GLOBAL ALPHA CAPITAL LIMITED

INFORMATION PROTECTION POLICY

DAR ES SALAAM
AUGUST 2025

GLOBAL ALPHA CAPITAL LIMITED

INFORMATION PROTECTION POLICY

Protecting Client Information, Market Data, Corporate Information and Information Systems

Document Owner	Chief Executive Officer / Senior Management	**Approval Authority**	Board of Directors
Policy Custodian	Compliance / Risk Function	**Effective Date**	Upon Board Approval
Version	1.0	**Review Cycle**	At least annually
Classification	Internal – Controlled Document	**Applies To**	All Alpha Capital operations
Supersedes	New Policy	**Next Review**	12 months from effective date
Related Policies	IT, Cybersecurity, Data Protection, BCP, AML/CFT, Records	**Regulatory Context**	Tanzania capital-markets and data-protection framework

1.0 Purpose

This Policy establishes the principles, responsibilities and minimum controls that Global Alpha Capital Limited ("Alpha Capital" or the "Company") shall apply to protect information against unauthorised access, disclosure, use, alteration, destruction, loss or disruption. It is intended to preserve confidentiality, integrity and availability of information while supporting the Company's stock brokerage, investment advisory, fund management, portfolio/wealth management, transaction execution and digital-client services.

The Policy recognises that information is a critical corporate asset and, in a regulated securities business, may also represent client property, confidential market information, personal data, commercially sensitive information or information subject to statutory, contractual and fiduciary obligations.

2.0 **Regulatory and Governance** Context

This Policy shall be implemented in conjunction with applicable laws, regulations, regulatory directives, licence conditions and contractual obligations. In particular, Alpha Capital shall take account of the Capital Markets and Securities Act and applicable CMSA regulations and guidelines, the Personal Data Protection Act, 2022 and applicable regulations, electronic-transactions and communications requirements, AML/CFT obligations, and any applicable requirements of the Dar es Salaam Stock Exchange (DSE), Central Depository and other market infrastructure providers.

The Personal Data Protection Act establishes the framework for collection and processing of personal data and the protection of data subjects, while the CMSA

Electronic Trading Guidelines require confidentiality, integrity and availability controls for electronic securities services. Alpha Capital shall therefore treat information protection as both a governance responsibility and a regulatory-control obligation.

3.0 Scope

This Policy applies to:

(a) All directors, officers, employees, consultants, temporary staff, interns, contractors and other persons authorised to access Alpha Capital information.

(b) All business units and functions, including Brokerage, Investment Advisory, Fund Management, PMS/Wealth Management, Finance, Operations, Compliance, Risk, ICT, HR and Corporate Services.

(c) All information created, received, processed, stored, transmitted or disposed of by or on behalf of Alpha Capital, whether electronic, physical, verbal or recorded in another medium.

(d) All information systems, applications and platforms, including the Broker Back Office (BBO), online Client Portal, corporate website, email, cloud services, endpoint devices, network infrastructure and interfaces with banks, mobile-money operators, DSE/CSDR and other service providers.

(e) Third parties processing Alpha Capital or client information under contract or otherwise on the Company's behalf.

4.0 **Policy** Objectives

(a) Protect client, investor, employee, counterparty and corporate information from unauthorised access or misuse.

(b) Protect the confidentiality of orders, transactions, portfolios, client identities, account information, research, mandates and commercially sensitive information.

(c) Maintain the accuracy and integrity of records, market information and transaction data.

(d) Maintain availability and recoverability of critical systems and information.

(e) Meet applicable legal, regulatory and contractual obligations.

(f) Reduce the likelihood and impact of cyber incidents, fraud, data leakage, operational errors and insider threats.

(g) Establish clear accountability for information ownership, access and handling.

(h) Support secure digital service delivery without unnecessarily restricting legitimate business activity.

5.0 Information Protection Principles

5.1 Need-to-Know and Least Privilege

Access shall be granted only where required for legitimate business purposes and shall be limited to the minimum information and system privileges necessary to perform an authorised role.

5.2 **Confidentiality**

Confidential information shall not be disclosed to any person unless the recipient is authorised and the disclosure is lawful, necessary and appropriately controlled.

5.3 **Integrity**

Information and records shall be protected against unauthorised alteration, deletion, manipulation or corruption. Critical transactions and changes shall be traceable through appropriate logs and approvals.

5.4 **Availability**

Critical information and systems shall be maintained in a manner that supports continuity of client service, trading, settlement, fund administration, regulatory reporting and other essential operations.

5.5 **Data Minimisation and Purpose Limitation**

Alpha Capital shall collect and process only information reasonably required for a legitimate business, legal, regulatory or contractual purpose and shall avoid retaining information longer than necessary, subject to applicable record-retention requirements.

5.6 **Accountability**

Information owners, users, system administrators, vendors and management shall be accountable for the protection of information within their respective responsibilities.

6.0 Information Classification

Information shall be classified according to sensitivity and potential impact of unauthorised disclosure, alteration or loss.

Classification	Typical Examples	Minimum Handling	Disclosure
Public	Approved public reports, published research, public website content, approved marketing material.	May be shared externally after appropriate approval.	Openly releasable.
Internal	Routine internal procedures, operational information, non-	Access limited to Alpha personnel/approved parties with business need.	Internal or authorised recipients.

	public management material.		
Confidential	Client files, account information, portfolio information, contracts, internal financial information, non-public research, staff records.	Need-to-know access; secure transmission/storage; controlled disclosure.	Authorised recipients only.
Restricted / Highly Confidential	Trading orders, credentials, security keys, privileged access information, sensitive personal data, material non-public information, security incidents, critical system configurations.	Strong access controls, encryption where appropriate, enhanced monitoring and senior/owner approval for disclosure.	Strictly limited and documented.

7.0 Roles and Responsibilities

7.1 Board of Directors

The Board shall:

(a) Approve this Policy and provide oversight of information and cyber-risk.

(b) Ensure management maintains appropriate resources and governance arrangements.

(c) Receive material information-security, data-protection and incident reports as appropriate.

7.2 Chief Executive Officer

It is the responsibility of the Chief Executive to:

(a) Ensure implementation of the Policy across the Company.

(b) Allocate appropriate resources and establish management accountability.

(c) Ensure material information-security incidents are escalated to the Board and regulators where required.

7.3 Compliance / Risk Function

(a) Monitor compliance with this Policy and applicable regulatory requirements.

(b) Coordinate risk assessments, control reviews and regulatory reporting.

(c) Maintain oversight of information-security and data-protection incidents and remediation.

7.4 ICT / System Administration

(a) Implement technical safeguards, access controls, backups, logging, patching and system hardening.

(b) Maintain secure configuration and change-management processes.

(c) Support incident detection, containment, recovery and forensic preservation.

7.5 Information Owners

(a) Determine classification, access requirements, retention and acceptable use for information under their control.

(b) Approve access requests and periodic access reviews.

(c) Ensure information is accurate and appropriately protected.

7.6 All Users

(a) Protect credentials and devices and follow approved security procedures.

(b) Use Company information only for authorised purposes.

(c) Immediately report suspected loss, unauthorised access, phishing, malware, misdirected communications or other security incidents.

8.0 Access Control

8.1 User access shall be based on approved roles and business need.

8.2 Privileged and administrative access shall be restricted to authorised personnel and separately controlled.

8.3 Strong authentication shall be required for critical systems and remote access; multi-factor authentication should be used wherever technically available and proportionate to risk.

8.4 User accounts shall be unique and shared accounts shall be prohibited except where technically unavoidable and specifically authorised.

8.5 Access shall be reviewed periodically and immediately upon termination, transfer or material change of responsibilities.

8.6 Dormant, unnecessary and former-employee accounts shall be disabled promptly.

8.7 Access to client wallets, holdings, orders, portfolio information and transaction records shall be subject to enhanced controls and audit trails.

9.0 Passwords, Credentials and Secrets

9.1 Passwords shall be unique, sufficiently strong and never shared.

9.2 Passwords, API keys, tokens, private keys and similar secrets shall not be stored in plain text or communicated through unsecured channels.

9.3 Default credentials shall be changed before production use.

9.4 Where supported, MFA and secure credential-management mechanisms shall be used for privileged and critical services.

9.5 Suspected credential compromise shall be reported immediately and credentials shall be reset or revoked without undue delay.

10.0 Personal Data Protection

10.1 Alpha Capital shall process personal data lawfully, fairly and transparently and shall maintain appropriate technical and organisational measures to protect personal data. The Company shall maintain appropriate arrangements for data-subject rights, lawful processing, retention, secure disposal, third-party processing and personal-data breach management.

10.2 Personal data shall be collected for defined and legitimate purposes and limited to what is reasonably necessary.

10.3 Access to personal data shall be restricted to authorised personnel with a legitimate business need.

10.4 Personal data shall be protected during transmission and storage using appropriate safeguards based on risk and sensitivity.

10.5 Third-party processors shall be subject to appropriate contractual and security requirements.

10.6 Cross-border transfers shall be undertaken only where lawful and after the relevant legal, regulatory and security requirements have been assessed.

10.7 A Data Protection Officer or other designated responsible officer shall perform the duties required by applicable law and Company governance arrangements.

11.0 Client, Trading and Investment Information

11.1 Because Alpha Capital is a regulated capital-markets intermediary, the following information requires heightened protection:

11.2 Client identification, KYC and account-opening information.

11.3 Orders, instructions, execution details, transaction histories and settlement information.

11.4 Client wallets, holdings, portfolio valuations and statements.

11.5 Investment-advisory records, mandates, investment recommendations and research.

11.6 Fund records, investor information, NAV-related information, portfolio holdings and fund transactions.

11.7 PMS/wealth-management portfolio information and client-specific strategies.

11.8 Non-public issuer, transaction, fundraising, listing and corporate-finance information.

11.9 Material non-public information and information subject to confidentiality, fiduciary or contractual restrictions.

11.10 Such information shall not be used for personal benefit, unauthorised trading, unauthorised solicitation, market abuse or any purpose outside the user's authorised responsibilities.

12.0 Electronic Trading, BBO and Online Client Portal

12.1 Systems supporting client access and securities transactions shall be designed and operated with controls appropriate to their risk. At minimum:

12.2 Client authentication and authorisation shall be controlled and auditable.

12.3 Order submission, amendments, cancellations and other material client actions shall be logged.

12.4 System interfaces and APIs shall use secure authentication, authorisation, encryption and appropriate rate-limiting or equivalent controls.

12.5 Data received from DSE, CSDR, banks, MNOs or other third parties shall be clearly distinguished from Alpha Capital-generated records where necessary, and reconciliation controls shall be maintained.

12.6 Market prices, holdings, balances and portfolio values displayed to clients shall be subject to reasonable integrity and reconciliation controls; third-party data limitations shall be appropriately disclosed.

12.7 Production changes affecting trading, client accounts, transaction processing or security controls shall be subject to documented change management and testing.

12.8 Critical systems shall have recovery arrangements and tested backups appropriate to their operational importance.

13.0 Encryption and Secure Transmission

13.1 Sensitive information shall be encrypted in transit over untrusted networks using industry-accepted secure protocols.

13.2 Sensitive information stored on portable devices or removable media shall be encrypted where risk warrants.

13.3 Cryptographic keys and certificates shall be protected, access-controlled and periodically reviewed.

13.4 Confidential information shall not be transmitted through personal email accounts, unapproved messaging applications or other unauthorised channels.

14.0 Email, Messaging and Social Engineering

14.1 Users shall exercise caution with unexpected links, attachments, payment instructions, password-reset requests and requests for confidential information.

14.2 Changes to client or counterparty bank details or other high-risk instructions shall be verified through an approved independent channel where required by procedure.

14.3 Confidential information shall not be disclosed merely because a request appears to originate from a senior employee, client, bank, regulator or supplier.

14.4 Suspected phishing, impersonation or business-email compromise shall be reported immediately.

15.0 Endpoint, Mobile and Remote Working Security

15.1 Company devices shall use supported operating systems, security updates and appropriate endpoint protection.

15.2 Devices used to access Company information shall be protected against unauthorised physical access.

15.3 Lost or stolen devices shall be reported immediately so that access can be revoked or remote protective measures activated where available.

15.4 Remote access shall use approved secure mechanisms.

15.5 Company information shall not be copied to personal devices or personal cloud storage unless specifically authorised and adequately protected.

16.0 Backup, Business Continuity and Disaster Recovery

16.1 Critical information shall be backed up according to documented recovery requirements.

16.2 Backups shall be protected from unauthorised access, corruption and ransomware, including through appropriate segregation or immutability where feasible.

16.3 Recovery procedures shall be documented and tested periodically.

16.4 Business continuity and disaster-recovery arrangements shall identify critical systems, recovery priorities, responsible persons and communication channels.

17.0 Incident Management and Data Breaches

17.1 All actual or suspected information-security incidents shall be reported immediately to the designated ICT, Compliance/Risk or management contact. Incidents include, without limitation, suspected unauthorised access, malware, ransomware, lost devices, accidental disclosure, phishing, compromised credentials, data leakage, fraudulent transactions and material system disruption.

17.2 Incidents shall be recorded, assessed, contained and investigated according to severity.

17.3 Evidence and relevant logs shall be preserved where appropriate.

17.4 Access credentials and compromised systems shall be contained or isolated where necessary.

17.5 Clients, CMSA, PDPC, law-enforcement authorities, market infrastructure providers or other stakeholders shall be notified where required by law, regulation, contract or materiality.

17.6 Post-incident reviews shall identify root causes, control weaknesses and corrective actions.

18.0 Third-Party and Outsourced Service Providers

18.1 Vendors with access to Alpha Capital or client information shall undergo risk-based due diligence before engagement.

18.2 Contracts shall address confidentiality, information security, data protection, permitted use, access controls, incident notification, subcontracting, audit/cooperation rights, data return/deletion and termination arrangements as appropriate.

18.3 Critical service providers shall be monitored periodically based on risk.

18.4 Cloud, API, hosting, software, payment, market-data and other technology providers shall be subject to appropriate security and business-continuity assessment.

19.0 Records Retention and Secure Disposal

Information shall be retained in accordance with applicable legal, regulatory, contractual and business requirements. When the retention period expires and no legal hold or other legitimate reason for continued retention exists, information shall be securely

deleted, destroyed or anonymised using a method appropriate to its sensitivity and medium.

20.0 Monitoring, Logging and Audit

20.1 Critical systems shall maintain logs sufficient to support security monitoring, investigation, reconciliation and accountability.

20.2 Logs and monitoring information shall themselves be protected from unauthorised alteration or deletion.

20.3 Access to sensitive systems and records shall be subject to periodic review.

20.4 The Company may conduct audits, vulnerability assessments, access reviews and security testing proportionate to risk.

20.5 Any security testing involving production systems shall be authorised and controlled to avoid disruption to client services or markets.

21.0 Security Awareness and Training

All personnel shall receive information-security and data-protection awareness appropriate to their role. Training shall cover confidentiality, phishing and social engineering, password security, personal-data handling, incident reporting, acceptable use and the specific risks associated with securities transactions and client information.

22.0 Information Sharing and Disclosure

22.1 External disclosure of Confidential or Restricted information requires a legitimate business, legal, regulatory or contractual basis and appropriate approval.

22.2 Regulatory and statutory disclosures shall be made through authorised channels.

22.3 Confidential information shall be shared with clients, counterparties, advisers, auditors and service providers only to the extent necessary and subject to applicable confidentiality arrangements.

22.4 Employees shall not make public statements on behalf of Alpha Capital unless authorised.

23.0 Prohibited Activities

23.1 Unauthorised access to systems, accounts or information.

23.2 Sharing passwords, tokens or access credentials.

23.3 Using client or Company information for personal benefit or unauthorised trading.

23.4 Copying confidential information to unauthorised personal storage or devices.

23.5 Installing unauthorised software or bypassing security controls.

23.6 Disabling or interfering with logging, security monitoring or protective measures.

23.7 Deliberately introducing malware, malicious code or unauthorised system changes.

23.8 Disclosing confidential information to unauthorised persons, including through social media or messaging platforms.

24.0 Information Security Risk Management

Information-security risks shall be identified, assessed, documented and treated in accordance with the Company's enterprise risk-management framework. Critical assets and processes shall receive enhanced controls based on business impact, regulatory significance, threat exposure and sensitivity of information.

25.0 Exceptions

Any exception to this Policy shall be documented, risk-assessed, approved by the appropriate authority and time-bound. Exceptions affecting regulatory obligations, client information, trading systems or material security controls shall be escalated to Compliance/Risk and senior management and, where appropriate, the Board.

26.0 Enforcement

Failure to comply with this Policy may expose Alpha Capital and its clients to financial, operational, regulatory and reputational risk. A breach may result in disciplinary action, withdrawal of access, contractual remedies, regulatory reporting or legal action, as appropriate.

27.0 Policy Review and Maintenance

This Policy shall be reviewed at least annually and whenever there is a material change in law, regulation, business activities, technology, information systems, cyber-risk profile or organisational structure. The Policy owner shall ensure that changes are documented and submitted for approval in accordance with the Company's governance arrangements.

28.0 Minimum Control Baseline

Control Area	Minimum Requirement	Frequency / Trigger
User access	Role-based access; approval; periodic review; prompt termination of leavers	At onboarding/change; periodic review
MFA	Required for critical/privileged access where technically available	Continuous
Patch management	Supported systems and timely security updates	Ongoing
Backups	Protected backups for critical systems	Per documented schedule
Incident response	Defined reporting, escalation and investigation process	Immediate upon incident
Vendor security	Risk-based due diligence and contractual controls	Pre-engagement and periodic
Security awareness	Mandatory awareness training	At onboarding and periodically

Access logs	Logging for critical systems and sensitive activities	Continuous
Data protection	Lawful processing, minimisation, security and retention controls	Continuous
Recovery testing	Test critical recovery arrangements	Periodically

29.0 Approval

This Information Protection Policy is submitted for approval by the Board of Directors of Global Alpha Capital Limited and shall become effective upon approval.