

System Security Plan (SSP)



APPLICABLE SCOPE

Prepared By:

Ryan Hoek

Chief Executive Officer

St. Michael LLC

Email: ryan@stmichaelenterprises.com

Phone: +1 (615) 626-1954

Prepared For:


Federal Government Contracting Officers and Prime Contract Clients

Assessment Level:

Cybersecurity Maturity Model Certification (CMMC) 2.0 – Level 1

 Version: 1.0

 Effective Date: May 01, 2025

 Policy Review Cycle: Bi-Annually

CONTENTS

1. Introduction	1
3. Security Responsibilities	2
4. Security Requirements Implementation (FAR 52.204-21)	2
5. Risk Assessment and Gap Identification	3
6. Maintenance and Monitoring.....	3
7. Contingency Planning.....	3
8. Documentation Control	3
9. Conclusion	3

SYSTEM SECURITY PLAN (SSP)

Organization Name: St. Michael LLC

Unique Entity ID: KC57D8EHLZ39

CAGE Code: 9MT36

Address: 4625 104th St SW, Byron Center, MI 49315-8701, USA

Prepared By: Ryan Hoek, Chief Executive Officer

Date Prepared: Wednesday, April 23, 2025

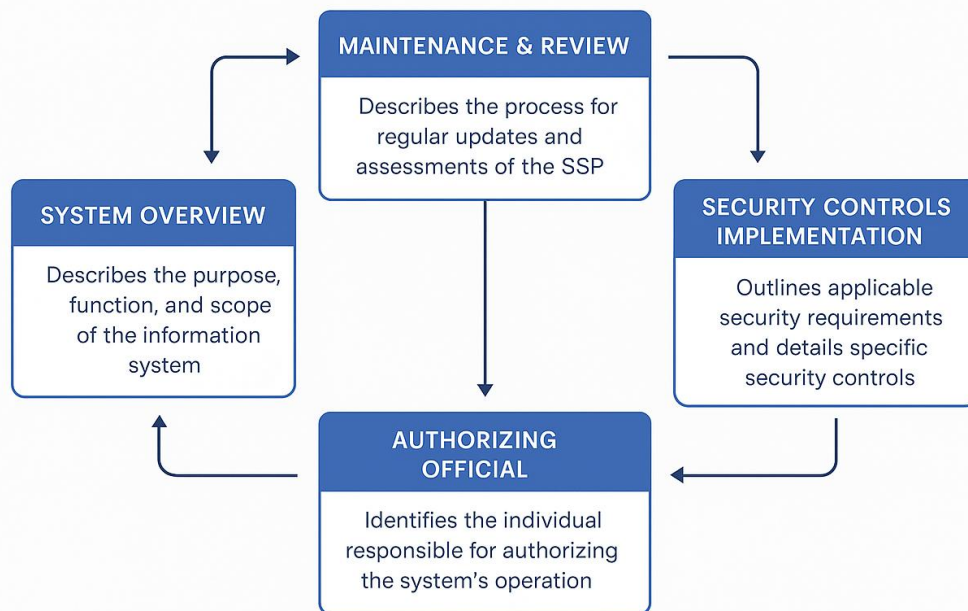
Assessment Level: CMMC 2.0 – Level 1 (Foundational)

System Name: St. Michael Federal Contract Support Infrastructure

1. INTRODUCTION

This System Security Plan (SSP) documents the implementation of cybersecurity practices and policies by St. Michael LLC in accordance with the requirements outlined in the Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 and FAR 52.204-21. It serves to demonstrate the company's compliance with federal security requirements for handling Federal Contract Information (FCI). This plan covers organizational security controls, system architecture, user access policies, physical and logical protections, and processes for ongoing security maintenance.

System Security Plan (SSP)



2. SYSTEM ENVIRONMENT DESCRIPTION

St. Michael LLC operates a hybrid infrastructure composed of:

- **Cloud-based Platforms:** Microsoft 365 (Exchange, SharePoint, OneDrive, Teams), Zoom, and Adobe Cloud.
- **Local Assets:** Company-owned and IT-managed Windows-based laptops and workstations.
- **Remote Access:** Enforced via VPN and secured endpoints; remote users are authenticated through MFA.
- **Security Stack:** Microsoft Defender for Endpoint, BitLocker for device encryption, Microsoft Intune for mobile device management (MDM), and firewalls with logging and outbound filtering.

This system environment is used to support communications, documentation, and information management functions across federal projects. All systems handling FCI are segregated from public access components and maintained under strict access control and monitoring policies.

3. SECURITY RESPONSIBILITIES

- **Authorizing Official:** Ryan Hoek, CEO
- **System Administrator:** Haroon Haider, VP of Compliance
- **IT Security Oversight:** Third-party cybersecurity consultant (retained annually)
- **Employees and Users:** Required to complete annual security training and abide by Acceptable Use Policy (AUP)

4. SECURITY REQUIREMENTS IMPLEMENTATION (FAR 52.204-21)

This section outlines how St. Michael LLC implements the 17 security controls required under CMMC Level 1.

Access Control (AC):

- AC.1.001: Only authorized users are granted system access. Role-based permissions enforced.
- AC.1.002: Access is limited to company-owned devices registered via MDM.
- AC.1.003: External system connections (e.g., USB drives, unsanctioned cloud apps) are disabled.
- AC.1.004: Data transfer to/from external systems is limited to approved cloud services.

Awareness and Training (AT):

- AT.1.001: Annual mandatory cybersecurity training provided to all staff via LMS; tracked and certified.

Audit and Accountability (AU):

- AU.1.001: Microsoft 365 logs, firewall logs, and endpoint logs are retained for 90 days.
- AU.1.002: Access to logs is limited to authorized IT administrators; read-only storage enforced.

Identification and Authentication (IA):

- IA.1.001: All users have unique IDs linked to organizational email accounts.
- IA.1.002: System access requires strong passwords and MFA.

Media Protection (MP):

- MP.1.001: All storage media is sanitized using DoD-approved methods before disposal or reuse.

Physical Protection (PE):

- PE.1.001: Offices and server rooms secured with badge access, logs, and CCTV.

- PE.1.002: Visitors are escorted and logged in via a manual visitor logbook.
- PE.1.003: Badge reader data retained for 30 days; reviewed monthly.
- PE.1.004: Physical media is securely stored; USB ports are locked via policy.

System and Communication Protection (SC):

- SC.1.001: Firewalls control traffic at all boundaries; email and web filters in place.
- SC.1.002: Public systems (e.g., website) are isolated in a separate subnet from internal systems.

System and Information Integrity (SI):

- SI.1.001: Microsoft Defender updates are automated daily; incident response playbook is in place.

5. RISK ASSESSMENT AND GAP IDENTIFICATION

A formal risk assessment is performed annually and whenever there is a significant system change. Risks are ranked using a 5x5 likelihood-impact matrix. Any gaps are documented in the POA&M with assigned corrective action timelines.

6. MAINTENANCE AND MONITORING

Security controls are continuously monitored through:

- Automated alerts for unauthorized access attempts
- Scheduled reviews of access permissions
- Monthly firewall and audit log analysis
- Bi-annual internal audits

7. CONTINGENCY PLANNING

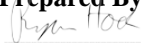
- Weekly encrypted backups via OneDrive for Business
- Disaster Recovery Plan reviewed and tested semi-annually
- All employees are briefed on incident response procedures

8. DOCUMENTATION CONTROL

- This SSP is version controlled and updated quarterly or upon change
- Change logs and version history maintained in SharePoint with restricted access

9. CONCLUSION

This SSP confirms that St. Michael LLC has implemented and maintains the required cybersecurity practices under CMMC 2.0 Level 1 to protect Federal Contract Information (FCI). It reflects a strong commitment to security, compliance, and operational excellence across all federal engagements.

Prepared By:

 Ryan Hoek
 Chief Executive Officer
 St. Michael LLC

