ANTI-FRAUD POLICY

Compliance Policies - Policy 4.1- Anti-fraud Policy

Approved by	The Board of Managers
Origin Date:	August 24, 2014
Last Revised Date:	May 5, 2015
Policy Owner(s):	Head of Forensic Department
Contact(s):	

In this document, the "Company" or "ERG" means Eurasian Resources Group S.a.r.l. and includes, where applicable, all subsidiaries.

1. Policy Objective

1.1. The policy's objectives are:
1.1.1. to ensure that the Company protects Company assets from theft or fraud in an effective and cost-efficient way;
1.1.2. to provide Company employees with clear requirements and universal guidelines on the prevention, detection and reporting of fraudulent behaviour;

1.2. The policy sets out:
1.2.1. the Company requirements for prevention, detection and handling of suspicious, attempted or actual fraudulent behaviour;
1.2.2. roles and responsibilities in fraud prevention and detection, design of controls and handling suspicious or actual fraud incidents.
1.2.3. the Policy should be applied in conjunction with the Company's Code of Conduct, Conflict of Interest Policy, Anti-Bribery and Corruption Policy and Whistleblowing and Investigation Policy

2. Scope

2.1. This policy applies to:
2.1.1. the Company, its subsidiaries and agents;
2.1.2. all employees (including temporary or contract staff);
2.1.3. all business dealings in all jurisdictions within which the Company conducts business; and
2.1.4. any actual or suspected fraudulent activity involving employees as well as shareholders, consultants, vendors, contractors, agents, and/or any other parties with a business relationship with the Company.

3. Definitions

3.1. The Board – the Board of Managers of Eurasian Resources Group SARL
3.2. Fraud - intentional abuse of position, false representation or concealment of a material fact, or prejudicing someone's rights for personal gain. Appendix 1 lists examples of actions, which are considered to fall within the definition of fraud.

4. Policy Statements

4.1. The Company acts responsibly, honestly and with integrity and does not engage in or tolerate any form of fraud. The Board through the Company's Code of Business Conduct and Company policies defines the boundaries for acceptable conduct.
4.2. The Company is committed to preventing, detecting and investigating fraud in order to build a culture with a zero tolerance for fraud.
4.3. Employees must act in the best interests of ERG at all times and must not engage in transactions or activities which substantially misuse, or use for personal gain, Company assets, defraud ERG, jeopardise ERG's integrity or reputation or which may damage ERG in any other manner.
4.4. Employees should be vigilant to any attempts of fraud and they should report suspected, attempted or actual fraud as per the Whistleblowing and Investigation Policy.
4.5. No employee will suffer in any way as a result of reporting reasonably held to be suspicions of fraud.
4.6. All Business Unit management should set and maintain cost-effective control procedures to identify, deter and detect fraud;

4.7. Business Unit management should ensure that fraud risk is considered and appropriate cost-effective controls are built into new systems and processes at the design stage;
4.8. Employees should comply with control procedures established by the Company in policies, procedures, instructions or business practice;
4.9. All incidents of actual, attempted or suspected fraud, and all instances of major control breakdown must be impartially investigated as per the Whistleblowing and Investigation Policy;
4.10. Where reasonable suspicion exists that fraud against the Company has taken place, the Company is entitled to investigate the matter thoroughly using recognised and legitimate investigative techniques.
4.11. Duly authorised investigation team shall have the right to enter any Company premises, be given access to any information requested, and have access to all staff (with reasonable notice) as part of the investigation process.
4.12. The rights of individuals will be respected during any investigation at all times.
4.13. Business Unit management should take action against individuals and organisations perpetrating fraud against the Company and seek restitution of any asset fraudulently obtained and the recovery of costs;
4.14. Business Unit management and employees should co-operate with any external investigations of fraud by the police or other appropriate authorities;
4.15. In order to promote continuous improvement around fraud prevention and detection, each fraud investigation should end with lessons learnt and practical and appropriate and proportionate recommendations for improvement with an objective to avoid similar situations in the future.
4.16. All employees and agents should be given trainings on Code of Business Conduct, including anti-fraud requirements. It is the employee's responsibility to undergo such training when provided by the Company
4.17. Group General Counsel should coordinate such Group-wide trainings, however it is the responsibility of each Business Unit Head to ensure that their staff and agents undergo such trainings on a timely and regular basis.
4.18. Any employee found to have violated Anti-Fraud Policy may be subject to disciplinary action, which could include summary dismissal. If an employee breached a law he/she can be additionally subject to civil or criminal claims.
4.19. The Group General Counsel should monitor effectiveness of this Policy and from time to time suggest to the Board improvements to this Policy to ensure the Policy remains suitable, effective and proportionate.

5. Responsibilities

5.1. The Board is responsible for establishing this Policy.
5.2. The Compliance Committee of the Board is responsible for oversight of compliance with this Policy.
5.3. The Group Chief Executive, supported by the Group General Counsel, has responsibility for implementing this policy in accordance with the requirements of the Board.
5.4. The Division and Business Unit Heads are responsible for:
5.4.1. Establishing appropriate responsibilities, procedures, training and internal controls within their respective operations to ensure the consistent implementation of this policy across all jurisdictions and compliance with its requirements.
5.4.2. Ensuring that their respective employees and all third party service suppliers acting on behalf of the Company are made aware of this policy.
5.4.3. Investigation into all known or suspected instances of fraud by an employee within their authority and in compliance with the Whistleblowing and Investigation Policy and local laws and regulations.
5.4.4. Management of any third parties employed and ensuring their adherence to this policy.
5.4.5. Ensuring compliance with this policy throughout their operations.
5.4.6. Considering risk of fraud and introducing preventative and detective controls into new and existing systems and processes.
5.4.7. Allocating sufficient and appropriate resources to implement this policy effectively.
5.5. It is the responsibility of each Company employee:
5.5.1. to comply with the Policy at all times;
5.5.2. to report known or suspected fraud, or instances of unethical or illegal behaviour within the company, as per the Whistleblowing and Investigation Policy.

6. Monitoring

6.1. The Group General Counsel should periodically, but not less than quarterly, report on the status of Anti-Money Laundering to the Compliance Committee of the Board.
6.2. Business Unit Heads and line managers should monitor effectiveness of key controls to ensure their effective mitigation of the fraud risk.
6.3. Business Units are encouraged to use data mining and data analysis to proactively manage the fraud risk and identify actual and potential problems.
6.4. Regional Management is responsible for effective implementation of this Policy in their respective areas of responsibility and for ensuring that adequate controls and procedures are implemented to ensure on-going compliance.
6.5. Internal Audit should periodically review compliance with this Policy and report any deficiencies and respective recommendations to the Group Management and the Compliance Committee of the Board.

Appendix 1

Examples of actions, which are considered to fall within the definition of fraud under the Anti-Fraud Policy. By its nature the following list is not exhaustive, but is meant only to provide guidance on types of behavior prohibited by the Company:

- theft of company property, including information;
- forgery or unauthorised alteration of company documents, accounting books, records, financial and management reports;
- falsification of signatures;
- wilful destruction or removal of company records;
- falsification of expense claims;
- unauthorised disclosure of confidential information to outside parties;
- misappropriation or use of company assets for personal gain;
- undertaking or assisting in illegal activity (including bribery, corruption, money laundering, sanctions violations, competition law violations, which are covered by the Group Anti-Bribery and Corruption Policy, Anti-Money Laundering Policy, Sanctions Compliance Policy, Anti-Trust and Competition Compliance Policy respectively);
- acceptance of bribes or gifts to favour third parties;
- unauthorised premium discounting;
- knowingly generating or paying false claims or invoices;
- concealment of material facts for the purpose of deceitful influencing management decisions;
- concealment of true nature of transactions for personal gain and/or at Company's loss;
- collusion to rig the bidding process;
- collusion to fix the prices;
- circumventing approval thresholds;
- bid rotation;
- bid suppression;
- complementary bidding; procurement, supply and acceptance of counterfeit and/or substandard materials and goods;
- artificially shortcutting procurement processes;
- abusing emergency procedures;
- knowingly using third parties for fraudulent purposes;
- procurement of goods which are not needed or which are unsuitable;
- providing unfair advantage to individual suppliers including undue advantage of information;
- approving invoices for works not done or goods not delivered;
- inflating contract prices;
- improper handling of bids, including tampering with the bid, compromising confidential bid-specific information, modification of bids or allowing such actions to be performed by others
- collusion between suppliers to defraud the Company; deliberately manipulating bid evaluation criteria or scores to get certain results;
- acting in the interest of suppliers neglecting interests of the Company;
- any other action taken for personal gain, which has an adverse impact on the Company.