Security Statement

Effective Date: July 1, 2026

1. Overview

This Security Statement describes the administrative, technical, organizational, and physical safeguards used or designed to be used by LKS BROTHERS LLC, doing business as LKSB ("LKS BROTHERS LLC," "LKSB," "we," "us," or "our") to protect information that we collect, receive, process, store, transmit, or maintain in connection with our website, business activities, investment-related activities, venture capital activities, market-entry services, partnership discussions, investor communications, data rooms, vendor relationships, and other interactions that link to or reference this Security Statement.

LKSB is committed to protecting the confidentiality, integrity, and availability of information in our possession or control, including personal information, investor-related information, business contact information, transaction materials, due diligence information, confidential business materials, and other sensitive data.

This Security Statement is intended to provide a high-level description of our security approach. It does not disclose confidential details of our systems, controls, architecture, incident response procedures, or security configurations. Specific security obligations, if any, may be addressed in separate written agreements, fund documents, investor agreements, data processing agreements, vendor agreements, confidentiality agreements, or other binding documents.

2. Scope of this Security Statement

This Security Statement applies to information processed in connection with the Services, including our website, online forms, email communications, investor or partner inquiry channels, business development materials, data rooms, due diligence processes, internal business systems, cloud-based platforms, and other systems or workflows operated by or on behalf of LKSB.

This Security Statement does not apply to third-party websites, platforms, applications, data rooms, payment systems, communication tools, cloud environments, or services that are not controlled by LKSB, even if they are linked from our website or communications.

Where a specific written agreement provides different or more specific security requirements, that written agreement will govern to the extent it conflicts with this Security Statement.

3. Security Governance and Risk Management

LKSB maintains, or is designed to maintain as the business develops, an information security governance framework appropriate to the nature, scale, complexity, and risk profile of our operations.

Our security governance approach may include:

- assignment of responsibility for information security oversight;
- risk-based security policies, standards, and procedures;
- periodic review of security risks, control effectiveness, and business changes;
- coordination among management, legal, compliance, technology, operations, and external advisors where appropriate;

- consideration of cybersecurity, privacy, legal, regulatory, investor, vendor, and reputational risk;
- documentation of key security decisions, risk assessments, and remediation actions where appropriate.

As LKSB expands into investment finance, venture capital, private investment, or regulated activities, our security governance framework may be updated to address applicable regulatory, contractual, investor, and operational requirements.

4. Information Security Program

LKSB implements and maintains, or is designed to implement and maintain, a risk-based information security program intended to protect information against unauthorized access, acquisition, use, disclosure, alteration, loss, destruction, or disruption.

The program may include administrative, technical, and physical safeguards designed to:

- identify and assess reasonably foreseeable internal and external risks;
- protect sensitive systems and information;
- detect potential security events or unauthorized activity;
- respond to and contain security incidents;
- support recovery of business operations and information assets;
- monitor third-party service provider risks;
- maintain records of relevant security practices and incidents where appropriate.

The specific controls used by LKSB may vary based on the sensitivity of the information, the system involved, the nature of the business relationship, the applicable legal requirements, and the operational maturity of the relevant process.

5. Data Classification and Handling

LKSB may classify information based on sensitivity, business importance, legal requirements, confidentiality obligations, investor expectations, and potential impact if the information is compromised.

Information that may require heightened protection includes:

- personal information;
- investor and prospective investor information;
- know-your-customer, know-your-investor, anti-money laundering, sanctions, and diligence information;
- financial information, account information, tax information, and source-of-funds information;
- fund documents, offering materials, subscription materials, investor communications, capital call materials, and distribution information;
- business plans, transaction materials, non-public project materials, confidential partner materials, and trade secrets;
- system credentials, access tokens, API keys, authentication data, security logs, and internal security documentation.

We seek to apply handling restrictions, access limitations, retention practices, and security controls that are appropriate to the sensitivity and intended use of the information.

6. Data Minimization and Purpose Limitation

LKSB seeks to collect and process only information that is reasonably necessary and proportionate for legitimate business, operational, compliance, legal, investor, transaction, security, or relationship management purposes.

Users, prospective investors, partners, vendors, and counterparties should not submit highly sensitive, regulated, confidential, privileged, or unnecessary information unless LKSB has requested it for a specific purpose or has provided an appropriate channel for submission.

Where information is no longer needed, LKSB may delete, de-identify, aggregate, archive, restrict access to, or otherwise handle the information in accordance with applicable law, contractual obligations, and record retention practices.

7. Access Control and Authentication

LKSB seeks to limit access to systems and information to authorized personnel, advisors, contractors, service providers, or other parties who have a legitimate business need to access the information.

Access control measures may include:

- role-based access controls;
- least-privilege access principles;
- unique user accounts where appropriate;
- multi-factor authentication for systems containing sensitive information where practicable;
- password and credential management requirements;
- periodic access review and removal of unnecessary access;
- segregation of duties for sensitive workflows where appropriate;
- approval procedures for access to investor, financial, diligence, or confidential project materials.

Users are responsible for maintaining the confidentiality of their credentials and for promptly notifying LKSB of suspected unauthorized access, compromise, or misuse.

8. Encryption and Data Protection

LKSB uses or seeks to use encryption and data protection measures appropriate to the sensitivity of the information, the system involved, and the relevant risk profile.

Such measures may include:

- encryption of sensitive data in transit using industry-standard transport security protocols where supported;
- encryption of sensitive data at rest where supported by applicable systems or service providers;
- secure configuration of cloud storage, data rooms, and document repositories;
- restricted sharing links, expiring access, watermarking, download restrictions, or document permissions where available and appropriate;

- credential protection, key management, and access logging where supported;
- data backup and recovery measures where appropriate.

No encryption or technical safeguard can eliminate all risk. LKSB uses reasonable measures designed to reduce risk, but cannot guarantee absolute security.

9. Secure Systems, Cloud, and Network Controls

LKSB may use cloud-based platforms, hosted applications, secure document repositories, investor portals, email systems, customer relationship management systems, analytics tools, collaboration tools, and other technology services to operate its business.

Security controls may include:

- firewalls, network protections, and secure configuration practices where applicable;
- segmentation or logical separation of sensitive systems or datasets where appropriate;
- secure administration of cloud accounts and workspaces;
- restriction of administrative privileges;
- endpoint protection and device security controls where appropriate;
- secure backup, logging, and recovery procedures;
- use of reputable third-party platforms that provide security features appropriate to the intended use.

LKSB does not guarantee that third-party technology platforms or networks will be uninterrupted, error-free, or immune from unauthorized access or service disruption.

10. Vulnerability Management and Security Testing

LKSB seeks to identify, assess, prioritize, and remediate security vulnerabilities in a risk-based manner.

Vulnerability management practices may include:

- secure system configuration reviews;
- software updates, patching, and version management;
- vulnerability scanning where appropriate;
- penetration testing or independent security assessments for higher-risk systems where appropriate;
- review of vendor security notices and threat advisories;
- remediation tracking for identified issues;
- secure development and change management practices where LKSB develops or customizes technology.

The timing and scope of vulnerability testing may vary based on the system, sensitivity of information, business impact, technical feasibility, and legal or contractual requirements.

11. Logging, Monitoring, and Detection

LKSB may maintain logging, monitoring, alerting, and detection capabilities designed to identify unauthorized access, suspicious activity, system misuse, security events, or operational anomalies.

Monitoring practices may include:

- authentication and access logs;
- administrative activity logs;
- data room or document access logs where available;
- email and collaboration platform security alerts;
- cloud platform security monitoring;
- network or endpoint alerts where applicable;
- review of unusual login activity, permission changes, file downloads, or data access patterns.

LKSB may monitor, preserve, review, or disclose activity information where necessary to operate systems, maintain security, investigate incidents, enforce terms, comply with law, or protect LKSB, users, investors, partners, counterparties, vendors, or others.

12. Security Incident Response

LKSB maintains, or is designed to maintain, procedures to assess, investigate, contain, remediate, document, and recover from security incidents that may affect information, systems, business operations, or third-party services.

Incident response procedures may include:

- internal escalation and triage;
- incident classification and impact assessment;
- containment of affected accounts, systems, files, or workflows;
- preservation and review of relevant logs and records;
- coordination with technology providers, legal counsel, forensic advisors, insurers, regulators, or law enforcement where appropriate;
- remediation of identified vulnerabilities or control gaps;
- post-incident review and improvement actions.

Where required by applicable law, contract, or regulatory obligation, LKSB will provide notices to affected individuals, investors, clients, counterparties, regulators, or other relevant parties within the required timeframe and in the required manner.

13. Business Continuity and Disaster Recovery

LKSB seeks to maintain business continuity and disaster recovery practices appropriate to the nature and maturity of our operations.

Such practices may include:

- backup and recovery procedures for important business information;
- use of cloud-based systems with availability and recovery features;
- alternative communication channels for urgent business or investor communications;
- continuity planning for key business processes;
- periodic review of critical vendors and system dependencies;
- recovery procedures for cyber incidents, outages, data loss, natural disasters, or other disruptions.

Business continuity and disaster recovery capabilities may depend on third-party platforms, internet connectivity, cloud service providers, and other external services that are not fully within LKSB control.

14. Third-Party and Vendor Security

LKSB may engage third-party service providers, advisors, consultants, technology platforms, cloud providers, data room providers, compliance providers, fund administrators, payment processors, analytics providers, marketing platforms, and other vendors that may process information on our behalf or support our operations.

We seek to evaluate third-party service providers based on the nature of the services, sensitivity of information, security capabilities, contractual protections, business importance, and applicable legal or regulatory requirements.

Vendor risk measures may include:

- security and privacy due diligence where appropriate;
- contractual confidentiality, data protection, and security obligations;
- limitations on use and disclosure of information;
- requirements for incident notification where appropriate;
- access controls and least-privilege permissions;
- periodic review of material vendors or higher-risk relationships.

LKSB is not responsible for the independent acts, omissions, policies, systems, or security failures of third-party providers except as required by applicable law or a separate written agreement.

15. Investor Portals, Data Rooms, and Investment Materials

Because LKSB may engage in investment finance, venture capital, private investment, strategic partnership, capital formation, or investor-related activities, certain information may be shared through investor portals, secure data rooms, subscription platforms, diligence platforms, fund administration systems, or other restricted-access channels.

Security measures for such channels may include:

- user-specific access permissions;
- multi-factor authentication where available and appropriate;
- document-level permissions, watermarking, download restrictions, or expiration controls where available;
- access logs and activity reporting where supported;
- segregation of materials by project, fund, investor group, or permission level;
- revocation of access when no longer needed;
- confidentiality notices or separate confidentiality agreements where appropriate.

Access to investor materials, fund materials, offering materials, or transaction materials does not create an investment opportunity, advisory relationship, subscription right, confidentiality obligation, or other legal relationship unless expressly established by separate written documents.

16. Employee, Contractor, and Advisor Safeguards

LKSB seeks to ensure that employees, contractors, advisors, and personnel with access to sensitive information understand their security, privacy, confidentiality, and compliance responsibilities.

Personnel safeguards may include:

- confidentiality obligations;
- role-based access restrictions;
- security and privacy training or awareness activities;
- onboarding and offboarding procedures;
- background checks where appropriate and permitted by law;
- policies for handling investor, personal, financial, diligence, and confidential business information;
- disciplinary or remedial action for violations of security requirements where appropriate.

Access to sensitive information may be limited based on business need, role, engagement, applicable law, and contractual obligations.

17. Physical and Environmental Security

LKSB seeks to protect physical locations, devices, records, and media containing sensitive information through reasonable physical and environmental safeguards.

Such safeguards may include:

- controlled access to offices, workspaces, meeting rooms, file storage, and equipment where appropriate;
- secure storage of physical documents and removable media;
- clear desk or secure document handling practices where appropriate;
- secure disposal or destruction of physical documents and media containing sensitive information;
- use of reputable data centers, cloud providers, or facilities with appropriate physical security controls where third-party hosting is used.

Physical security controls may vary depending on location, work arrangement, vendor environment, and the sensitivity of information handled.

18. Secure Disposal and Retention

LKSB retains information for as long as reasonably necessary for the purposes for which it was collected, to comply with legal and regulatory obligations, to manage business and investor relationships, to maintain records, to resolve disputes, to enforce agreements, and to protect rights and interests.

When information is no longer needed, LKSB may delete, de-identify, aggregate, archive, restrict access to, or securely dispose of the information in accordance with applicable law, contractual obligations, and record retention practices.

Secure disposal practices may include secure deletion of electronic files, revocation of access permissions, destruction of physical records, deletion or expiration of data room access, or other reasonable measures appropriate to the information and system involved.

19. Artificial Intelligence and Automated Tools Security

LKSB may use artificial intelligence, machine learning, automation, analytics, transcription, translation, summarization, document review, or similar tools to support business operations, investor communications, due diligence, research, compliance, and workflow efficiency.

When such tools process information, LKSB seeks to use reasonable measures designed to protect confidentiality, limit unnecessary data use, maintain human oversight where appropriate, and avoid submitting highly sensitive information to tools that are not approved for such use.

Users should not submit sensitive, confidential, privileged, regulated, or investment-related information through public or unsecured AI tools on behalf of LKSB unless authorized and appropriate safeguards are in place.

20. Email, Communications, and Phishing Awareness

Electronic communications, including email, may present risks such as interception, misdelivery, phishing, malware, business email compromise, impersonation, and unauthorized forwarding.

LKSB may use reasonable email and communication security measures such as authentication, spam filtering, malware scanning, secure links, identity verification steps, and out-of-band confirmation for sensitive instructions where appropriate.

Users, investors, partners, vendors, and counterparties should verify payment instructions, wire instructions, bank account changes, subscription instructions, confidential document requests, or unusual communications through a trusted channel before acting on them.

LKSB will not be responsible for losses caused by user negligence, compromised user accounts, third-party email compromise, phishing, or reliance on fraudulent instructions, except where required by applicable law or a separate written agreement.

21. User Responsibilities

Security is a shared responsibility. Users, investors, partners, vendors, advisors, and counterparties are responsible for taking reasonable steps to protect their own information, systems, devices, accounts, credentials, and communications.

You should:

- use strong, unique passwords and multi-factor authentication where available;
- keep devices, browsers, and software updated;
- protect login credentials and avoid sharing accounts;
- use secure networks and avoid transmitting sensitive information over unsecured channels;
- verify the authenticity of LKSB communications and payment instructions;
- avoid clicking suspicious links or opening unexpected attachments;
- promptly notify LKSB of suspected unauthorized access, phishing, misdirected information, credential compromise, or suspicious activity.

If you believe that your interaction with LKSB has involved unauthorized access or suspicious activity, contact LKSB promptly using the information in the Contact Us section.

22. No Guarantee of Absolute Security

No method of transmission, processing, authentication, storage, or security control is completely secure. Although LKSB uses reasonable measures designed to protect information, we cannot guarantee that unauthorized access, acquisition, use, disclosure, alteration, loss, destruction, system outage, or misuse will never occur.

The security of information may depend on factors outside LKSB control, including user conduct, third-party service providers, internet infrastructure, device security, software vulnerabilities, malicious actors, and events beyond reasonable control.

This Security Statement does not create any warranty, guarantee, representation, fiduciary duty, advisory duty, or contractual obligation beyond those required by applicable law or expressly stated in a separate written agreement signed or otherwise accepted by LKSB.

23. Regulatory and Legal Considerations

If LKSB or any affiliated entity becomes subject to specific cybersecurity, privacy, financial services, investment adviser, broker-dealer, fund, consumer financial information, or other regulatory requirements, LKSB may update its policies, procedures, disclosures, controls, and contracts to address those requirements.

Where applicable, LKSB may consider legal and regulatory frameworks relating to customer information safeguards, privacy, incident response, vendor oversight, record retention, data disposal, investor protection, anti-fraud, securities regulation, and cybersecurity governance.

This Security Statement is not intended to summarize all legal obligations that may apply to LKSB, its affiliates, investors, partners, vendors, or users. Specific legal obligations may depend on the entity, activity, jurisdiction, data type, contractual relationship, and regulatory status involved.

24. Changes to this Security Statement

LKSB may update this Security Statement from time to time to reflect changes in our practices, systems, technologies, business operations, legal requirements, regulatory expectations, or risk environment.

When we update this Security Statement, we will revise the Effective Date above or otherwise indicate that changes have been made. The updated version will apply when posted or otherwise made available, subject to applicable law and any separate written agreement.

25. Contact Us

If you have questions about this Security Statement, our security practices, or a suspected security issue involving LKSB, please contact us at:

LKS BROTHERS LLC
Doing business as LKSB
Email: info@lksbrothers.com
Address: Las Vegas, Nevada, United States

If your message involves a suspected security incident, please include enough information for LKSB to evaluate the issue, such as the date and time of the event, affected systems or communications, relevant screenshots or headers where appropriate, and a description of the suspected issue. Do not include unnecessary sensitive information in your initial report.