Principal Service Commitments and System Requirements for Marinade Finance

Introduction

This document outlines the principal service commitments and system requirements as per SOC 2 standards from AICPA.

Security Principle

Service Commitments:

1. **Data Protection:** Marinade Finance commits to protecting user data through encryption both in transit and at rest.
2. **Access Control:** Implement strict access control measures to ensure that only authorized personnel have access to sensitive data and systems.
3. **Incident Response:** Maintain a robust incident response plan to address any security breaches or vulnerabilities promptly.
4. **User Authentication:** Utilize multi-factor authentication (MFA) for user accounts to enhance security.
5. **Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks.
6. **Smart Contract Security:** Ensure the security of on-chain smart contracts through formal audits and a bug bounty program.

System Requirements:

1. **Encryption:** Use industry-standard encryption protocols (e.g., AES-256) for data at rest and TLS for data in transit.
2. **Access Management:** Implement role-based access control (RBAC) and ensure that access rights are reviewed periodically.
3. **Monitoring and Logging:** Deploy comprehensive monitoring and logging systems to detect and respond to suspicious activities.
4. **Firewall and Network Security:** Use firewalls and intrusion detection/prevention systems (IDS/IPS) to protect the network perimeter.
5. **Patch Management:** Ensure timely application of security patches and updates to all systems and software.
6. **Smart Contract Audits:** Conduct regular audits of smart contracts by reputable security firms and maintain a bug bounty program to incentivize the discovery of vulnerabilities.

Availability Principle

Service Commitments:

1. **Uptime Guarantee:** Marinade Finance commits to maintaining a high level of system availability, with a target uptime of 99.9%. Marinade does not guarantee Solana network's uptime.

2. **Disaster Recovery:** Implement a disaster recovery plan to ensure business continuity in the event of a system failure or natural disaster.
3. **Scalability:** Ensure the platform can scale to handle increased user demand without compromising performance.
4. **Maintenance Windows:** Schedule regular maintenance windows and communicate them to users in advance to minimize disruption.
5. **Redundancy:** Utilize redundant systems and data backups to prevent data loss and ensure continuous operation.

System Requirements:

1. **Load Balancing:** Implement load balancing to distribute traffic evenly across servers and prevent overload.
2. **Backup and Recovery:** Perform regular data backups and test recovery procedures to ensure data integrity and availability.
3. **Failover Mechanisms:** Deploy failover mechanisms to automatically switch to backup systems in case of primary system failure.
4. **Performance Monitoring:** Continuously monitor system performance and resource utilization to identify and address potential bottlenecks.
5. **Cloud Infrastructure:** Leverage cloud infrastructure with built-in redundancy and high availability features.

Conclusion

Marinade Finance is committed to ensuring the security and availability of its staking automation platform on the Solana network. By adhering to the outlined service commitments and system requirements, Marinade Finance aims to provide a secure, reliable, and efficient service to its users, in line with SOC 2 standards from AICPA. The platform's emphasis on smart contract security, robust access control, and disaster recovery planning further strengthens its commitment to user trust and safety.