

BOARD OF DIRECTORS CHARTER

SEREEL TECHNOLOGIES, INC.

BOARD OF DIRECTORS CHARTER

Version: 2.0

Adopted: March 11, 2026

1. PURPOSE OF CHARTER

Pursuant to the Fifth and Seventh paragraphs of the Certificate of Incorporation of Sereel Technologies Inc., this Charter forms part of the bylaws of the Company. It also sets out the role, composition, responsibilities, and operating procedures of the Board of Directors (the "Board") of Sereel Technologies, Inc., a Delaware C-corporation ("Sereel" or the "Company"). The Board is the highest governing body of the Company and is responsible for overseeing management, safeguarding stakeholder interests, and ensuring the Company operates with integrity, in compliance with applicable laws and regulations, and in alignment with its mission to build blockchain-based capital markets infrastructure for institutional clients.

2. PURPOSE OF THE BOARD

The Board serves two broad purposes: **compliance** and **performance**.

Compliance. The Board is responsible for ensuring that the Company is compliant with all applicable rules and regulations from governing institutions, including but not limited to Delaware corporate law, securities regulations, data protection laws, financial services regulations, and digital asset licensing requirements in each jurisdiction where the Company operates. The Board shall remain current on regulatory developments and hold management accountable for compliance obligations.

Performance. The Board shall hold the CEO accountable for the conduct of the Company's operations, the development and maintenance of strategy, and the integrity of the information it communicates to stockholders, investors, regulators, and the public. The Board shall guide the Company in pursuit of its mission to democratize access to capital markets through tokenization, custody, and compliance infrastructure.

3. MISSION AND VALUES

Sereel Technologies exists to democratize access to capital markets through tokenization, custody, and compliance infrastructure. The Board shall guide the Company in pursuit of this mission while upholding the following principles:

- Fiduciary responsibility to stockholders and stakeholders
 - Transparency and accountability in governance
 - Ethical conduct in all business dealings
 - Sound risk management and internal control practices
 - Commitment to information security and data protection
-

4. BOARD COMPOSITION

4.1 Structure

The Board shall be elected by shareholders and consist of no fewer than three (3) and no more than seven (7) directors, composed of:

- **Executive Directors:** The Chief Executive Officer and such other officers as the Board deems appropriate.
- **Investor Directors:** Representatives designated by lead investors in accordance with the Company's stockholders' agreement or investor rights agreement, as applicable.
- **Independent Advisors:** Non-executive advisors who provide strategic counsel and independent oversight. Advisors serve at the invitation of the Board and may participate in Board deliberations. Advisor voting rights, if any, shall be defined in their respective advisory agreements.

4.2 Current Composition

Name	Role	Type
Lance Davis	CEO & Board Chair	Executive Director
Fredrick Waihenya	CTO	Executive Director
Désiré Nzengou	—	Director / Advisor
Paul Reynolds	—	Director / Advisor

4.3 Qualifications

Directors and advisors shall possess the experience, integrity, and judgment necessary to oversee the Company's strategy, operations, and risk profile. The Board shall collectively have

competency across the following domains: blockchain and digital asset technology, financial services and capital markets, information security and compliance, legal and regulatory affairs, and general management.

4.4 Term and Removal

Directors shall serve until their successors are duly elected or appointed, or until their earlier resignation, removal, or death. Directors may be removed with or without cause by stockholder vote in accordance with Delaware law and the Company's certificate of incorporation and bylaws.

5. ROLES AND RESPONSIBILITIES

5.1 Strategic Oversight

The Board shall:

- Review and approve the Company's strategic plan, annual budget, and key business objectives.
- Oversee execution of the Company's business strategy, including product development, go-to-market initiatives, partnerships, and geographic expansion.
- Approve policies and procedures; otherwise approve material transactions, including fundraising activities, equity issuances, acquisitions, strategic partnerships, and any single expenditure or commitment exceeding \$50,000 (or such other threshold as the Board may establish).
- Review and approve the Company's organizational structure and key executive appointments.

5.2 Financial Oversight

The Board shall:

- Review the Company's financial performance on at least a quarterly basis, including revenue, burn rate, funding requirements, and cash position.
- Approve annual budgets, financial projections, and material deviations from budget and strategy.
- Oversee the integrity of the Company's financial controls, reporting and accounting practices.
- Ensure the Company maintains adequate insurance coverage.
- Oversee tax compliance and treasury management.

5.3 Risk Management and Internal Control

The Board shall:

- Establish and maintain a risk management and control frameworks appropriate to the Company's size, stage, and risk profile.
- Identify and evaluate the principal risks facing the Company, including operational, financial, strategic, legal, regulatory, cybersecurity, and reputational risks.
- Ensure that management implements and maintains effective internal controls over financial reporting, operations, and compliance.
- Review the adequacy and effectiveness of the Company's internal control environment at least annually.
- Receive and review reports from management on the status of key risks and the effectiveness of mitigation measures.
- Ensure that findings from internal and external audits, compliance assessments, and security reviews are addressed in a timely manner.

5.4 Information Security and Compliance Oversight

Given the nature of the Company's business — handling digital assets, cryptographic material, and sensitive client data — the Board recognizes information security and compliance as critical governance functions. The Board's information security responsibilities are organized across four governance functions: Evaluate, Monitor, Direct, and Communicate.

5.4.1 Evaluation

The Board shall discuss information security regularly and shall not restrict such discussion to annual or semi-annual reports. Specifically, the Board shall:

- Review the status of information security key performance indicators (KPIs), including the adequacy of resources and competencies within the security organization.
- Evaluate information security concerns in new initiatives and projects before granting approval.
- Approve information security KPIs proposed by management.
- Question management's prioritization of security resources and funding.

5.4.2 Monitor

The Board shall:

- Require periodic reviews from qualified third parties (internal audit or independent assessors) to assess the effectiveness of the Company's Information Security Management System (ISMS).

- Receive and review reports from management on information security implications of their activities.
- Review results of security tests, vulnerability assessments, and penetration testing.
- Review how management proposes to handle audit recommendations and require plans for improvement where deficiencies are identified.
- Ensure the Company engages qualified independent auditors for SOC 2 Type II and other applicable compliance examinations.
- Receive regular reports (no less than quarterly) from management or the designated security function on: the status of the ISMS, security incidents and their resolution, compliance certification status (SOC 2, ISO 27001, CMTA, etc.), and material changes to the Company's threat landscape or risk posture.

5.4.3 Direct

The Board shall:

- Instruct the organization to implement and maintain an ISMS aligned with SOC 2 Trust Services Criteria and ISO 27001.
- Require that there is a clearly designated responsible person for information security (such as a Chief Information Security Officer or equivalent) with sufficient authority and organizational standing.
- Ensure that sufficient funding is allocated to information security measures commensurate with the Company's risk profile and regulatory obligations.
- Establish the organization's risk appetite for information security and cybersecurity risks.
- Approve the Company's information security strategy and the plan for ISMS implementation.
- Require clear roles and responsibilities within the security organization.
- Make decisions on how top information security risks should be handled, including whether to pursue cyber risk insurance.
- Review and approve the Company's information security policies at least annually, including but not limited to: Acceptable Use Policy, Access Control Policy, Data Classification and Handling Policy, Incident Response Plan, Business Continuity and Disaster Recovery Plan, Vendor and Third-Party Risk Management Policy, and Cryptographic Key Management Policy.
- Ensure information security and privacy management processes are integrated with the Company's strategic and operational planning processes.
- Ensure the Company maintains a formal incident response capability and that significant security incidents are escalated to the Board promptly.

- Oversee regulatory compliance, including compliance with applicable data protection laws (GDPR, CCPA, and other jurisdictional requirements), financial services regulations, and any VASP or digital asset licensing requirements in jurisdictions where the Company operates.

5.4.4 Communicate

The Board shall:

- Share best governance practices across institutional boundaries where appropriate, including with industry bodies and peer organizations.
- Ensure that the Company collaborates with suppliers, partners, and other organizations on improving cyber resilience.
- Foster a positive information security culture within the organization, led by the Board's own example and commitment.
- Review management's plans for collaborations with suppliers and sector organizations on cybersecurity matters.
- Review and support the Company's information security awareness program and question how the organization can best share knowledge and collaborate with partners.

5.5 Legal and Ethical Oversight

The Board shall:

- Ensure the Company operates in compliance with applicable laws and regulations, including Delaware corporate law, securities regulations, and international regulatory requirements.
- Establish and enforce a Code of Conduct applicable to all directors, officers, employees, and contractors.
- Oversee the Company's policies on conflicts of interest, related-party transactions, and whistleblower protections.
- Review and approve material legal matters, litigation, and regulatory actions.

5.6 Human Capital Oversight

The Board shall:

- Approve executive compensation, equity grants, and incentive structures.
- Review the Company's organizational health, hiring plans, and key personnel decisions.
- Ensure the Company maintains appropriate employment agreements, confidentiality obligations, and ISMS compliance requirements for all personnel (as set forth in the Company's Employment Agreement template).
- Oversee compliance with background verification requirements for personnel with access to sensitive systems and data.

- Ensure adequate personnel training is provided to enable all employees, contractors, and relevant third parties to comply with security and privacy requirements in applicable legislation, executive orders, policies, directives, instructions, standards, and guidelines. Such training shall be conducted upon onboarding, periodically thereafter (at least annually), and upon material changes to policies or regulations.
-

6. BOARD CULTURE

The Board is committed to fostering a culture of transparency, integrity, and accountability within the organization. The Board commits to ensuring the confidentiality, integrity, and availability of the Company's services, systems, and data.

The Board shall lead by example in adhering to the Company's information security policies and ethical standards. Directors shall promote open communication, constructive challenge, and an environment in which management and employees feel empowered to raise concerns without fear of retaliation. The Board recognizes that strong governance culture is foundational to the Company's ability to earn and maintain the trust of clients, regulators, partners, and investors.

7. BOARD OPERATIONS

7.1 Meetings

The Board shall meet at least four (4) times per year (quarterly), with additional meetings convened as necessary. Meetings may be held in person or by video or telephone conference. Meeting agendas shall include topics required for the compliance certifications the Company is pursuing or maintaining, including SOC 2 Trust Services Criteria, and shall ensure that information security and compliance matters receive regular Board-level attention.

The CEO will chair Board meetings; otherwise another member of the Board will chair.

7.2 Quorum

A quorum for the transaction of business shall consist of a majority of the directors then serving on the Board.

7.3 Notice

Written notice of Board meetings shall be provided to all directors at least five (5) business days in advance, except in cases of emergency where reasonable notice shall suffice. Notice shall include the meeting agenda and any materials for Board review.

7.4 Minutes

Proceedings of all meetings shall be recorded and maintained as part of the Company's corporate records. Minutes shall document attendance, key discussions, resolutions, and any dissenting opinions. Minutes shall be signed by the Co-Founders (or, in their absence, by the Board Chair and one additional director) and communicated to all Board members. Any proposed changes to the minutes shall be reviewed and approved by the Board at the subsequent meeting.

7.5 Written Consent

The Board may act without a meeting by unanimous written consent of all directors, in accordance with Delaware General Corporation Law Section 141(f).

7.6 Board Materials

Management shall provide the Board with timely, accurate, and complete information necessary for informed decision-making and execution of its purpose and other obligations. Standing Board reporting shall include: financial statements and KPIs, product and technology updates, compliance and security status reports (including information security KPIs), fundraising and investor relations updates, policies, procedures, risk frameworks, and material risk developments.

8. COMMITTEES

The Board may establish committees as it deems necessary and appropriate. At minimum, as the Company scales, the Board anticipates establishing:

8.1 Audit and Risk Committee

Responsible for overseeing financial reporting, internal and external audit functions, risk management, and the effectiveness of internal controls.

8.2 Compensation Committee

Responsible for overseeing executive compensation, equity incentive plans, and overall compensation philosophy.

8.3 Governance and Nominating Committee

Responsible for Board composition, director nominations, governance policies, and periodic Board self-assessment.

Each committee shall operate under a written charter approved by the Board. Until such committees are formally constituted, the full Board shall retain responsibility for all committee functions.

9. CONFLICTS OF INTEREST

9.1 Disclosure

Each director shall promptly disclose to the Board any actual or potential conflict of interest relating to any matter under Board consideration.

9.2 Recusal

A conflicted director shall recuse themselves from deliberation and voting on any matter in which they have a material personal, financial, or professional interest.

9.3 Related-Party Transactions

All related-party transactions shall be disclosed to, reviewed by, and approved by the disinterested members of the Board. Terms of such transactions must be no less favorable to the Company than those available from unaffiliated third parties.

10. DIRECTOR AND ADVISOR OBLIGATIONS

All directors and advisors shall:

- Act in good faith and in the best interests of the Company and its stockholders.
 - Exercise the care, skill, and diligence that a reasonably prudent person would exercise in comparable circumstances.
 - Comply with the Company's confidentiality and non-disclosure obligations, including the NDA executed upon appointment.
 - Comply with the Company's information security policies to the extent they access Company systems, data, or Confidential Information.
 - Promptly report any suspected security incidents, compliance violations, or ethical concerns to the Board Chair or designated officer.
 - Attend Board meetings regularly and prepare adequately for deliberations.
-

11. BOARD EVALUATION

The Board shall conduct an annual self-assessment to evaluate its effectiveness, composition, and governance practices. The assessment shall consider whether the Board is fulfilling its

responsibilities under this Charter, including its oversight of risk management, internal controls, and information security.

12. ACCESS TO MANAGEMENT AND ADVISORS

Directors shall have full and unrestricted access to the Company's management and, where necessary, to independent legal, financial, and technical advisors at the Company's expense, subject to coordination through the Board Chair.

13. INDEMNIFICATION

Directors and advisors shall be indemnified by the Company to the fullest extent permitted by Delaware law and the Company's certificate of incorporation and bylaws. The Company shall maintain directors' and officers' (D&O) liability insurance at levels appropriate to the Company's size and risk profile.

14. REPORTING

Proceedings of all Board meetings are recorded and maintained for future reference. Meeting minutes shall be signed by the Co-Founders and communicated to all Board members, with any proposed changes approved by the Board. Board meeting agendas and discussions shall include topics required per the compliance certifications the Company is achieving, including SOC 2 Trust Services Criteria. The Board shall receive standing reports from management on financial performance, product and technology updates, compliance and security status, fundraising updates, and material risk developments.

15. PUBLICATION OF THE CHARTER

Key features of this Charter shall be outlined in the Company's Annual Report or equivalent annual disclosure to stockholders. A summary of the Charter's principal provisions — including Board composition, committee structure, and governance responsibilities — shall be made available to investors and stakeholders as appropriate.

16. REVIEW OF CHARTER

The Board shall review this Charter at least annually to ensure it remains consistent with the Board's objectives, responsibilities, and the Company's regulatory and compliance

environment. This Charter may be amended at any time by a resolution of the Board.

17. ADOPTION

This Charter was adopted by resolution of the Board of Directors of Sereel Technologies, Inc. on March 11, 2026.

APPROVED AND ADOPTED:

Lance Davis, CEO & Board Chair

Sereel Technologies, Inc.

Date: March 11, 2026

Fredrick Waihenya, CTO

Sereel Technologies, Inc.

Date: March 11, 2026

Désiré Nzengou

Date: March 11, 2026

Paul Reynolds

Date: March 11, 2026