CYBERSECURITY & DATA PROTECTION OVERVIEW

Assetlink is committed to protecting the confidentiality, integrity, and availability of the data entrusted to us by our clients, partners, and stakeholders. As a technology-driven financial platform, security is a core element of our operations, systems and culture. We have adopted a layered approach that includes comprehensive policies, robust technical and administrative safeguards, and continuous monitoring to protect client data and infrastructure.

SECURITY CONTROLS

Security Governance & Program Oversight

Assetlink has developed and maintains a formal information security program that is aligned with industry best standards such as NIST CSF and SOC 2. The program is overseen by security leadership and supported by a cross-functional team across engineering, operations, and compliance.

Risk Management

We follow a risk-based approach to cybersecurity. Risk assessments are conducted at least annually with identified issues prioritized and tracked through a risk management process. This allows Assetlink to allocate adequate resources to protecting critical systems and data while proactively addressing evolving threats.

Access Control

Access to systems and data is restricted to only authorized users and based on the principle of least privilege. User access is granted according to job responsibilities and reviewed periodically to ensure appropriateness.

Data Protection & Privacy

Assetlink has set protecting client and business data as a key priority. Data is classified based on sensitivity and handled according to defined data protection requirements. Safeguards have been implemented such as encryption, secure data storage, data retention and disposal procedures e.t.c.

AI Governance & Responsible Use

Our platform leverages artificial intelligence to enhance its capabilities and as such, we maintain strong governance and oversight. AI system development activities are managed in a manner to emphasize security, transparency, accountability, and risk management. Risk assessment of AI use cases, including data sensitivity and potential impact are conducted at least annually. Monitoring is in place to capture unexpected behavior, model drift, or misuse.

Monitoring, Logging & Detection
We maintain logging and monitoring capabilities to detect potential security events in a timely manner. Security logs are captured to support investigation, incident response, and compliance requirements.

Vulnerability Management
We have developed a vulnerability management program to identify, prioritize, and remediate security weaknesses within timelines based on criticality. We perform vulnerability scans of systems and applications, resolve insecure configurations or vulnerabilities in a timely manner, and perform validation of remediation efforts. In addition, we perform annual independent penetration testing using accredited vendors to evaluate the effectiveness of our security controls and identify potential attack vectors. Any findings are tracked through remediation to closure.

Incident Response
Assetlink has a formal incident response process to ensure prompt identification, containment, and remediation of security incidents. The incident response plan is designed to minimize impact, support recovery, and meet stakeholder notification obligations when required.

Business Continuity & Resilience
To support stable delivery of services to our clients, Assetlink maintains an operational readiness and resilience in the occurrence of a disruptive event. Data is backed up on a cadence based on criticality, recovery procedures are documented, and business continuity processes are tested annually.

Security Awareness & Training
We promote a culture of security awareness and personnel receive periodic training to reinforce their responsibilities related to information security and data protection. In addition to a mandatory security awareness training, specialized training is provided to personnel commensurate with their responsibilities or privileges.

Compliance and Assurance
Assetlink undergoes independent third-party assessments, including SOC 2 examinations, to evaluate the design and effectiveness of security controls. Reports may be made available to qualified parties upon request after appropriate confidentiality obligations have been met.

This document is intended to provide a high-level overview of Assetlink's cybersecurity practices and does not disclose sensitive security details that could increase risk.