Alpha Fund – SOC 2 Type 2 Report (Expanded Condensed Version)

Purpose and Scope:

This synthesized SOC 2 Type 2 report summarizes the control environment and operational safeguards of Kolide, Inc., the primary service organization supporting Alpha Fund's IT and data infrastructure. The audit, conducted by Prescient Assurance, covered the six-month period from January 1 to June 30, 2024, and evaluated controls under the Trust Services Criteria for Security.

1. Management Assertion:

Kolide's management asserts that the system was appropriately designed, implemented, and operated effectively to meet its service commitments related to data protection, confidentiality, and system availability. The report includes all relevant control descriptions, testing results, and auditor observations.

2. Auditor's Opinion:

The independent auditor concluded that, in all material respects, the system was designed and operated effectively throughout the audit period. No significant control deficiencies were identified. Testing confirmed the effective operation of access control, data protection, change management, and incident response controls.

3. System Overview:

Kolide provides a cloud-based endpoint security platform used by Alpha Fund and its portfolio companies to manage endpoint compliance, data protection, and user access. The system architecture is composed of a SaaS console, endpoint agents, monitoring dashboards, and integrations with identity providers such as Okta.

Key infrastructure components include:

- **Heroku Cloud Services** for containerized deployment and managed databases.

- **PostgreSQL and Redis** databases for transactional storage and caching.

- **GitHub** for version control and change management.

- **Google Workspace and Slack** for communication and collaboration.

- **Vanta** for continuous compliance monitoring.

4. Security and Control Environment:

Kolide enforces strong governance through defined policies, procedures, and technical controls. Policies cover code of conduct, risk management, data retention, and vendor management. Employees undergo security training annually, and access rights are reviewed quarterly. Background checks are performed for all staff with privileged access.

The control environment is structured around five trust service principles:

- **Security:** Multi-factor authentication, firewalls, intrusion detection, and encryption at rest and in transit.

- **Availability:** Cloud redundancy, real-time monitoring, and incident escalation procedures.

- **Processing Integrity:** Automated change tracking and peer review of code changes.

- **Confidentiality:** Role-based access control and encrypted storage of sensitive data.

- **Privacy:** GDPR-aligned data processing and deletion procedures.

5. Risk Assessment and Mitigation:

Kolide performs a comprehensive risk assessment annually, mapping threats to security objectives. Risks are classified as low, medium, or high, with corresponding mitigation plans. Incident management procedures define escalation paths and post-incident root-cause analysis. The company maintains insurance coverage for cybersecurity and business interruption risks.

6. Control Testing and Results:

During the audit period, 47 key controls were tested. These included:

- Logical access provisioning and deprovisioning.

- Vulnerability scanning and patch management.

- Data backup integrity verification.

- Change management review and approval.

- Incident response testing and documentation.

All controls tested were found to be operating effectively. Sampling methodologies included inquiry, observation, inspection, and re-performance. The testing scope excluded subservice organization controls managed by Heroku; however, Heroku’s SOC 2 report was reviewed and found satisfactory.

7. Complementary User and Subservice Controls:

Kolide relies on Heroku for physical and environmental security. Users (such as Alpha Fund) are responsible for implementing complementary access and data governance controls. These include endpoint compliance, MFA enforcement, and internal monitoring.

8. Continuous Improvement:

Kolide maintains a formal continuous improvement program for its security operations. Post-audit recommendations are documented and tracked through its governance system. Planned initiatives for 2025 include automation of incident response workflows, expansion of vulnerability detection coverage, and ISO 27001 certification alignment.

Conclusion:

Kolide, Inc. maintains an effective control environment that provides reasonable assurance that system objectives were achieved. The SOC 2 Type 2 audit validates Alpha Fund’s reliance on Kolide’s infrastructure as secure, compliant, and aligned with AICPA Trust Services Criteria.