System Security Plan (SSP) for

Assessment Date: [Current Date]
Next Review Date: [Future Date]

Section 1: Executive Summary

The System Security Plan (SSP) for establishes a structured approach to protecting the organization's information systems, assets, and data from cybersecurity threats. This plan details security controls, risk management strategies, and compliance measures in accordance with NIST 800-53, CMMC, and other relevant federal regulations.

Objectives:

- Ensure confidentiality, integrity, and availability (CIA) of organizational data.
- Protect against cybersecurity threats and vulnerabilities.
- Establish incident response and business continuity protocols.
- Maintain compliance with industry and regulatory standards.

This SSP is the primary reference for security policies and procedures, ensuring all personnel understand their responsibilities in maintaining a secure environment.

Section 2: System Identification

System Name & ID:

- **System Name:**
- **System ID:**

System Owner:

- **Name:** [System Owner's Name]
- **Department:** IT Security & Compliance
- **Email:** [Owner's Email]
- **Phone:** [Owner's Contact]

System Categorization:

Based on the Federal Information Processing Standard (FIPS) 199, this system is categorized as follows:

Security Objective	Impact Level (Low/Moderate/High)
Confidentiality	[Low / Moderate / High]
Integrity	[Low / Moderate / High]

Security Objective	Impact Level (Low/Moderate/High)
Availability	[Low / Moderate / High]

Section 3: System Environment

System Components

Component Type	Description	Location	Security Controls
Servers	Cloud-based and on-premises database servers	AWS / Data Center	Firewall, IDS/IPS, Encryption
Workstations	Laptops and desktops used by employees	Office & Remote	Device Encryption, Endpoint Protection
Cloud Services	Microsoft 365, Google Workspace, AWS	Cloud	Access Control, Logging & Monitoring
Network Devices	Firewalls, Routers, VPNs	Data Center & Branches	Network Segmentation, Zero Trust
Email System	Corporate email and collaboration tools	Cloud	DMARC, SPF, DKIM, Phishing Protection

Section 4: Security Roles & Responsibilities

Role	Responsibilities
System Owner	Ensure system security and compliance.
System Administrator	Implement security policies, patches, and access control.
Security Analyst	Conducts threat monitoring and risk assessments.
Incident Response Team (IRT)	Handles cybersecurity incidents and forensic investigations.
Compliance Officer	Ensure legal and regulatory compliance.

Section 6: Risk Management Strategy

Risk ID	Threat	Vulnerability	Impact	Likelihood	Risk Level	Mitigation Strategy
R001	Data Breach	No MFA for Admins	High	High	Critical	Enforce MFA, Regular Audits
R002	Insider Threat	No Security Awareness Training	High	Medium	High	Quarterly Training, Least Privilege Access
R003	Ransomware	Unsegmented Network	High	High	Critical	Implement Network Segmentation & Air-Gapped Backups
R004	Phishing Attack	Weak Email Security	High	High	Critical	Enforce DMARC, SPF, DKIM

Section 7: Security Awareness & Training

- **Annual Cybersecurity Training:** Required for all employees.
- **Quarterly Phishing Simulations:** Test user awareness and response to phishing attacks.
- **Incident Response Drills:** Conducted bi-annually to improve emergency response efficiency.

Section 8: Incident Response Plan (IRP)

Incident Response Lifecycle (NIST 800-61)

1. **Preparation:** Security controls and incident response policies documented.
2. **Detection & Analysis:** Threat monitoring through SIEM tools.
3. **Containment:** Affected systems are isolated to prevent further compromise.
4. **Eradication & Recovery:** Threats removed, and systems restored securely.
5. **Lessons Learned:** Post-incident reviews were conducted to improve future responses.

Section 9: Security Controls & Compliance

✅ **Access Control (AC):** Role-based permissions and authentication protocols.
✅ **Audit & Accountability (AU):** System logging and security event monitoring.
✅ **Incident Response (IR):** Procedures for handling security incidents.
✅ **System & Communications Protection (SC):** Secure data transmission and firewall

policies.
✅ **Security Training (AT):** Continuous security awareness programs for employees.

Section 10: Plan of Action & Milestones (POA&M)

Control ID	Action Item	Responsible Party	Deadline	Status
AC-2	Implement Zero Trust Architecture	IT Security	[Date]	In Progress
IR-4	Deploy Advanced Threat Detection	Security Team	[Date]	Planned
SC-5	Upgrade Network Firewalls	Network Admin	[Date]	Not Started
AT-3	Conduct Phishing Training	Compliance Team	[Date]	Ongoing

Section 11: Review & Approval

Assessment Review:
This System Security Plan (SSP) has been reviewed and approved to ensure 's compliance, security readiness, and risk mitigation strategies align with industry standards.

Approver Name: [Name]
Signature: [Signature]
Date: [Date]