SSP-01 System Security Plan (SSP)

Version: 2.0
Effective Date: [YYYY-MM-DD]
System Boundary: SB-Client
Prepared By: [PROVIDER] (Advisory)
Ownership: [Client]
Review Frequency: Annual or after significant change

---

1. System Identification

Field	Entry
Organization Name	[CLIENT_NAME]
System Name	Client CUI Processing Environment (SB-Client)
System Description	Cloud-first CUI-capable environment operated by the client and supported by MSP and [PROVIDER] advisory services.
System Category	CMMC Level 2 (Controlled Unclassified Information)
Primary IT Support	[MSP_NAME]
Primary Compliance Support	[PROVIDER]
Executive Sponsor	[CLIENT_EXEC_SPONSOR_NAME]
Security Lead	[CLIENT_SECURITY_LEAD]

---

2. System Environment

The organization maintains a **cloud-forward system environment** using Microsoft 365 and Azure Entra ID for identity, access, collaboration, and device management.

2.1 Core Components

Component Type	Description	Responsible Party
Identity Provider	Microsoft Entra ID	MSP
Endpoint Protection	Microsoft Defender for Endpoint	MSP
Device Management	Microsoft Intune	MSP
Collaboration Suite	Microsoft 365 (SharePoint, Teams, Exchange)	Client + MSP
Security Compliance Advisory	[PROVIDER]	[PROVIDER]

2.2 Data Classification in Scope

Data Type	Examples	Classification
CUI	DoD Contract Technical Info, Supplier Data	Controlled
FCI	General contract communications	Sensitive
Internal Business	HR, Finance	Internal Use

> **No CUI is stored at [PROVIDER].**
> Client retains full ownership and control.

---

3. System Security Roles

Role	Responsibility	Assigned To
Executive Sponsor	Accepts risk & approves policies	[CLIENT]
Security Lead	Coordinates security decisions	[CLIENT]
MSP / IT Service Provider	Executes technical changes & monitoring	[MSP]
[PROVIDER] (if contracted)	Compliance program management, SSP/POAM updating, evidence preparation	[PROVIDER]
All Personnel	Follow policies and report incidents	All Staff

---

4. System Boundaries & Architecture

4.1 Boundary Summary

The system boundary includes: - Only **managed corporate devices** - Only **Microsoft 365 cloud applications** - Only **authorized user identities** - Only **approved collaboration channels**

4.2 Out of Scope

- Personal devices (BYOD)
- Personal cloud storage
- Any [PROVIDER] internal systems

4.3 Diagrams *(placeholders — completed during onboarding)*

Appendix B — Network / Architectural Diagram
Appendix C — Data Flow Diagram

---

5. System Authorization Basis

Component	Document Name	Maintained By
Policies	POL-IS-00 through POL-WE-18 (19	[PROVIDER]

	policies)	
SSP	SSP-01	[PROVIDER] + Client
POAM	REF-PO-01	[PROVIDER]
Evidence Register	REF-EV-01	[PROVIDER]
Access / Asset Registers	REF-AC-01, REF-TP-01	MSP / Client

---

6. Control Implementation Summary (by Family)

> *Each control below references the corresponding policy section.*
> *Detailed implementation evidence is maintained in the Evidence Register (REF-EV-01).*

6.1 Access Control (AC)

Control	Description	Implemented In	Evidence Ref
3.1.x (22 controls)	Access permissions, RBAC, MFA, remote access, wireless	**POL-AC-01**	REF-AC-01, REF-AC-02, REF-AC-03, REF-AC-04

6.2 Awareness and Training (AT)

Control	Description	Implemented In	Evidence Ref
3.2.x (3 controls)	Security awareness & role-based training	**POL-AT-02**	REF-AT-01, REF-AT-02, REF-AT-03, REF-AT-04

6.3 Audit & Accountability (AU)

Control	Description	Implemented In	Evidence Ref
3.3.x (9 controls)	Audit logging, SIEM, log retention, log review	**POL-AU-03**	REF-AU-01, REF-AU-02

6.4 Configuration Management (CM)

Control	Description	Implemented In	Evidence Ref
3.4.x (9 controls)	Change control, baselines, security impact analysis	**POL-CM-04**	REF-CM-01, REF-CM-02, REF-CM-03, REF-CM-04

6.5 Identification & Authentication (IA)

Control	Description	Implemented In	Evidence Ref
3.5.x (11 controls)	Identity enrollment, MFA, password complexity	**POL-IA-05**	REF-IA-01, REF-IA-02

6.6 Incident Response (IR)

Control	Description	Implemented In	Evidence Ref
3.6.x (5 controls)	Incident detection, DFARS 72-hour reporting	**POL-IR-06**	REF-IR-01, REF-IR-02, REF-IR-03

6.7 Maintenance (MA)

Control	Description	Implemented In	Evidence Ref
3.7.x (6 controls)	Maintenance procedures, vendor escorting	**POL-MA-07**	REF-MA-01, REF-MA-02, REF-MA-03, REF-MA-04

6.8 Media Protection (MP)

Control	Description	Implemented In	Evidence Ref
3.8.x (9 controls)	CUI media marking, encryption, sanitization (NIST SP 800-88)	**POL-MP-08**	REF-MP-01, REF-MP-02, REF-MP-03, REF-MP-04

6.9 Personnel Security (PS)

Control	Description	Implemented In	Evidence Ref
3.9.x (7 controls)	Background checks, onboarding, termination	**POL-PS-09**	REF-PS-01 through REF-PS-07

6.10 Physical Protection (PE)

Control	Description	Implemented In	Evidence Ref
3.10.x (6 controls)	Facility access controls, visitor management	**POL-PE-10**	REF-PE-01 through REF-PE-08

6.11 Risk Assessment (RA)

Control	Description	Implemented In	Evidence Ref
3.11.x (4 controls)	Annual risk assessments, vulnerability scanning	**POL-RA-11**	REF-RA-01 through REF-RA-05

6.12 Security Assessment (CA)

Control	Description	Implemented In	Evidence Ref
3.12.x (6 controls)	Security assessments, POA&M, continuous monitoring	**POL-CA-12**	REF-CA-01 through REF-CA-06, REF-PO-01

6.13 System & Communications Protection (SC)

Control	Description	Implemented In	Evidence Ref
3.13.x (13 controls)	Network segmentation, encryption (TLS 1.2+, FIPS 140-2)	**POL-SC-13**	REF-SC-01 through REF-SC-04

6.14 System Integrity (SI)

Control	Description	Implemented In	Evidence Ref
3.14.x (10 controls)	Flaw remediation, anti-malware, vulnerability management	**POL-SI-14**	REF-SI-01 through REF-SI-05

6.15 Contingency Planning (CP)

Control	Description	Implemented In	Evidence Ref
Contingency planning	RTO/RPO, backup testing, disaster recovery	**POL-CP-15**	REF-CP-01 through REF-CP-08

6.16 Third-Party Risk (TP)

Control	Description	Implemented In	Evidence Ref
Vendor risk management	Vendor assessments, contracts, supply chain	**POL-TP-16**	REF-TP-01 through REF-TP-09

---

7. Continuous Monitoring & Maintenance

Monitoring and improvement activities include:

Frequency	Activity	Performed By
Monthly	Compliance review & evidence updating	[PROVIDER] (if contracted)
Quarterly	Risk posture review	[PROVIDER] + Client
Annual	Full SSP refresh	[PROVIDER]

---

8. Change History

Version	Date	Summary of Change	Author
2.0	[YYYY-MM-DD]	Initial standardized release	[PROVIDER]

Appendices

Appendix A — System Component Inventory

(Maintain system component inventory using configuration management tools or spreadsheet. Document all CUI systems, network devices, and endpoints.)

Appendix B — Network Diagram *(placeholder)*

Appendix C — Data Flow Diagram *(placeholder)*

Appendix D — Policies & Artifact Index

(Auto-generated once all document IDs finalize)