Document Code: AETOS-CMS-001
Version: 1.0
Effective Date: 02 March 2026
Document Owner: Chief Executive Officer
Approved by: General Director
Ulugbek Sultan
Classification: Internal Corporate Document

CORPORATE COMPLIANCE MANUAL

Policies, Procedures & Governance Framework

AETOS SYSTEMS

TOO | BIN 180640015679 | Astana, Kazakhstan

Version 1.0 | March 2026 | CONFIDENTIA

TABLE OF CONTENTS

Right-click the TOC and select "Update Field" to refresh page numbers

Section 1: Corporate Governance Framework 8

1.1 Purpose and Scope 8

1.2 Corporate Structure 8

1.2.1 Organizational Chart 8

1.2.2 Key Governance Bodies 9

1.3 Board of Directors Responsibilities 10

1.3.1 Compliance Oversight 10

1.3.2 Delegation of Authority 10

Section 2: Anti-Bribery & Anti-Corruption Policy 11

2.1 Policy Statement 11

2.2 Prohibited Conduct 11

2.2.1 Offering, Promising, or Giving Bribes 11

2.2.2 Soliciting or Accepting Bribes 12

2.2.3 Bribing Through Third Parties 12

2.2.4 Fraud and Misrepresentation 12

2.3 Gifts and Hospitality 12

2.3.1 Approval Thresholds 13

2.3.2 Prohibited Gifts 13

2.4 Facilitation Payments 13

2.5 Due Diligence on Third Parties 14

2.6 Record Keeping 14

Section 3: Know Your Customer (KYC) & Due Diligence Policy 16

3.1 KYC Policy Overview 16

3.2 Customer Identification Procedures 16

3.2.1 Corporate Entities 16

3.2.2 Natural Persons 17

3.2.3 Government Entities and State-Owned Enterprises 17

3.3 Risk-Based Approach 18

3.3.1 Risk Factors 18

3.4 Enhanced Due Diligence 18

3.4.1 Politically Exposed Persons (PEPs) 19
3.5 Ongoing Monitoring 19
Section 4: Sanctions & Export Control Compliance 20
4.1 Applicable Sanctions Regimes 20
4.1.1 United Nations Sanctions 20
4.1.2 European Union Sanctions 20
4.1.3 United States Sanctions 20
4.1.4 United Kingdom Sanctions 20
4.1.5 Kazakhstan National Sanctions 21
4.2 Screening Procedures 21
4.2.1 Screening Scope 21
4.2.2 Screening Triggers 21
4.2.3 Screening Process 22
4.2.4 Match Resolution 22
4.3 Export Control Requirements 22
4.4 Reporting and Escalation 23
Section 5: Conflict of Interest Policy 24
5.1 Definition and Scope 24
5.1.1 Types of Conflicts 24
5.2 Disclosure Requirements 24
5.2.1 Timing of Disclosure 25
5.2.2 Content of Disclosure 25
5.3 Review and Management 25
5.3.1 Assessment Criteria 25
5.3.2 Management Measures 26
5.3.3 Documentation 26
Section 6: Whistleblower Protection Policy 27
6.1 Policy Statement 27
6.2 Reporting Channels 27
6.2.1 Internal Reporting Channels 27
6.2.2 Anonymous Reporting 27
6.2.3 External Reporting 28
6.3 Investigation Procedures 28
6.3.1 Initial Assessment 28

6.3.2 Investigation Process 28
6.3.3 Investigation Outcome 29
6.4 Protection Against Retaliation 29
6.4.1 Protection Measures 29
6.4.2 Reporting Retaliation 29
Section 7: Code of Business Conduct & Ethics 30
7.1 Core Values 30
7.1.1 Integrity 30
7.1.2 Accountability 30
7.1.3 Respect 30
7.1.4 Excellence 30
7.1.5 Sustainability 30
7.2 Fair Dealing 30
7.2.1 Competition Law Compliance 31
7.2.2 Procurement Integrity 31
7.3 Insider Trading 31
7.3.1 Information Handling 32
7.4 Confidentiality 32
7.4.1 Categories of Confidential Information 32
7.4.2 Information Security Obligations 32
7.4.3 Personal Data Protection 32
Section 8: Third-Party Risk Management 34
8.1 Third-Party Classification 34
8.2 Risk Assessment Framework 34
8.2.1 Integrity Risk 34
8.2.2 Financial Risk 34
8.2.3 Operational Risk 35
8.2.4 Legal and Regulatory Risk 35
8.2.5 Reputational Risk 35
8.3 Contractual Safeguards 36
8.3.1 Minimum Contractual Provisions 36
8.3.2 Enhanced Provisions for High-Risk Third Parties 36
8.4 Ongoing Monitoring 36
Section 9: Record Keeping & Documentation Standards 38

9.1 Document Retention Policy 38
9.1.1 Retention Periods 38
9.1.2 Suspension of Destruction 38
9.2 Electronic Records 39
9.2.1 Data Integrity 39
9.3 Audit Trail Requirements 39
9.3.1 Financial Records 40
9.3.2 Compliance Records 40

Section 10: Training & Awareness Program 41
10.1 Training Requirements 41
10.1.1 Mandatory Training 41
10.1.2 Training Content 41
10.1.3 Training Delivery 42
10.2 Certification and Testing 42
10.2.1 Remedial Training 43
10.3 Record Keeping 43

Section 11: Monitoring, Audit & Review 44
11.1 Internal Audit Function 44
11.1.1 Audit Scope 44
11.1.2 Audit Frequency 44
11.1.3 Audit Process 45
11.1.4 Audit Reporting 45
11.2 Risk Assessment 45
11.2.1 Risk Assessment Methodology 45
11.2.2 Risk Assessment Process 46
11.3 Management Review 46
11.3.1 Review Output 46

Section 12: Incident Reporting & Investigation Protocol 48
12.1 Incident Classification 48
12.1.1 Critical Incidents 48
12.1.2 Major Incidents 48
12.1.3 Minor Incidents 49
12.2 Investigation Protocol 49
12.2.1 Reporting and Initial Response 49

12.2.2 Investigation Process 49
12.2.3 Investigation Report 49
12.3 Corrective Actions 50
12.3.1 Types of Corrective Actions 50
12.3.2 Implementation and Follow-Up 50
Annex A: Compliance Certificate Template 51
Annex B: Third-Party Due Diligence Checklist 52
B.1 General Information 52
B.2 Ownership and Control 52
B.3 Management and Key Personnel 52
B.4 Financial Standing 52
B.5 Compliance and Integrity 53
B.6 Business Rationale 53
Annex C: Gifts and Hospitality Register 54
Instructions for Completion: 54
Annex D: Conflict of Interest Disclosure Form 55
D.1 Personal Information 55
D.2 Disclosure 55
D.3 Assessment 56
Annex E: Whistleblower Report Form 57
E.1 Reporter Information (Optional) 57
E.2 Report Details 57
E.3 Description of Concern 57
E.4 Supporting Documents 58
E.5 Office Use Only 58
Annex F: Sanctions Screening Log 59
Annex G: Training Attendance Record 60
Annex H: Incident Report Template 61
H.1 Incident Identification 61
H.2 Incident Description 61
H.3 Persons Involved 62
H.4 Investigation Summary 62

H.5 Corrective Actions 63
H.6 Sign-Off 63

Section 1: Corporate Governance Framework

1.1 Purpose and Scope

This Corporate Governance Framework sets forth the governance structure, decision-making processes, and accountability mechanisms for Aetos Systems (hereinafter referred to as the "Company" or "Aetos Systems"), a limited liability partnership organized and existing under the laws of the Republic of Kazakhstan.

The purpose of this Manual is to:

- Establish a comprehensive compliance management system aligned with international best practices and applicable regulatory requirements;
- Define roles, responsibilities, and reporting lines for compliance-related matters;
- Provide clear guidance to all directors, officers, employees, contractors, and third-party representatives on expected standards of conduct;
- Ensure adherence to applicable laws, regulations, and international standards, including but not limited to the Criminal Code of the Republic of Kazakhstan, the Law on Combating Corruption, the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act 2010, and applicable sanctions regimes;
- Support the Company's objectives in securing international financing, participating in public procurement processes, and engaging with governmental bodies, international financial institutions, and EPC contractors.

This Manual applies to all employees, directors, officers, agents, consultants, contractors, joint venture partners, and any other persons acting on behalf of or representing Aetos Systems, regardless of their location or contractual arrangement.

1.2 Corporate Structure

Aetos Systems operates under a clearly defined corporate governance structure designed to ensure effective oversight, risk management, and compliance. The Company's governance framework comprises the following key elements:

1.2.1 Organizational Chart

The Company maintains a documented organizational structure that delineates reporting lines, functional responsibilities, and authority levels. The organizational structure is reviewed annually and

updated as necessary to reflect changes in the Company's operations, regulatory environment, or strategic priorities.

Governance Body	Primary Function	Accountability
General Meeting of Participants	Strategic decisions, charter amendments, appointment of Director	Participants
Director	Executive management, operations, compliance oversight	General Meeting
Compliance Officer	Policy development, risk assessment, training, investigations	Director
Finance Department	Financial controls, reporting, tax compliance	Director
PMO	Project execution, HSE compliance, contractual compliance	Director

1.2.2 Key Governance Bodies

The governance framework of Aetos Systems is built upon the following key bodies, each with clearly defined mandates, authority levels, and accountability mechanisms:

General Meeting of Participants: The supreme governing body responsible for fundamental decisions including amendments to the charter, approval of annual financial statements, appointment and removal of the Director, and major transactions requiring participant approval under Kazakhstan law.

Director (Sole Executive Body): Responsible for the day-to-day management of the Company, implementation of decisions taken by the General Meeting, strategic planning, and ensuring compliance with applicable laws and internal policies. The Director serves as the primary compliance officer unless a dedicated Compliance Officer is appointed.

Compliance Officer (appointed): Responsible for developing, implementing, and monitoring compliance policies and procedures, conducting risk assessments, coordinating training programs, investigating compliance violations, and reporting to the Director and General Meeting on compliance matters.

Finance and Accounting Department: Responsible for financial reporting, internal controls, record keeping, and ensuring compliance with tax and accounting regulations of the Republic of Kazakhstan and applicable international standards.

Project Management Office: Responsible for the execution of energy and infrastructure projects, ensuring compliance with contractual obligations, environmental regulations, health and safety standards, and applicable international norms.

1.3 Board of Directors Responsibilities

In exercising its governance functions, the Director and, where applicable, the General Meeting bear the following compliance-related responsibilities:

- Overseeing the development and approval of compliance policies, procedures, and internal controls;
- Reviewing and approving the annual compliance work plan and budget;
- Receiving and reviewing regular compliance reports, including risk assessments, incident reports, and audit findings;
- Ensuring adequate resources are allocated to compliance activities, including staffing, training, and technology;
- Setting the tone at the top by demonstrating unwavering commitment to ethical conduct and compliance;
- Addressing significant compliance violations and ensuring appropriate disciplinary actions are taken;
- Reviewing and approving engagement with high-risk third parties, including government officials, international financial institutions, and major EPC contractors;
- Ensuring timely disclosure of material compliance matters to relevant authorities, lenders, and project partners as required by law or contract.

1.3.1 Compliance Oversight

The Director shall ensure that a comprehensive compliance oversight mechanism is maintained at all times. This includes:

- At least quarterly compliance review meetings;
- Annual comprehensive compliance risk assessment;
- Bi-annual reporting to the General Meeting on compliance performance;
- Immediate reporting of material compliance breaches or regulatory investigations.

1.3.2 Delegation of Authority

The Director may delegate specific compliance functions to designated officers or departments, provided that such delegation is documented, communicated to all relevant personnel, and does not diminish the ultimate responsibility of the Director for compliance matters. Any delegation must include clear parameters of authority, reporting requirements, and escalation procedures.

Section 2: Anti-Bribery & Anti-Corruption Policy

2.1 Policy Statement

Aetos Systems maintains a zero-tolerance policy toward bribery and corruption in all forms. The Company is committed to conducting its business with the highest standards of integrity, transparency, and ethical conduct. This policy applies to all business activities undertaken by Aetos Systems, including interactions with government officials, international financial institutions, EPC contractors, suppliers, and other business partners across all jurisdictions in which the Company operates.

This policy is designed to ensure compliance with:

- The Criminal Code of the Republic of Kazakhstan (Article 311, Article 366, and related provisions);
- The Law of the Republic of Kazakhstan dated November 18, 2015 No. 410-V "On Combating Corruption";
- The United States Foreign Corrupt Practices Act of 1977 (15 U.S.C. sections 78dd-1 et seq.);
- The United Kingdom Bribery Act 2010 (Chapter 23);
- The OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions;
- Applicable United Nations Convention Against Corruption (UNCAC) obligations.

Any violation of this policy may result in disciplinary action, up to and including termination of employment or contractual relationship, and may be reported to relevant law enforcement authorities. The Company shall cooperate fully with any official investigation into allegations of bribery or corruption.

2.2 Prohibited Conduct

The following conduct is strictly prohibited and constitutes a violation of this policy:

2.2.1 Offering, Promising, or Giving Bribes

No employee, officer, director, agent, or representative of Aetos Systems shall directly or indirectly offer, promise, give, or authorize the giving of any item of value to any person, including but not limited to:

- Any government official, public servant, or employee of a state-owned enterprise;

- Any officer, employee, or representative of an international financial institution (including but not limited to EBRD, EIB, ADB, World Bank, GCF);
- Any private sector counterpart, customer, supplier, or contractor;
- Any family member, associate, or nominee of any of the foregoing.

The term "item of value" includes, but is not limited to: cash, cash equivalents, gifts, loans, travel expenses, hospitality, entertainment, charitable contributions, political donations, employment opportunities, contracts, subcontracts, and any other benefit or advantage.

2.2.2 Soliciting or Accepting Bribes

No employee, officer, director, agent, or representative of Aetos Systems shall solicit, request, agree to receive, or accept any item of value from any person in connection with the Company's business activities, regardless of whether such item is offered in exchange for any specific action or as a general goodwill gesture.

2.2.3 Bribing Through Third Parties

The Company prohibits the use of third parties, including agents, consultants, distributors, joint venture partners, contractors, or any other intermediaries, to engage in conduct that would constitute a violation of this policy if undertaken directly by the Company.

All third parties acting on behalf of Aetos Systems must be subject to appropriate due diligence, contractual safeguards, and ongoing monitoring as detailed in Section 8 of this Manual.

2.2.4 Fraud and Misrepresentation

No person acting on behalf of Aetos Systems shall engage in fraud, deceit, misrepresentation, or any other dishonest conduct in connection with the Company's business activities, including in applications for permits, licenses, financing, or in contractual negotiations and performance.

2.3 Gifts and Hospitality

Aetos Systems recognizes that the exchange of modest gifts and hospitality is a common business practice. However, all such exchanges must comply with the following principles:

- Legitimacy: Gifts and hospitality must be given and received for legitimate business purposes only, such as building relationships or expressing appreciation;
- Proportionality: The value of any gift or hospitality must be reasonable, modest, and proportionate to the legitimate business purpose;
- Legality: Gifts and hospitality must comply with all applicable laws, including the laws of Kazakhstan and the laws of the recipient's jurisdiction;

- Transparency: All gifts and hospitality must be accurately recorded in the Gifts and Hospitality Register (Annex C);
- No Quid Pro Quo: No gift or hospitality shall be offered or accepted with the expectation, express or implied, of any specific benefit, advantage, or favorable treatment in return.

2.3.1 Approval Thresholds

Category	Value Threshold	Approval Required
Gifts to Government Officials	Any value	Director (pre-approval)
Gifts to Private Counterparties	Up to USD 100	Department Head
Gifts to Private Counterparties	USD 100 - 200	Compliance Officer
Gifts to Private Counterparties	Above USD 200	Prohibited
Hospitality (per person)	Up to USD 150	Department Head
Hospitality (per person)	USD 150 - 300	Compliance Officer
Hospitality (per person)	Above USD 300	Director

2.3.2 Prohibited Gifts

The following categories of gifts are prohibited under all circumstances:

- Cash or cash equivalents (including gift cards, vouchers, and certificates);
- Gifts of significant value (exceeding USD 200 or local currency equivalent);
- Gifts that may create an appearance of impropriety or conflict of interest;
- Gifts to government officials that are not pre-approved by the Director;
- Hospitality involving illegal activities or venues;
- Personal services or favors.

2.4 Facilitation Payments

Facilitation payments (small payments made to government officials to expedite routine, non-discretionary governmental actions) are prohibited under this policy. Aetos Systems does not permit the making of facilitation payments regardless of local customs or practices.

If an employee or representative is confronted with a demand for a facilitation payment, the following steps must be taken:

- Refuse the payment demand if it is safe and legally permissible to do so;
- Immediately report the demand to the Compliance Officer or Director;

- Document all relevant details including the date, location, amount demanded, identity of the official, and circumstances;
- Seek legal guidance on available remedies under local law.

In exceptional circumstances where an individual's health or safety is at risk, a facilitation payment may be made to avoid imminent harm. Such payment must be immediately reported to the Compliance Officer and fully documented.

2.5 Due Diligence on Third Parties

All third parties engaged by Aetos Systems that may interact with government officials, international financial institutions, or counterparties on behalf of the Company must undergo anti-corruption due diligence. The scope and depth of due diligence shall be proportionate to the assessed risk level of the engagement.

Minimum due diligence requirements include:

- Verification of legal existence, registration, and ownership structure;
- Identification of ultimate beneficial owners;
- Background checks on key principals and management;
- Review of any past or pending corruption-related allegations, investigations, or proceedings;
- Assessment of the third party's own anti-corruption policies and procedures;
- Sanctions and watchlist screening (see Section 4).

2.6 Record Keeping

All transactions and relationships involving government officials, international financial institutions, and high-risk counterparties must be accurately documented and recorded. Records must be maintained in accordance with the document retention policy set forth in Section 9 of this Manual.

Records relating to anti-corruption compliance shall include:

- Third-party due diligence files;
- Contracts and agreements with third-party representatives;
- Gifts and hospitality registers;
- Training records;
- Incident reports and investigation records;

- Internal audit reports.

Section 3: Know Your Customer (KYC) & Due Diligence Policy

3.1 KYC Policy Overview

Aetos Systems maintains a comprehensive Know Your Customer (KYC) and Customer Due Diligence (CDD) program designed to mitigate legal, financial, and reputational risks associated with business relationships. This policy applies to all customers, counterparties, joint venture partners, suppliers, contractors, agents, and other third parties with whom the Company establishes or maintains a business relationship.

The KYC policy is based on the following core principles:

- Risk-Based Approach: The scope and depth of due diligence shall be proportionate to the assessed risk level of the customer or counterparty;
- Identity Verification: All business relationships shall be subject to satisfactory verification of identity and legal existence;
- Beneficial Ownership: The Company shall identify and verify the ultimate beneficial owners of all corporate customers and counterparties;
- Ongoing Monitoring: Business relationships shall be subject to continuous monitoring and periodic review;
- Record Retention: All KYC records shall be maintained in accordance with applicable retention requirements.

3.2 Customer Identification Procedures

Before establishing any business relationship, Aetos Systems shall obtain and verify the following minimum information:

3.2.1 Corporate Entities

- Full legal name, registered address, and place of incorporation;
- Registration number, tax identification number, and BIN (Business Identification Number) where applicable;
- Certificate of incorporation, articles of association, or equivalent constitutional documents;

- Evidence of authorization of persons acting on behalf of the entity (power of attorney, board resolution);
- Identity documents of authorized signatories and senior management;
- Ownership structure chart identifying all shareholders holding 10% or more;
- Identification of ultimate beneficial owners (UBOs) as defined under applicable law.

3.2.2 Natural Persons

- Full name, date of birth, nationality, and residential address;
- Government-issued identification document (passport, national ID card);
- Purpose and intended nature of the business relationship;
- Source of funds and wealth (for high-risk relationships).

3.2.3 Government Entities and State-Owned Enterprises

When engaging with government entities, state-owned enterprises, or international financial institutions, the Company shall:

- Verify the official status and mandate of the entity;
- Identify the relevant government agency or department;
- Obtain evidence of authorization to enter into the proposed transaction;
- Comply with applicable public procurement laws and regulations.

3.3 Risk-Based Approach

Aetos Systems categorizes all business relationships into three risk tiers for due diligence purposes. The risk classification determines the scope and frequency of due diligence measures to be applied.

Risk Level	Characteristics	Due Diligence Measures
Low	Established corporations in low-risk jurisdictions, transparent ownership, non-sensitive industries	Standard CDD, 3-year review cycle
Medium	Complex structures, moderate-risk jurisdictions, certain regulated entities	Standard CDD + additional verification, 2-year review cycle
High	PEPs, high-risk jurisdictions, government contracts, sanctions exposure, complex beneficial ownership	Enhanced Due Diligence, annual review, senior management approval

3.3.1 Risk Factors

In assessing the risk level of a business relationship, the Company shall consider the following risk factors:

- Country risk: Jurisdictions subject to sanctions, high corruption risk (per Transparency International CPI), weak AML/CFT controls, or political instability;
- Customer risk: Government officials, state-owned enterprises, politically exposed persons (PEPs), cash-intensive businesses, complex ownership structures;
- Transaction risk: Unusual complexity, large cash payments, transactions with no apparent economic purpose, cross-border transfers to high-risk jurisdictions.

3.4 Enhanced Due Diligence

Enhanced Due Diligence (EDD) measures shall be applied to all high-risk business relationships. EDD measures shall include all standard due diligence measures plus the following additional requirements:

- Senior management approval for establishing or continuing the relationship;
- Independent source verification of identity, ownership, and beneficial ownership;
- Detailed understanding of the source of funds and wealth;
- Enhanced ongoing monitoring, including more frequent transaction review;

- Additional background checks on principals and UBOs, including sanctions, adverse media, and litigation screening;
- On-site visits or third-party verification where appropriate;
- Periodic re-assessment of risk classification (at least annually).

3.4.1 Politically Exposed Persons (PEPs)

A Politically Exposed Person is defined as an individual who is or has been entrusted with a prominent public function, including heads of state, heads of government, ministers, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned enterprises, and senior officials of political parties.

When a customer or beneficial owner is identified as a PEP, the following measures shall be applied:

- Mandatory senior management approval;
- Enhanced ongoing monitoring of the relationship;
- Documentation of the source of wealth and funds;
- Screening of family members and known close associates.

3.5 Ongoing Monitoring

All business relationships shall be subject to ongoing monitoring to ensure that transactions and activities are consistent with the Company's knowledge of the customer and the customer's business and risk profile.

Ongoing monitoring shall include:

- Periodic review of customer information (at least annually for high-risk, biennially for medium-risk, and triennially for low-risk);
- Transaction monitoring to identify unusual or suspicious activity;
- Screening against updated sanctions lists and adverse media;
- Documentation of any significant changes in customer circumstances, ownership, or business activities;
- Escalation of any concerns to the Compliance Officer.

Section 4: Sanctions & Export Control Compliance

4.1 Applicable Sanctions Regimes

Aetos Systems is committed to full compliance with all applicable international sanctions and export control regimes. The Company recognizes that violations of sanctions laws can result in severe criminal and civil penalties, reputational damage, and loss of access to international financial markets.

The following sanctions regimes are applicable to the Company's operations:

4.1.1 United Nations Sanctions

As a member of the United Nations, the Republic of Kazakhstan is obligated to implement UN Security Council resolutions imposing sanctions. Aetos Systems shall ensure compliance with all applicable UN sanctions, including asset freezes, travel bans, arms embargoes, and sectoral sanctions.

4.1.2 European Union Sanctions

EU sanctions may apply to the Company's activities, particularly in connection with projects funded by EU financial institutions (EBRD, EIB), engagement with EU counterparties, or transactions denominated in Euro. The Company shall monitor EU sanctions lists and ensure compliance with applicable restrictions.

4.1.3 United States Sanctions

U.S. sanctions administered by the Office of Foreign Assets Control (OFAC) may apply to the Company's activities, particularly in connection with:

- Transactions involving U.S. persons, U.S. financial institutions, or the U.S. financial system;
- Projects involving U.S.-origin goods, technology, or services;
- Business with U.S.-owned or controlled entities;
- Transactions denominated in U.S. dollars cleared through U.S. correspondent banks.

4.1.4 United Kingdom Sanctions

UK sanctions may apply to transactions involving UK persons, UK financial institutions, or business activities with a UK nexus. The Company shall ensure compliance with the UK Sanctions and Anti-Money Laundering Act 2018 and related regulations.

4.1.5 Kazakhstan National Sanctions

The Company shall comply with any sanctions or restrictive measures adopted by the Government of the Republic of Kazakhstan, including those implementing UN Security Council resolutions.

Regime	Authority	Applicable To
UN	UN Security Council	All UN member states; mandatory
EU	European Council	EU nationals, entities, transactions in EU; optional for non-EU
US (OFAC)	U.S. Treasury	U.S. persons, USD transactions, U.S.-origin items; extraterritorial
UK (OFSI)	HM Treasury	UK persons, entities, and territorial activities
Kazakhstan	Government of RK	All entities operating in Kazakhstan

4.2 Screening Procedures

Aetos Systems shall maintain robust screening procedures to ensure that the Company does not engage in prohibited transactions or dealings with sanctioned persons, entities, or jurisdictions.

4.2.1 Screening Scope

Screening shall be conducted against the following categories of sanctions lists:

- Consolidated UN Security Council sanctions list;
- EU consolidated financial sanctions list;
- U.S. OFAC Specially Designated Nationals and Blocked Persons (SDN) List;
- U.S. OFAC sectoral sanctions and other sanctions lists;
- UK HM Treasury consolidated sanctions list;
- Any applicable Kazakhstan national sanctions lists.

4.2.2 Screening Triggers

Screening shall be conducted in the following circumstances:

- Prior to entering into any new business relationship or contractual arrangement;
- Prior to any payment or financial transaction;
- On a periodic basis for all existing relationships (at least quarterly);
- Upon any update to sanctions lists;

- When there is a change in ownership, control, or management of an existing counterparty.

4.2.3 Screening Process

The screening process shall include:

- Name matching against all applicable sanctions lists;
- Fuzzy matching to identify potential name variations and aliases;
- Review of country of residence, incorporation, or nationality;
- Review of vessel and aircraft identifiers where applicable;
- Investigation and resolution of any matches or alerts;
- Documentation of screening results and any remedial actions taken.

4.2.4 Match Resolution

When a potential sanctions match is identified, the following steps shall be taken immediately:

- Freeze any pending transactions;
- Escalate to the Compliance Officer and Director;
- Conduct enhanced due diligence to confirm or rule out the match;
- If the match is confirmed, block any assets and report to the relevant sanctions authority;
- Maintain full documentation of the match and resolution process.

4.3 Export Control Requirements

Aetos Systems shall comply with all applicable export control laws and regulations governing the export, re-export, transfer, and brokering of goods, software, technology, and technical data.

Key export control obligations include:

- Obtaining all required export licenses and authorizations prior to shipment or transfer;
- Classifying all controlled items under applicable export control classification systems;
- Implementing end-user and end-use verification procedures;
- Maintaining complete export documentation and records;
- Screening against denied party and entity lists.

4.4 Reporting and Escalation

All sanctions and export control compliance matters shall be subject to the following reporting and escalation procedures:

- The Compliance Officer shall maintain a sanctions screening log documenting all screening activities and results;
- Any sanctions match, potential violation, or compliance concern shall be reported immediately to the Director;
- The Director shall ensure that any confirmed sanctions violation is reported to the relevant regulatory authority within the timeframe required by applicable law;
- The Company shall cooperate fully with any regulatory inquiry or investigation into sanctions compliance matters.

Section 5: Conflict of Interest Policy

5.1 Definition and Scope

A conflict of interest exists when an employee's, director's, or officer's personal interests (whether financial, familial, or otherwise) interfere or appear to interfere with the best interests of Aetos Systems. Conflicts of interest can undermine the integrity of business decisions, damage the Company's reputation, and expose the Company to legal and regulatory risk.

This policy applies to all directors, officers, employees, consultants, agents, and representatives of Aetos Systems. The obligation to identify, disclose, and manage conflicts of interest is a personal responsibility of every individual subject to this policy.

5.1.1 Types of Conflicts

Conflicts of interest may arise in various forms, including but not limited to:

- Financial Interest: Direct or indirect financial interest in a competitor, supplier, customer, or counterparty of the Company;
- Outside Employment: Engagement in outside employment, consulting, or advisory services that may compete with or detract from the Company's business;
- Family Relationships: Business relationships involving immediate family members (spouse, parents, children, siblings) that may influence business decisions;
- Gifts and Favors: Acceptance of gifts, favors, or hospitality that could create an obligation or expectation of preferential treatment;
- Use of Position: Use of the Company's position, assets, or information for personal gain or the gain of others;
- Board Memberships: Service on the board of directors or advisory board of any organization that may have a business relationship with the Company.

5.2 Disclosure Requirements

All individuals subject to this policy have a continuing obligation to disclose any actual, potential, or perceived conflict of interest. Disclosures shall be made in writing using the Conflict of Interest Disclosure Form (Annex D).

5.2.1 Timing of Disclosure

Disclosures shall be made:

- Upon commencement of employment or engagement with the Company;
- Annually thereafter, as part of the annual compliance certification process;
- Whenever a new conflict of interest arises or an existing conflict changes in nature or significance;
- Prior to participating in any decision, negotiation, or transaction that may be affected by the conflict.

5.2.2 Content of Disclosure

Each disclosure shall include:

- A description of the conflict or potential conflict;
- The nature and extent of the individual's interest;
- The names of any other persons or entities involved;
- An assessment of the potential impact on the Company;
- Any proposed measures to manage or mitigate the conflict.

5.3 Review and Management

Upon receipt of a conflict of interest disclosure, the Compliance Officer (or Director in the absence of a designated Compliance Officer) shall conduct a review to determine the appropriate course of action.

5.3.1 Assessment Criteria

In assessing a disclosed conflict, the following factors shall be considered:

- The materiality and significance of the conflict;
- The potential impact on the Company's business, reputation, and legal exposure;
- Whether the conflict can be adequately managed through safeguards;
- Whether the conflict is so significant that it requires termination of the underlying relationship or the individual's employment.

5.3.2 Management Measures

Depending on the assessment, the following management measures may be imposed:

- Monitoring: The conflict is documented and the individual is required to provide periodic updates;
- Recusal: The individual is required to recuse themselves from any decision-making, negotiation, or transaction related to the conflict;
- Divestiture: The individual is required to divest the conflicting interest within a specified timeframe;
- Restriction: The individual is restricted from certain activities or relationships;
- Termination: In severe cases, the conflict may require termination of employment or the underlying relationship.

5.3.3 Documentation

All conflict of interest disclosures, assessments, and management measures shall be documented and maintained by the Compliance Officer. Such records shall be treated as confidential and accessed only on a need-to-know basis.

Section 6: Whistleblower Protection Policy

6.1 Policy Statement

Aetos Systems is committed to maintaining a culture of integrity, transparency, and accountability. The Company recognizes that individuals who report concerns about misconduct, violations of law, or breaches of Company policy play a vital role in safeguarding the Company's reputation and operations.

This policy establishes safe, confidential, and accessible channels for reporting concerns, and provides robust protections against retaliation for individuals who make reports in good faith.

This policy applies to all employees, directors, officers, contractors, agents, suppliers, and other stakeholders who have a business relationship with Aetos Systems.

6.2 Reporting Channels

Aetos Systems provides multiple channels for reporting concerns, ensuring that reporters can choose the method with which they are most comfortable.

6.2.1 Internal Reporting Channels

Compliance Officer: The Compliance Officer serves as the primary recipient of whistleblower reports. Reports may be submitted in writing, by telephone, or in person. The Compliance Officer is responsible for acknowledging receipt of all reports within five business days.

Director: Reports may be submitted directly to the Director, particularly where the concern involves the Compliance Officer or where the reporter prefers to bypass the Compliance Officer.

General Meeting of Participants: In exceptional cases, reports may be submitted to the General Meeting of Participants, particularly where the concern involves the Director or relates to fundamental governance matters.

6.2.2 Anonymous Reporting

Reports may be submitted anonymously through a dedicated email address or telephone hotline. While anonymous reports are accepted, reporters are encouraged to identify themselves to facilitate investigation and follow-up. The Company shall make reasonable efforts to investigate anonymous reports, subject to the availability of sufficient information.

6.2.3 External Reporting

Nothing in this policy shall prevent a reporter from making a report to an external regulatory or law enforcement authority where the reporter believes such reporting is necessary or appropriate. The Company shall not take any adverse action against an individual for making a good-faith report to an external authority.

Channel	Contact	Appropriate For
Compliance Officer	compliance@aetos.kz	General compliance concerns
Director	director@aetos.kz	Serious matters, CO involvement
Anonymous Hotline	+7 (7172) XXX-XXX	Anonymous reports
External Authority	Regulatory body	When internal channels inadequate

6.3 Investigation Procedures

Upon receipt of a whistleblower report, the following investigation procedures shall be followed:

6.3.1 Initial Assessment

The Compliance Officer shall conduct an initial assessment of the report within ten business days to determine:

- Whether the report falls within the scope of this policy;
- The seriousness and urgency of the reported concern;
- Whether the report can be investigated internally or requires external expertise;
- The appropriate investigation methodology and timeframe.

6.3.2 Investigation Process

Investigations shall be conducted in a manner that is:

- Independent: The investigator shall be independent of the subject matter and individuals involved;
- Thorough: The investigation shall gather all relevant evidence and interview all relevant witnesses;
- Fair: The investigation shall afford the subject of the report a reasonable opportunity to respond to allegations;
- Timely: The investigation shall be completed as expeditiously as possible;
- Confidential: The investigation and its findings shall be treated as strictly confidential.

6.3.3 Investigation Outcome

Upon completion of the investigation, a written report shall be prepared summarizing the findings, conclusions, and any recommended corrective actions. The report shall be submitted to the Director and, where appropriate, to the General Meeting of Participants.

The reporter shall be informed of the outcome of the investigation to the extent permitted by law and confidentiality obligations.

6.4 Protection Against Retaliation

Aetos Systems strictly prohibits any form of retaliation against individuals who make good-faith reports under this policy. Retaliation includes, but is not limited to:

- Termination, suspension, or demotion;
- Reduction in compensation, benefits, or responsibilities;
- Harassment, intimidation, or hostile treatment;
- Damage to professional reputation or career prospects;
- Any other adverse action taken because of the report.

6.4.1 Protection Measures

The Company shall implement appropriate measures to protect reporters, including:

- Maintaining the confidentiality of the reporter's identity, subject to legal obligations;
- Monitoring for signs of retaliation;
- Taking prompt corrective action if retaliation is identified;
- Providing support and assistance to reporters who experience difficulties as a result of their report.

6.4.2 Reporting Retaliation

Any individual who believes they have been subjected to retaliation for making a good-faith report should immediately report the retaliation to the Compliance Officer or Director. All such reports shall be investigated promptly and thoroughly.

Section 7: Code of Business Conduct & Ethics

7.1 Core Values

Aetos Systems is guided by a set of core values that define our corporate culture and guide our business conduct. These values are the foundation of our commitment to ethical behavior and compliance with all applicable laws and regulations.

7.1.1 Integrity

We conduct our business with honesty, fairness, and transparency. We honor our commitments, communicate truthfully, and uphold the highest ethical standards in all our dealings. We do not engage in deception, misrepresentation, or any form of dishonest conduct.

7.1.2 Accountability

We take responsibility for our actions and decisions. We are accountable to our stakeholders, including our employees, business partners, government authorities, and the communities in which we operate. We acknowledge our mistakes and take corrective action when necessary.

7.1.3 Respect

We treat all individuals with dignity and respect, regardless of their position, background, or affiliation. We foster an inclusive work environment free from discrimination, harassment, and intimidation. We respect the human rights of all individuals affected by our operations.

7.1.4 Excellence

We strive for excellence in everything we do. We pursue continuous improvement, innovation, and the highest standards of quality in our products, services, and processes. We set ambitious goals and work diligently to achieve them.

7.1.5 Sustainability

We are committed to sustainable development that balances economic growth with environmental protection and social responsibility. We seek to minimize the environmental impact of our operations and contribute positively to the communities in which we work.

7.2 Fair Dealing

Aetos Systems is committed to fair dealing in all business relationships. We compete vigorously but fairly, and we do not engage in anti-competitive practices, fraud, or deceptive conduct.

7.2.1 Competition Law Compliance

The Company shall comply with all applicable competition and antitrust laws. The following conduct is prohibited:

- Agreements with competitors to fix prices, allocate markets, or restrict output;
- Abuse of a dominant market position through predatory pricing, exclusive dealing, or other exclusionary practices;
- Bid-rigging or collusion in tender processes;
- Exchange of competitively sensitive information with competitors.

7.2.2 Procurement Integrity

In all procurement activities, the Company shall:

- Conduct fair, open, and transparent tender processes;
- Evaluate bids based on objective criteria;
- Maintain confidentiality of bid information;
- Avoid conflicts of interest in supplier selection;
- Comply with applicable public procurement laws and international standards.

7.3 Insider Trading

All individuals with access to material non-public information about Aetos Systems, its business partners, or counterparties are prohibited from trading in securities or recommending trades based on such information. This prohibition applies to securities of the Company and any other company about which the individual possesses material non-public information.

Material non-public information includes, but is not limited to:

- Financial results prior to public announcement;
- Pending mergers, acquisitions, or divestitures;
- Major contract awards or terminations;
- Regulatory approvals or enforcement actions;
- Significant changes in management or corporate strategy.

7.3.1 Information Handling

All material non-public information shall be handled in accordance with the Company's confidentiality policies. Unauthorized disclosure of such information to third parties is strictly prohibited.

7.4 Confidentiality

All employees, officers, directors, and representatives of Aetos Systems have a duty to protect the confidentiality of proprietary, sensitive, and personal information obtained in the course of their duties.

7.4.1 Categories of Confidential Information

Confidential information includes, but is not limited to:

- Proprietary business information: trade secrets, know-how, technical data, business plans, strategies, and financial projections;
- Third-party information: confidential information provided by business partners, customers, and counterparties;
- Personal data: information relating to identifiable individuals, including employees, customers, and business contacts;
- Government information: classified or restricted information obtained from government sources.

7.4.2 Information Security Obligations

All individuals handling confidential information shall:

- Access confidential information only on a need-to-know basis;
- Store confidential information securely and protect it from unauthorized access;
- Transmit confidential information only through secure channels;
- Dispose of confidential information securely when no longer needed;
- Report any actual or suspected breach of information security immediately.

7.4.3 Personal Data Protection

The Company shall process personal data in accordance with applicable data protection laws, including the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" and, where applicable, the EU General Data Protection Regulation (GDPR). Personal data shall be collected and

processed only for lawful purposes, with appropriate consent where required, and maintained only for as long as necessary.

Section 8: Third-Party Risk Management

8.1 Third-Party Classification

Aetos Systems engages with a wide range of third parties in the course of its business activities. Effective risk management requires a systematic approach to classifying third parties based on the nature of the relationship and the associated risk profile.

Category	Description	Risk Level
EPC Contractors	Engineering, procurement, and construction contractors for major projects	High
Government Partners	State-owned enterprises, government agencies, public officials	High
Suppliers	Equipment, materials, and services suppliers	Medium
Advisors	Legal, financial, technical consultants	Medium
Agents/Intermediaries	Commercial agents, brokers, finders	High
Joint Venture Partners	Equity partners in project SPVs	High
Financial Institutions	Banks, insurers, export credit agencies	Medium

8.2 Risk Assessment Framework

All third parties shall be subject to a risk assessment prior to engagement and on a periodic basis thereafter. The risk assessment shall evaluate the following categories of risk:

8.2.1 Integrity Risk

The risk that the third party may engage in corrupt, fraudulent, or unethical conduct. Assessment factors include:

- Country corruption risk (per Transparency International CPI);
- Industry sector risk profile;
- Nature of interactions with government officials;
- Third party's own compliance program and controls;
- Past corruption allegations or enforcement actions.

8.2.2 Financial Risk

The risk of financial loss arising from the third party's failure to perform. Assessment factors include:

- Financial stability and creditworthiness;
- Insurance coverage and bonding;
- Performance track record;
- Dependency on the relationship.

8.2.3 Operational Risk

The risk of operational disruption arising from the third party's actions or failures. Assessment factors include:

- Quality of products or services;
- Health, safety, and environmental performance;
- Business continuity planning;
- Subcontracting practices.

8.2.4 Legal and Regulatory Risk

The risk of legal or regulatory exposure arising from the third party's conduct. Assessment factors include:

- Sanctions and export control exposure;
- Compliance with applicable labor and employment laws;
- Environmental regulatory compliance;
- Intellectual property rights.

8.2.5 Reputational Risk

The risk of damage to the Company's reputation arising from association with the third party. Assessment factors include:

- Public perception of the third party;
- Association with controversial activities or individuals;
- Media coverage and adverse publicity.

8.3 Contractual Safeguards

All contracts with third parties shall include appropriate compliance safeguards. The specific contractual provisions shall be proportionate to the assessed risk level of the engagement.

8.3.1 Minimum Contractual Provisions

All third-party contracts shall include, at a minimum:

- Representations and warranties regarding compliance with applicable laws;
- Anti-bribery and anti-corruption covenants;
- Right to audit and inspect records;
- Termination rights for compliance violations;
- Indemnification for losses arising from compliance breaches;
- Requirement to maintain adequate insurance.

8.3.2 Enhanced Provisions for High-Risk Third Parties

Contracts with high-risk third parties shall additionally include:

- Detailed compliance obligations and reporting requirements;
- Ongoing due diligence and monitoring obligations;
- Training requirements for third-party personnel;
- Enhanced audit rights;
- Step-in rights for compliance failures;
- Exclusion of subcontractors without prior written consent.

8.4 Ongoing Monitoring

Third-party relationships shall be subject to ongoing monitoring to ensure continued compliance with contractual obligations and applicable laws.

Monitoring activities shall include:

- Periodic review of third-party performance and compliance (at least annually);
- Screening against updated sanctions and watchlists (at least quarterly);

- Review of third-party financial condition;
- Site visits and inspections where appropriate;
- Review of any complaints, incidents, or adverse information;
- Re-assessment of risk classification based on changed circumstances.

Section 9: Record Keeping & Documentation Standards

9.1 Document Retention Policy

Aetos Systems maintains a comprehensive document retention policy designed to ensure that all business records are preserved for the periods required by applicable law, regulation, and contractual obligation, while facilitating efficient retrieval and disposal.

9.1.1 Retention Periods

The following minimum retention periods shall apply, unless a longer period is required by law or contract:

Document Category	Examples	Retention Period
Corporate Records	Charter, resolutions, shareholder agreements	Permanent
Financial Statements	Annual reports, audit reports, tax returns	10 years
Accounting Records	General ledger, journals, supporting documents	7 years
Contracts	All agreements, amendments, terminations	Duration + 7 years
Employment Records	Contracts, payroll, performance reviews	Duration + 7 years
Compliance Records	Due diligence, training, incident reports	10 years
Project Documentation	Technical specifications, HSE records	Duration + 10 years
Correspondence	Business emails, formal letters	5 years

9.1.2 Suspension of Destruction

The destruction of any documents shall be suspended upon:

- Receipt of a legal hold notice or litigation hold;
- Commencement of or threat of litigation, arbitration, or regulatory investigation;
- Internal investigation into a compliance matter;
- Direction from the Director or Compliance Officer.

Once a destruction suspension is in effect, no relevant documents shall be destroyed until the suspension is formally lifted in writing by the Director or Compliance Officer.

9.2 Electronic Records

Electronic records shall be managed with the same care and diligence as paper records. The following standards apply to electronic record keeping:

- All electronic records shall be stored on Company-approved systems with appropriate access controls;
- Email communications related to Company business shall be retained in accordance with the retention schedule;
- Personal email accounts, messaging applications, and cloud storage services shall not be used for Company business;
- Electronic records shall be backed up regularly to prevent loss;
- Electronic records shall be protected against unauthorized access, modification, and deletion;
- Upon termination of employment, all Company records in an individual's possession shall be returned or transferred to the Company.

9.2.1 Data Integrity

Electronic records must accurately reflect the information they purport to record. The following controls shall be maintained:

- System-generated timestamps and audit trails shall be preserved;
- Records shall not be altered after creation without proper authorization and documentation of the change;
- Version control shall be maintained for all significant documents;
- Electronic signatures, where used, shall comply with the Law of the Republic of Kazakhstan "On Electronic Document and Electronic Digital Signature."

9.3 Audit Trail Requirements

An adequate audit trail shall be maintained for all significant transactions and decisions. The audit trail shall enable a reviewer to understand:

- The nature and purpose of the transaction or decision;

- The individuals involved in the process;
- The sequence of events and approvals;
- The documentation supporting the transaction or decision.

9.3.1 Financial Records

All financial transactions shall be supported by adequate documentation, including invoices, receipts, contracts, and approvals. Financial records shall be maintained in accordance with the accounting policies of the Company and the requirements of applicable tax and accounting regulations of the Republic of Kazakhstan.

9.3.2 Compliance Records

The following compliance-related records shall be maintained:

- Third-party due diligence files;
- Gifts and hospitality registers;
- Conflict of interest disclosures;
- Whistleblower reports and investigation records;
- Training records;
- Sanctions screening results;
- Internal audit reports;
- Incident reports and corrective action records.

Section 10: Training & Awareness Program

10.1 Training Requirements

Aetos Systems is committed to ensuring that all employees, officers, directors, and relevant third parties are adequately trained on compliance policies, procedures, and applicable legal requirements. Training is a critical component of the Company's compliance program and risk management framework.

10.1.1 Mandatory Training

The following training is mandatory for all employees, officers, and directors:

- Induction Training: All new hires must complete compliance induction training within 30 days of commencing employment;
- Annual Refresher Training: All personnel must complete annual refresher training covering all policies in this Manual;
- Role-Specific Training: Personnel in high-risk roles (finance, procurement, project management, government relations) must complete additional role-specific training.

10.1.2 Training Content

Compliance training shall cover, at a minimum, the following topics:

- Overview of the Company's compliance program and governance structure;
- Anti-bribery and anti-corruption laws and policies;
- KYC and due diligence requirements;
- Sanctions and export control compliance;
- Conflict of interest identification and disclosure;
- Whistleblower reporting channels and protections;
- Code of business conduct and ethics;
- Third-party risk management;
- Record keeping and documentation requirements;
- Incident reporting procedures.

Training Module	All Staff	Mgmt	High-Risk
Anti-Bribery & Anti-Corruption	Annual	Annual	Bi-annual
KYC & Due Diligence	Induction	Annual	Annual
Sanctions Compliance	Induction	Annual	Quarterly
Conflict of Interest	Annual	Annual	Annual
Whistleblower Policy	Induction	Induction	Induction
Code of Conduct	Induction	Induction	Annual
Third-Party Risk	-	Annual	Annual
Record Keeping	Induction	Induction	Annual

10.1.3 Training Delivery

Training may be delivered through various methods, including:

- In-person workshops and seminars;
- E-learning modules;
- Case study discussions;
- One-on-one coaching for high-risk roles;
- External training programs and certifications.

10.2 Certification and Testing

All training participants shall be required to demonstrate understanding of the training material through written or electronic testing. A minimum passing score of 80% is required for successful completion.

Upon successful completion of training, participants shall be required to sign a Compliance Certificate acknowledging that they:

- Have read and understood the applicable compliance policies;
- Agree to comply with such policies in the performance of their duties;
- Understand the consequences of non-compliance;
- Are aware of reporting channels for compliance concerns.

10.2.1 Remedial Training

Personnel who fail to achieve the minimum passing score or who are identified as having compliance knowledge gaps shall be required to complete remedial training. Failure to complete required remedial training may result in disciplinary action.

10.3 Record Keeping

The Compliance Officer shall maintain comprehensive records of all training activities, including:

- Training attendance records (Annex G);
- Training completion certificates;
- Test results and scores;
- Signed compliance certificates;
- Training materials and course content;
- Remedial training records.

Training records shall be maintained for a minimum of ten years and shall be made available to internal auditors, external auditors, and regulatory authorities upon request.

Section 11: Monitoring, Audit & Review

11.1 Internal Audit Function

Aetos Systems maintains an internal audit function responsible for independently evaluating the effectiveness of the Company's compliance program, internal controls, and risk management processes. The internal audit function reports directly to the Director and, on material matters, to the General Meeting of Participants.

11.1.1 Audit Scope

The internal audit function shall conduct audits covering, but not limited to, the following areas:

- Compliance with this Manual and other internal policies;
- Effectiveness of anti-bribery and anti-corruption controls;
- Adequacy of KYC and due diligence procedures;
- Compliance with sanctions and export control requirements;
- Management of conflicts of interest;
- Handling of whistleblower reports;
- Third-party risk management;
- Record keeping and documentation standards;
- Training program effectiveness.

11.1.2 Audit Frequency

The internal audit plan shall be developed on an annual basis, taking into account the Company's risk profile, regulatory requirements, and historical audit findings. As a general guideline:

- High-risk areas: at least annually;
- Medium-risk areas: at least biennially;
- Low-risk areas: at least triennially;
- Ad hoc audits: as warranted by specific events or concerns.

11.1.3 Audit Process

Internal audits shall be conducted in accordance with the following process:

- Planning: Development of an audit scope, objectives, and work plan;
- Notification: Advance notice to relevant departments (except where surprise is warranted);
- Fieldwork: Collection and analysis of evidence, interviews with relevant personnel;
- Reporting: Preparation of an audit report detailing findings, conclusions, and recommendations;
- Follow-up: Tracking of management's implementation of audit recommendations.

11.1.4 Audit Reporting

Audit reports shall be submitted to the Director and, where material compliance issues are identified, to the General Meeting of Participants. Audit reports shall include:

- A summary of the audit scope and methodology;
- Key findings, including any identified control weaknesses or compliance violations;
- An assessment of the severity and significance of each finding;
- Recommendations for remediation;
- Management's response and action plan.

11.2 Risk Assessment

Aetos Systems conducts periodic compliance risk assessments to identify, evaluate, and prioritize compliance risks. The risk assessment process is integral to the Company's enterprise risk management framework.

11.2.1 Risk Assessment Methodology

Compliance risks shall be assessed based on two dimensions:

- Likelihood: The probability that a compliance event will occur, taking into account the effectiveness of existing controls;
- Impact: The potential consequences of a compliance event, including financial loss, legal penalties, reputational damage, and operational disruption.

The combination of likelihood and impact shall determine the overall risk rating for each identified risk.

Impact	Low Likelihood	Medium Likelihood	High Likelihood	Rating
High	Medium	High	Critical	-
Medium	Low	Medium	High	-
Low	Low	Low	Medium	-

11.2.2 Risk Assessment Process

The annual compliance risk assessment shall involve:

- Identification of compliance risks across all areas of the Company's operations;
- Evaluation of existing controls and their effectiveness;
- Assessment of likelihood and impact for each identified risk;
- Prioritization of risks based on overall risk rating;
- Development of risk mitigation plans for high and medium risks;
- Presentation of the risk assessment to the Director and General Meeting.

11.3 Management Review

The Director shall conduct a formal review of the compliance program at least annually to ensure its continued suitability, adequacy, and effectiveness. The management review shall consider:

- The results of internal and external audits;
- Compliance risk assessment findings;
- Incident reports and investigation outcomes;
- Training program effectiveness;
- Changes in applicable laws and regulations;
- Changes in the Company's business activities, structure, or risk profile;
- Feedback from employees and stakeholders;
- Benchmarking against industry best practices.

11.3.1 Review Output

The output of the management review shall include:

- An assessment of the overall effectiveness of the compliance program;

- Identified areas for improvement;
- Approved action plans with assigned responsibilities and timelines;
- Resource allocation decisions;
- Updates to policies and procedures as necessary.

Section 12: Incident Reporting & Investigation Protocol

12.1 Incident Classification

Compliance incidents shall be classified based on their severity and potential impact on the Company. The classification determines the response and escalation procedures to be followed.

Severity	Description	Response Time	Escalation
Critical	Severe legal, financial, or reputational impact	Immediate (24h)	Director + General Meeting
Major	Substantial compliance impact	Within 72 hours	Director
Minor	Limited impact, readily addressable	Within 14 days	Compliance Officer

12.1.1 Critical Incidents

Critical incidents are those that pose an immediate and significant threat to the Company's legal position, financial stability, or reputation. Examples include:

- Confirmed bribery or corruption involving Company personnel;
- Confirmed dealings with sanctioned persons or entities;
- Material fraud or embezzlement;
- Regulatory enforcement action or criminal investigation;
- Significant data breach or loss of confidential information.

12.1.2 Major Incidents

Major incidents are those that have a substantial impact on the Company's operations or compliance posture, but do not pose an immediate existential threat. Examples include:

- Significant control failures with potential for material non-compliance;
- KYC deficiencies in high-risk relationships;
- Contractual breaches with compliance implications;
- Multiple minor incidents indicating systemic issues.

12.1.3 Minor Incidents

Minor incidents are those with limited impact that can be readily addressed through routine procedures. Examples include:

- Documentation deficiencies;
- Delays in compliance reporting;
- Minor training failures;
- Isolated procedural non-compliance.

12.2 Investigation Protocol

All compliance incidents shall be subject to investigation in accordance with the following protocol:

12.2.1 Reporting and Initial Response

Upon discovery or receipt of a report of a compliance incident:

- The incident shall be reported immediately to the Compliance Officer;
- The Compliance Officer shall assess the severity and classify the incident;
- Immediate protective measures shall be taken to prevent further harm or loss;
- Critical incidents shall be reported to the Director within 24 hours.

12.2.2 Investigation Process

Investigations shall be conducted in a manner that is:

- Prompt: Investigations shall be initiated without undue delay;
- Thorough: All relevant evidence shall be collected and analyzed;
- Independent: The investigator shall be free from conflicts of interest;
- Fair: The subject of the investigation shall be afforded an opportunity to respond;
- Confidential: The investigation and its findings shall be treated as confidential.

12.2.3 Investigation Report

Upon completion of the investigation, a written report shall be prepared containing:

- Background and summary of the incident;

- Description of the investigation methodology;
- Summary of evidence gathered;
- Findings of fact;
- Assessment of policy violations;
- Recommendations for corrective and disciplinary actions;
- Identification of any systemic control weaknesses.

12.3 Corrective Actions

Appropriate corrective actions shall be taken in response to all identified compliance incidents. Corrective actions shall be designed to address the root cause of the incident and prevent recurrence.

12.3.1 Types of Corrective Actions

Corrective actions may include:

- Disciplinary Measures: Warning, suspension, demotion, or termination of employment;
- Contractual Remedies: Termination of third-party relationships, claims for damages;
- Process Improvements: Revision of policies, procedures, and controls;
- Training: Additional training for relevant personnel;
- Monitoring: Enhanced monitoring and supervision;
- Self-Disclosure: Voluntary disclosure to regulatory authorities where appropriate.

12.3.2 Implementation and Follow-Up

The Compliance Officer shall be responsible for tracking the implementation of all corrective actions. The status of corrective actions shall be reported to the Director and, for critical and major incidents, to the General Meeting of Participants.

The effectiveness of corrective actions shall be verified through follow-up reviews. If corrective actions are found to be inadequate, additional measures shall be implemented.

Annex A: Compliance Certificate Template

The following template shall be used for annual compliance certifications by all employees, officers, and directors:

COMPLIANCE CERTIFICATE

Aetos Systems | Corporate Compliance Manual

I, _____, [Name], holding the position of _____, [Position], at Aetos Systems, hereby certify as follows:

1. I have received, read, and understood the Corporate Compliance Manual of Aetos Systems, including all policies and procedures set forth therein.

2. I have completed all mandatory compliance training as required by my role and risk classification.

3. I am not aware of any violation of the Company's compliance policies, except as disclosed in writing to the Compliance Officer.

4. I have disclosed all actual, potential, or perceived conflicts of interest as required by Section 5 of the Manual.

5. I have accurately reported all gifts and hospitality received or given in the reporting period.

6. I agree to comply with all applicable laws, regulations, and Company policies in the performance of my duties.

7. I understand that failure to comply with Company policies may result in disciplinary action, up to and including termination of employment.

Date: _____

Signature: _____

Annex B: Third-Party Due Diligence Checklist

The following checklist shall be completed for all high-risk third parties prior to engagement:

B.1 General Information

- ☐ [ ] Full legal name verified against official registry
- ☐ [ ] Country of incorporation and registration number confirmed
- ☐ [ ] Registered office address verified
- ☐ [ ] Legal form and corporate structure documented
- ☐ [ ] Date of incorporation confirmed
- ☐ [ ] Good standing certificate obtained (where applicable)

B.2 Ownership and Control

- ☐ [ ] Ownership structure chart prepared (10%+ shareholders)
- ☐ [ ] Ultimate beneficial owners identified and verified
- ☐ [ ] PEP screening completed for all UBOs and senior management
- ☐ [ ] No sanctions matches identified for UBOs or key personnel
- ☐ [ ] History of ownership changes documented

B.3 Management and Key Personnel

- ☐ [ ] Directors and senior management identified
- ☐ [ ] Background checks completed for key personnel
- ☐ [ ] No adverse media findings for key personnel
- ☐ [ ] Credentials and qualifications verified (for advisors/consultants)

B.4 Financial Standing

- ☐ [ ] Latest audited financial statements reviewed

- [ ] Credit reference obtained (where appropriate)
- [ ] No material financial distress indicators identified
- [ ] Insurance coverage verified (for contractors)

B.5 Compliance and Integrity

- [ ] Sanctions screening completed (all applicable lists)
- [ ] Adverse media screening completed
- [ ] No past or pending corruption allegations identified
- [ ] Third party's own compliance program assessed
- [ ] Contractual compliance provisions agreed

B.6 Business Rationale

- [ ] Business purpose of engagement clearly documented
- [ ] Compensation structure is commercially reasonable
- [ ] No unusual or unnecessary intermediaries involved
- [ ] Engagement approved by appropriate authority

Completed by: _____ Date: _____

Reviewed by (Compliance Officer): _____ Date: _____

Approved by (Director): _____ Date: _____

Annex C: Gifts and Hospitality Register

All gifts and hospitality given or received in the course of business shall be recorded in the Gifts and Hospitality Register. The following template shall be used:

Date	Name	Gave/Received	Description	Value (USD)	Approver

Instructions for Completion:

- All gifts and hospitality with a value exceeding USD 50 must be recorded;
- The register shall be maintained by the Compliance Officer;
- Entries shall be made within five business days of the gift or hospitality being given or received;
- The Director shall review the register on a quarterly basis.

Annex D: Conflict of Interest Disclosure Form

This form shall be completed by all employees, officers, and directors upon commencement of employment and annually thereafter, or whenever a new conflict arises.

D.1 Personal Information

Name: _____

Position: _____

Department: _____

Date: _____

D.2 Disclosure

Please describe any actual, potential, or perceived conflict of interest, including:

- Financial interests in competitors, suppliers, or customers

- Outside employment or consulting arrangements

- Family members employed by or doing business with competitors, suppliers, or customers

- Board memberships or advisory roles

- Any other circumstances that could create a conflict of interest

_____

_____

_____

_____

D.3 Assessment

Assessment by Compliance Officer (for office use only):

Risk Level: [ ] Low [ ] Medium [ ] High

Management Measure: [ ] Monitor [ ] Recuse [ ] Divest [ ] Restrict [ ] Other

Comments: _____

Compliance Officer Signature: _____ Date: _____

Annex E: Whistleblower Report Form

This form may be used to report compliance concerns through the Company's whistleblower channels. Anonymous submissions are accepted.

E.1 Reporter Information (Optional)

Name: _____

Position: _____

Department: _____

Contact Information: _____

Preferred Contact Method: [ ] Email [ ] Phone [ ] Do not contact

E.2 Report Details

Date of Incident: _____

Location: _____

Persons Involved: _____

Type of Concern: [ ] Bribery/Corruption [ ] Fraud [ ] Sanctions Violation [ ] Conflict of Interest [ ] Other

E.3 Description of Concern

Please describe the concern in as much detail as possible, including what happened, when, where, who was involved, and any evidence:

_____

_____

_____

_____

_____

_____

E.4 Supporting Documents

Are there any supporting documents or evidence? [ ] Yes [ ] No

If yes, please describe: _____

E.5 Office Use Only

Report Received By: _____ Date: _____

Acknowledgment Sent: [ ] Yes [ ] N/A (anonymous) Date: _____

Investigation Assigned To: _____ Date: _____

Annex F: Sanctions Screening Log

All sanctions screening activities shall be recorded in the Sanctions Screening Log. The following template shall be used:

Date	Screened Name/Entity	List Screened	Result	Match?	By

Annex G: Training Attendance Record

All compliance training sessions shall be documented using the following attendance record:

Employee Name	Department	Date Completed	Signature

Annex H: Incident Report Template

All compliance incidents shall be documented using the following template:

H.1 Incident Identification

Incident Reference Number: _____

Date Reported: _____

Reported By: _____

Severity Classification: [ ] Critical [ ] Major [ ] Minor

H.2 Incident Description

Brief description of the incident:

_____

_____

_____

H.3 Persons Involved

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

H.4 Investigation Summary

Investigator: _____ Date: _____

Findings:

_____

_____

H.5 Corrective Actions

Action Item: _____ Responsible: _____ Due Date: _____

Action Item: _____ Responsible: _____ Due Date: _____

Action Item: _____ Responsible: _____ Due Date: _____

H.6 Sign-Off

Prepared by: _____ Date: _____

Reviewed by Compliance Officer: _____ Date: _____

Approved by Director: _____ Date: _____

AETOS SYSTEMS

Building Energy Infrastructure Across Central Asia

TOO "Aetos Systems" | BIN 180640015679

Astana, Kazakhstan | Kenesery st, h. 69a, office 60A.

This document contains confidential and proprietary information.Unauthorized distribution is strictly prohibited.

Version 1.0 | March 2026