

Vendor: ApexMacro Technologies Pvt. Ltd.

Document: Security & Risk Assessment

Version: 1.3

Last Updated: March 2024

1. Introduction

ApexMacro Technologies provides cloud-based analytics and data processing services to enterprise customers.

This document outlines ApexMacro's information security practices, controls, and risk management posture.

2. Information Security Governance

ApexMacro maintains an internal information security program overseen by the Security & Compliance team.

Security policies are reviewed annually. Some policies are informal and not centrally documented.

3. Data Encryption

Encryption in Transit: All data is encrypted using TLS 1.2 or higher. Control implemented and effective.

Encryption at Rest: Sensitive data is encrypted in most systems, but some legacy systems lack consistent enforcement.

Control partially implemented.

4. Access Control

Role-based access controls are enforced. Quarterly access reviews are conducted, but removal of unnecessary access

is not consistently tracked.

Multi-Factor Authentication:

MFA is enforced for VPN and admin access but not all internal applications.

5. Logging & Monitoring

Logs are retained for 90 days. Monitoring gaps and alerting weaknesses have been identified.

6. Vulnerability Management

Monthly vulnerability scans are performed. Remediation timelines are not formally defined.

7. Incident Response

An Incident Response Plan exists, but testing and customer notification procedures are incomplete.

8. Backup & Disaster Recovery

Daily backups are performed. Disaster recovery testing is irregular.

9. Vendor & Subprocessor Management

Subprocessors are not consistently disclosed and due diligence is informal.

10. Compliance & Certifications

SOC 2 certification is in progress. Vendor certification verification is inconsistent.

11. Privacy & Data Protection

No formal data classification policy exists. Data subject rights handling is informal.

12. Service Level Commitments

Uptime SLAs and credit mechanisms are not formally defined.

13. Summary of Known Risks

Inconsistent encryption at rest, monitoring gaps, weak subprocessor governance, and incomplete incident response procedures.