SpendLogic®

Technical Specification Datasheet

Overall Security Posture

SpendLogic is a SaaS solution with years of experience serving defense and Government clients. Our development team is comprised of professionals specialized in state-of-the-art cybersecurity. We are committed to upholding the highest standards of protection. The team remains constantly vigilant and updated with recent exploits and vulnerabilities, ensuring that SpendLogic's application remains especially hardened against emerging threats. This proactive approach, combined with robust infrastructure, advanced encryption, and stringent compliance adherence, positions SpendLogic at the forefront of secure web application providers, guaranteeing the integrity, confidentiality, and availability of client data.

Infrastructure and Hosting

- **Cloud Provider**: AWS GovCloud
- **Hosting Service**: Amazon EC2
- **Security Strategy:** Rooted in NIST 800-171 framework for the protection of confidential unclassified information (CUI)
- **Network Security**: Each SpendLogic instance is given its own network, virtually air-gapping each of our client systems for enhanced isolation and security. We employ strict port management, with only two encrypted ports open to the internet for application exposure and server management. Both ports are protected by large asymmetric key distribution (4096 RSA initiated encryption).

Authentication and Access Control

- **Authentication Mechanism**: SAML-driven Single Sign-On (SSO)

Compliance and Encryption Standards

- **Compliance**: Fully FIPS compliant systems.
- **Encryption for Data in Transit**: Utilizes the latest AES encryption standards.
- **Encryption for Data at Rest**: All storage volumes encrypted at rest.
- **Access Control:** Based on the model of least privilege and stringent control.

Database Management and Security

- **Database Engine**: MySQL, enhanced with hashing and salting techniques.

- **Database Network Exposure**: Strictly internal, with no direct exposure to the internet.
- **Data Security Measures**: Beyond standard encryption, additional security layers are implemented for enhanced protection.

Security Practices and Protocols

- **Third-Party Integrations**: Absence of third-party integrations or data agreements within the application, minimizing external security risks.
- **Security Audits**: Monthly vulnerability scans and frequent penetration testing conducted by an independent, specialized third-party team.
- **Continuous Monitoring**: Ongoing surveillance and assessment, including Dark Web scanning, to uphold the highest security standards.