. Provide an implementation statement and evidence reference for each one.

3.4.1 L2

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Implementation: _____

Evidence: _____

3.4.2 L2

Establish and enforce security configuration settings for information technology products employed in organizational systems.

Implementation: _____

Evidence: _____

3.4.3 L2

Track, review, approve or disapprove, and log changes to organizational systems.

Implementation: _____

Evidence: _____

3.4.4 L2

Analyze the security impact of changes prior to implementation.

Implementation: _____

Evidence: _____

3.4.5 L2

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Implementation: _____

Evidence: _____

3.4.6 L2

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Implementation: _____

Evidence: _____

3.4.7 L2

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Implementation: _____

Evidence: _____

3.4.8 L2

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Implementation: _____

Evidence: _____

3.4.9 L2

Control and monitor user-installed software.

Implementation: _____

Evidence: _____

---

6. Identification and Authentication (IA)

11 controls. Provide an implementation statement and evidence reference for each one.

3.5.1 L1

Identify system users, processes acting on behalf of users, and devices.

Implementation: _____

Evidence: _____

3.5.2 L1

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Implementation: _____

Evidence: _____

3.5.3 L2

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Implementation: _____

Evidence: _____

3.5.4 L2

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Implementation: _____

Evidence: _____

3.5.5 L2

Prevent reuse of identifiers for a defined period.

Implementation: _____

Evidence: _____

3.5.6 L2

Disable identifiers after a defined period of inactivity.

Implementation: _____

Evidence: _____

3.5.7 L2

Enforce a minimum password complexity and change of characters when new passwords are created.

Implementation: _____

Evidence: _____

3.5.8 L2

Prohibit password reuse for a specified number of generations.

Implementation: _____

Evidence: _____

3.5.9 L2

Allow temporary password use for system logons with an immediate change to a permanent password.

Implementation: _____

Evidence: _____

3.5.10 L2

Store and transmit only cryptographically-protected passwords.

Implementation: _____

Evidence: _____

3.5.11 L2

Obscure feedback of authentication information.

Implementation: _____

Evidence: _____

---

7. Incident Response (IR)

3 controls. Provide an implementation statement and evidence reference for each one.

3.6.1 L2

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Implementation: _____

Evidence: _____

3.6.2 L2

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Implementation: _____

Evidence: _____

3.6.3 L2

Test the organizational incident response capability.

Implementation: _____

Evidence: _____

8. Maintenance (MA)

6 controls. Provide an implementation statement and evidence reference for each one.

3.7.1 L2

Perform maintenance on organizational systems.

Implementation: _____

Evidence: _____

3.7.2 L2

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Implementation: _____

Evidence: _____

3.7.3 L2

Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Implementation: _____

Evidence: _____

3.7.4 L2

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Implementation: _____

Evidence: _____

3.7.5 L2

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Implementation: _____

Evidence: _____

3.7.6 L2

Supervise the maintenance activities of maintenance personnel without required access authorization.

Implementation: _____

Evidence: _____

9. Media Protection (MP)

9 controls. Provide an implementation statement and evidence reference for each one.

3.8.1 L2

Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Implementation: _____

Evidence: _____

3.8.2 L2

Limit access to CUI on system media to authorized users.

Implementation: _____

Evidence: _____

3.8.3 L1

Sanitize or destroy system media containing CUI before disposal or release for reuse.

Implementation: _____

Evidence: _____

3.8.4 L2

Mark media with necessary CUI markings and distribution limitations.

Implementation: _____

Evidence: _____

3.8.5 L2

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Implementation: _____

Evidence: _____

3.8.6 L2

Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Implementation: _____

Evidence: _____

3.8.7 L2

Control the use of removable media on system components.

Implementation: _____

Evidence: _____

3.8.8 L2

Prohibit the use of portable storage devices when such devices have no identifiable owner.

Implementation: _____

Evidence: _____

3.8.9 L2

Protect the confidentiality of backup CUI at storage locations.

Implementation: _____

Evidence: _____

10. Personnel Security (PS)

2 controls. Provide an implementation statement and evidence reference for each one.

3.9.1 L2

Screen individuals prior to authorizing access to organizational systems containing CUI.

Implementation: _____

Evidence: _____

3.9.2 L2

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Implementation: _____

Evidence: _____

11. Physical Protection (PE)

6 controls. Provide an implementation statement and evidence reference for each one.

3.10.1 L1

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

Implementation: _____

Evidence: _____

3.10.2 L2

Protect and monitor the physical facility and support infrastructure for organizational systems.

Implementation: _____

Evidence: _____

3.10.3 L1

Escort visitors and monitor visitor activity.

Implementation: _____

Evidence: _____

3.10.4 L1

Maintain audit logs of physical access.

Implementation: _____

Evidence: _____

3.10.5 L1

Control and manage physical access devices.

Implementation: _____

Evidence: _____

3.10.6 L2

Enforce safeguarding measures for CUI at alternate work sites.

Implementation: _____

Evidence: _____

---

12. Risk Assessment (RA)

3 controls. Provide an implementation statement and evidence reference for each one.

3.11.1 L2

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Implementation: _____

Evidence: _____

3.11.2 L2

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Implementation: _____

Evidence: _____

3.11.3 L2

Remediate vulnerabilities in accordance with risk assessments.

Implementation: _____

Evidence: _____

13. Security Assessment (CA)

4 controls. Provide an implementation statement and evidence reference for each one.

3.12.1 L2

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Implementation: _____

Evidence: _____

3.12.2 L2

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Implementation: _____

Evidence: _____

3.12.3 L2

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Implementation: _____

Evidence: _____

3.12.4 L2

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Implementation: _____

Evidence: _____

14. System and Communications Protection (SC)

16 controls. Provide an implementation statement and evidence reference for each one.

3.13.1 L1

Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Implementation: _____

Evidence: _____

3.13.2 L2

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Implementation: _____

Evidence: _____

3.13.3 L2

Separate user functionality from system management functionality.

Implementation: _____

Evidence: _____

3.13.4 L2

Prevent unauthorized and unintended information transfer via shared system resources.

Implementation: _____

Evidence: _____

3.13.5 L1

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Implementation: _____

Evidence: _____

3.13.6 L2

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Implementation: _____

Evidence: _____

3.13.7 L2

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Implementation: _____

Evidence: _____

3.13.8 L2

Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Implementation: _____

Evidence: _____

3.13.9 L2

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Implementation: _____

Evidence: _____

3.13.10 L2

Establish and manage cryptographic keys for cryptography employed in organizational systems.

Implementation: _____

Evidence: _____

3.13.11 L2

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Implementation: _____

Evidence: _____

3.13.12 L2

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Implementation: _____

Evidence: _____

3.13.13 L2

Control and monitor the use of mobile code.

Implementation: _____

Evidence: _____

3.13.14 L2

Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Implementation: _____

Evidence: _____

3.13.15 L2

Protect the authenticity of communications sessions.

Implementation: _____

Evidence: _____

3.13.16 L2

Protect the confidentiality of CUI at rest.

Implementation: _____

Evidence: _____

15. System and Information Integrity (SI)

7 controls. Provide an implementation statement and evidence reference for each one.

3.14.1 L1

Identify, report, and correct system flaws in a timely manner.

Implementation: _____

Evidence: _____

3.14.2 L1

Provide protection from malicious code at designated locations within organizational systems.

Implementation: _____

Evidence: _____

3.14.3 L2

Monitor system security alerts and advisories and take action in response.

Implementation: _____

Evidence: _____

3.14.4 L1

Update malicious code protection mechanisms when new releases are available.

Implementation: _____

Evidence: _____

3.14.5 L1

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Implementation: _____

Evidence: _____

3.14.6 L2

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Implementation: _____

Evidence: _____

3.14.7 L2

Identify unauthorized use of organizational systems.

Implementation: _____

Evidence: _____

Appendix A — References

- NIST SP 800-171 Rev 2 (February 2020) — *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- NIST SP 800-171A — Assessment procedures
- 32 CFR Part 170 — CMMC Program Final Rule (October 2024)
- 48 CFR DFARS 252.204-7012 — Safeguarding Covered Defense Information + Cyber Incident Reporting
- 48 CFR DFARS 252.204-7021 — Cybersecurity Maturity Model Certification Requirements

Appendix B — Glossary

CUI

Controlled Unclassified Information. Information the government creates or possesses that requires safeguarding under federal law/regulations.

C3PAO

CMMC Third-Party Assessor Organization. Authorized to perform Level 2 certification assessments.

SSP

System Security Plan. This document. Describes the security posture of a system handling CUI.

POA&M

Plan of Action and Milestones. Tracks gaps in control implementation with target remediation dates.

FIPS

Federal Information Processing Standards. NIST 800-171 §3.13.11 requires FIPS-validated cryptography for CUI.

Appendix C — Need a hand?

This template gets you to a structure. Filling in 110 control implementations is where most subs lose a few weeks. Readyline GRC generates implementation statements + tracks evidence from your actual config, so the SSP stays current automatically.

readylinegrc.com · **hello@readylinegrc.com** · Cipher One Tech LLC · Maryland, USA