

Information Technology Policy

SERNET Financial Services Private Limited

Version 1.0 • Effective 12 October 2026

Next scheduled review: by 12 October 2027

1. Purpose and policy status

SERNET Financial Services Private Limited (SERNET) shall govern its technology to protect the confidentiality, integrity and availability of investor and business information, support dependable distribution services and meet applicable legal, regulatory and contractual obligations.

Version 1.0 is approved for publication and effective from 12 October 2026. The next scheduled review is due by 12 October 2027. This policy sets governance requirements; its publication is not certification that every control has been implemented or independently audited.

2. Business and technology boundaries

SERNET acts as an AMFI-registered mutual fund distributor (ARN 35275; EUIN E025145) and APMI-registered PMS distributor (APRN 10097; EUIN E19955). Both registrations are valid until 28 October 2028. SERNET is not itself a stock broker, Research Analyst, Registered Investment Adviser or portfolio manager.

The policy applies to employees and authorised contractors or vendors accessing SERNET information. It covers the website, internal and client/partner portals, CRM, HR and support systems, business email, cloud services, domains, integrations, devices, records and backups under SERNET control.

Independent AMC, RTA, portfolio-manager, insurance and other product-provider platforms remain subject to their own operational and regulatory responsibilities. An external link or distribution relationship does not transfer their registrations or responsibilities to SERNET. Requirements applicable to a regulated portfolio manager shall not automatically be represented as SERNET distributor obligations.

3. Responsibility assignments

MD & CEO — Bhavesh A Vora: approve the policy, resources, material risk acceptance and time-bound exceptions. CTO — Akshat B Vora: technical owner, responsible for access, inventory, safeguards, monitoring, vendor technical review and recovery evidence.

Compliance Executive — Gaurav V Shah: compliance coordinator for applicability review, policy evidence, record-retention obligations and incident-reporting coordination. This does not appoint him as a statutory compliance officer or CERT-In point of contact without separate authorisation.

CHRO — Bhumika B Vora: coordinate joiner/mover/leaver notifications and training. Ops Manager — Triveni M Suthar: coordinate service continuity and provider escalation. Ops Executive — Arvind Mishra and RM — Shrey Patel: follow approved workflows and report service or security concerns. Formal notification contacts shall be documented and authorised separately.

Identity, devices and permitted use

4. Inventory and lifecycle management

The CTO or authorised delegate shall maintain an inventory of material systems, devices, domains, subscriptions and integrations. Each entry shall identify a business owner, purpose, data classification, criticality, dependencies, vendor, support status and recovery priority. Actual hosting, storage and log locations shall be verified rather than inferred from a provider name.

New services require business approval and proportionate technical, privacy and continuity assessment. On retirement, access and integrations shall be removed, required records preserved, and remaining information securely deleted or returned. Inventory reviews shall occur annually and after material changes.

5. Accounts, access and authentication

Access shall use individually assigned accounts, least privilege and role-based authorisation. Business owners approve requests; the CTO records provisioning and changes. Public website access must remain separate from access to investor, personnel and administrative records. User-editable profile information shall not determine administrative privileges.

CHRO shall promptly notify the CTO when employment, engagement or duties change. Departing users shall have access disabled at the end of authorised access, and immediately where a security risk requires it. Company devices, active sessions, recovery factors and shared-service access shall be reviewed during offboarding.

Privileged access shall be separately approved and reviewed quarterly; other business access shall be reviewed at least annually. These are SERNET review requirements, not a claim of completed reviews. Multi-factor authentication shall be required for privileged cloud, domain/DNS, business-email and administrative accounts wherever supported. Unsupported systems require documented compensating controls and a dated remediation plan.

Passwords shall be strong and unique. Passwords, OTPs, recovery codes and access tokens must not be shared. Secrets shall be kept in approved secure storage, not source code, documents or ordinary chat. Suspected compromised credentials shall be revoked or rotated promptly.

6. Devices, software and acceptable use

Company devices shall be recorded, maintained, patched according to risk and protected with supported software, screen locks and appropriate encryption or endpoint safeguards. Lost or stolen devices must be reported immediately upon discovery.

Personal-device business access requires written manager and CTO approval with defined security and data-removal conditions. Unauthorised software, credential sharing, bulk copying of investor information and personal storage of business records are prohibited. Devices shall be returned and business data securely removed before reassignment or disposal.

Information handling and third parties

7. Privacy, confidentiality and data integrity

Investor, KYC, financial, employee and commercial information shall be classified and handled according to sensitivity. Collection, access, sharing and retention shall be limited to an authorised purpose and applicable consent, agreement or law. Sensitive documents shall use approved restricted channels rather than public or predictable download links.

SERNET shall apply proportionate access controls, secure transmission and storage safeguards, logging and controlled write access. Corrections and material changes to business records shall be traceable. Production information shall not be copied into development or testing without approval and appropriate minimisation or de-identification.

External disclosures shall be limited to the relevant authorised provider or service vendor. Information received from AMCs, RTAs and portfolio managers shall be used only for permitted distribution and servicing purposes. Privacy requests shall follow the published Privacy Policy and any applicable legal exceptions. Confidentiality obligations continue after engagement ends.

No control eliminates all risk. This policy shall not promise absolute security, guaranteed uptime or guaranteed prevention of fraud.

8. Vendors, cloud services and integrations

Material vendors shall be assessed before onboarding and at least annually for information access, security, service dependency, incident notification, subcontracting, continuity, data location, record export and exit arrangements. Contracts and operational arrangements shall address confidentiality and return or deletion of information where applicable.

Vendor privileges and integration credentials shall be restricted, recorded and removed when no longer required. The CTO and compliance coordinator shall establish evidence of the storage, processing and log-retention arrangements required by law. A provider-hosted service does not remove SERNET's applicable responsibilities.

Independent product-provider applications shall be identified as such. SERNET shall coordinate service issues through their authorised channels without suggesting that SERNET manages their underlying investment, execution or custody systems.

9. AI, automation and communications

AI and automation may support approved informational or internal workflows but shall not be represented as regulated investment advice, independent research or assured investment outcomes. Client-facing financial or compliance content requires suitable human review.

Passwords, OTPs, access tokens and unnecessary identifiable KYC, financial or employee records shall not be submitted to unapproved AI services. Approved AI processing requires purpose limitation, vendor review and controls proportionate to the information involved.

Business email and domain changes shall be authorised and checked for service impact. Sender authentication and DNS changes shall be tested against every approved sending service. Suspicious messages and payment requests shall be independently verified through known channels.

Controlled change and incident response

10. Development, change and vulnerability management

Changes to applications, access rules, integrations, infrastructure and DNS shall identify the owner, purpose, impact, approval, testing and rollback arrangements. Changes affecting investor access or sensitive records shall include relevant business review.

Testing shall check both permitted and denied access and essential public services. Releases shall be recorded and monitored. Emergency fixes may proceed to contain a serious risk or restore service, with the reasons documented and retrospective review promptly arranged.

The CTO shall review security alerts and vulnerabilities, prioritise by severity and exposure, assign remediation owners and record verification. Risk-based target dates shall be maintained in an internal remediation register; overdue items require escalation or approved exceptions.

11. Monitoring, incident response and reporting

Critical applications, authentication, business email, domains, integrations and backup jobs shall have proportionate monitoring. Suspected compromise, data exposure, phishing, lost devices or material outages shall be reported immediately to the designated internal contact. Personnel shall preserve evidence and avoid unapproved deletion or investigation.

The incident owner shall record discovery time, scope, affected systems, containment, recovery and communications. The CTO and compliance coordinator shall assess legal reporting duties promptly. Where an incident is reportable under the applicable CERT-In directions, SERNET shall report it within six hours of noticing it or being brought to notice, using available information and supplementing it as permitted. Internal approval or completion of investigation must not delay a mandatory report.

A formally authorised point of contact and reporting channels shall be maintained as required. Notification to affected people, providers, authorities or other parties shall follow the applicable law and contractual duties. The published security contact is not automatically the statutory point of contact.

Material incidents shall have a post-incident review, corrective actions, responsible owners and closure evidence. An internal response procedure shall define escalation, evidence preservation and communications without exposing sensitive operational details publicly.

12. ICT logs and reliable timestamps

SERNET shall enable relevant ICT logs and retain them securely for a rolling minimum of 180 days within Indian jurisdiction as required by the applicable CERT-In directions, or longer where another applicable obligation requires. Access shall be restricted and logs protected against unauthorised alteration or deletion.

The CTO shall verify vendor support and the completeness of authentication, administrative, security and other relevant system logs; evidence of location and retention shall be maintained. ICT clocks shall follow applicable CERT-In time-synchronisation requirements using NPL/NIC servers or an appropriately traceable accurate time source as permitted. Current implementation must be verified before compliance is claimed.

Records, recovery and continuity

13. Record retention and secure disposal

The compliance coordinator and business owners shall prepare a management-approved retention schedule for investor, transaction, KYC, consent, complaints, employee, vendor and audit records. Periods shall follow applicable legal, regulatory and contractual requirements; a single unverified retention period shall not be applied to every category.

The CTO shall implement storage, access, archival and disposal controls. Records subject to a complaint, investigation, litigation hold or regulatory request shall be preserved until authorised release. Disposal shall address relevant copies and backups according to the approved schedule and documented technical constraints.

14. Backups and restoration

Critical records and configurations shall have documented backup arrangements that identify coverage, frequency, retention, protection, responsible owner and restoration steps. The CTO shall monitor backup success and escalate failed or incomplete jobs.

A backup is not evidence of recoverability until restoration is tested. Restore tests shall occur at least annually and after material recovery changes; results shall record data-integrity checks, recovery duration, failures and remedial action.

Recovery time objectives and recovery point objectives shall be set separately for each critical service based on business impact, dependencies, vendor capability and demonstrated recovery results. Management approval is required. Recovery targets and backup frequencies shall be documented internally and validated before assurances are given.

15. Business continuity and provider dependency

The CTO and Ops Manager shall maintain a continuity procedure covering responsible people, alternative communications and work arrangements, provider contacts, restoration sequence, reconciliation and service validation. The procedure shall identify limitations where a third-party provider controls service restoration.

During an outage, investor requests shall be directed only through authorised provider channels. Staff shall not improvise transaction acceptance, promise provider processing times or bypass authentication and payment safeguards. Affected teams shall receive accurate status updates.

A continuity walkthrough or exercise shall occur at least annually. Findings shall have assigned owners and target dates, and the plan shall be updated following material changes or incidents.

16. Training and operational evidence

Employees and relevant contractors shall receive induction and periodic awareness on phishing, credential protection, investor confidentiality, approved data sharing and incident escalation. Roles with administrative or sensitive-data access shall receive appropriate additional guidance.

Evidence shall include approvals, inventory and access reviews, changes, vendor assessments, incidents, retention decisions, restoration tests, exercises and corrective actions. Evidence containing sensitive operational information shall remain restricted rather than be published with this policy.

Review, accountability and contact

17. Review, exceptions and accountability

The policy shall be reviewed at least annually and after a material business, technology, regulatory or incident-driven change. The CTO and compliance coordinator shall propose revisions for management approval and maintain version history and review evidence.

Exceptions shall identify the requirement, reason, scope, risk, compensating controls, owner and expiry or review date. Material exceptions require MD & CEO approval. An exception cannot waive a mandatory legal duty. Suspected policy breaches shall be investigated fairly and handled under applicable employment, contractual and legal procedures.

18. Related public policies and contact

This policy supplements, rather than replaces, SERNET's Privacy Policy, Policies & Procedures, Terms & Conditions, Disclosures and Grievance Redressal. Wording and links shall be maintained consistently across those documents.

For public policy questions, contact compliance@sernetindia.com. Service concerns may also be raised through SERNET's support portal and escalated under Grievance Redressal. Users must never send passwords, OTPs or access tokens with a report.