Whistleblowing Policy in Eldik Bank OJSC

Content

1. GENERAL PROVISIONS....2
2. LEGAL BASIS....2
3. TERMS AND DEFINITIONS....3
4. BASIC PRINCIPLES....5
5. SCOPE AND PROCEDURE FOR REPORTING VIOLATIONS....5
6. WHILE PROTECTION, CONFIDENTIALITY, AND NON-RECOVERY....9
7. REGISTRY MAINTENANCE, INFORMATION STORAGE AND REPORTING....9
8. ROLES AND RESPONSIBILITIES....10
9. FINAL PROVISIONS....10

1. GENERAL PROVISIONS

1.1. This Whistleblowing Policy in Eldik Bank OJSC (hereinafter referred to as the Policy) sets out the commitment of Eldik Bank OJSC (hereinafter referred to as the Bank) to strengthening the system of integrity, transparency and accountability, as well as to ensuring the protection of all persons, including the Bank's employees, clients, counterparties, and other third parties, who in good faith report violations or unlawful actions, from retaliation, discrimination, or any other adverse consequences..

1.2. The purpose of this Policy is to enable and encourage the safe and confidential reporting, in good faith and without fear of retaliation, of suspected wrongdoing, violations, misconduct, and unethical practices related to the Bank's activities, including transactions financed, supported, or carried out with the participation of the Bank, as well as activities within the Bank, so that the Bank may effectively protect its interests, resources, and mission through the timely review and appropriate handling of such reports.

1.3. This Policy defines the rights and obligations of the Bank's employees, the Bank's management, and external parties in terms of reporting alleged violations, non-compliance with the legislation of the Kyrgyz Republic, internal regulations and Codes of Ethical Standards.

1.4. The Policy sets out the procedures for using reporting channels, guarantees protection from retaliation, and defines the procedures for submitting, assessing, and reviewing reports.

1.5. The Compliance Control Department is responsible for the overall oversight of the implementation of this Policy, as well as for the ongoing review, updating, and maintenance of this document.

At the same time, the structural unit implementing the function of service quality management is responsible for reviewing requests and complaints from applicants in accordance with the Bank's internal procedures for handling requests.

If a message received through one of these functions falls within the purview of another structural unit, it is immediately forwarded to the appropriate structural unit in accordance with internal procedures. The relevant functions ensure effective communication and information exchange, if necessary, while maintaining confidentiality.

2. LEGAL BASIS

2.1. This Policy has been developed in accordance with the legislation of the Kyrgyz Republic, as well as the regulatory legal acts of the National Bank of the Kyrgyz Republic (hereinafter referred to as the National Bank of the Kyrgyz Republic), which stipulate the need for the Bank to operate an effective system of internal control, risk management, compliance with ethical standards and prevention of violations.

2.2. This Policy applies in conjunction with the Bank's internal regulatory documents, which detail approaches to ensuring ethical standards, compliance risk management, and internal control. Such documents include, but are not limited to:

- Code of Business Ethics of Eldik Bank OJSC;
- Code of Business Ethics for Counterparties of Eldik Bank OJSC;
- Personnel policy of Eldik Bank OJSC;
- Gender equality policy of Eldik Bank OJSC;
- The procedure for considering Clients' requests to Eldik Bank OJSC;
- The methodology "Procedure for actions and accounting of transactions upon detection of unauthorized transactions on deposit accounts of individual clients", (currently in the process of revision and approval in a new version entitled "Procedure for actions and accounting of transactions upon detection of unauthorized transactions on client accounts and intra-bank accounts");
- Regulation on the prevention and response to cases of violence and harassment in the workplace for employees of Eldik Bank OJSC;
- Internal policies and procedures of the Bank in the area of compliance control, risk management and internal control;

2.3. This Policy has also been developed taking into account relevant international standards and best practices, including the principles of transparency, accountability and integrity applied by international financial institutions, and is aimed at ensuring compliance with the requirements of the Bank's international partners, including organizations in the field of climate finance and development. These documents enshrine the core values of the Bank and oblige the Bank's employees to act conscientiously, honestly, professionally and in the interests of the Bank in the performance of their official duties.

3. TERMS AND DEFINITIONS

For the purposes of this Policy, the following terms have the following meanings:

3.1. Whistleblowing means a report made in good faith regarding suspected or actual violations, unethical behavior, or non-compliance with applicable laws and the Bank's internal regulations.

3.2. Informant - any individual who has submitted a report in accordance with this Policy, regardless of whether such person is an employee of the Bank or an external party.

3.3. A whistleblower is a person who reports facts of corruption in good faith and is recognized as such in accordance with the Law of the Kyrgyz Republic "On the Protection of Persons Who Reported Corruption Offenses."

3.4. Applicant - any individual or legal entity (including an individual entrepreneur) who applies to the Bank with a complaint, application or request submitted within the framework of this Policy.

3.5. Protected activity - a good faith report of a suspected or actual violation, participation in an audit or investigation, provision of information or other assistance to the Bank in connection with a report submitted under this Policy.

3.6. Violation - any action or omission that violates the law, internal regulations, ethical standards or principles of good faith, including, but not limited to:

- fraud, corruption, bribery or embezzlement;
- misuse or appropriation of funds, assets or resources of the Bank;
- conflict of interest or abuse of office;
- financial irregularities, accounting irregularities or misrepresentations;
- violation of internal policies, procedures or codes of conduct;
- obstructing an audit, investigation or the functioning of the internal control system;
- concealment or failure to provide information about known violations;
- any actions or inactions that may result in financial, reputational, legal or operational damage to the Bank;
- other actions that are contrary to the principles of good faith, transparency and accountability;
- other actions that are contrary to the principles of good faith, transparency and accountability.

3.7. Confidential information is information constituting a commercial secret, personal data, or banking secrecy, as well as other information that is not publicly available, including information related to a message (including information about the identity of the informant and other involved parties), provided by an external source (such as a Bank Client or other third party) under the terms of its confidentiality, subject to protection from unauthorized disclosure, and to be used exclusively for the purposes for which it was provided. Confidential information may exist in any form (written, oral, electronic, etc.).

3.8. A report is any information, statement, or concern provided by a whistleblower regarding suspected or actual violations or sanctionable practices. For the purposes of this Policy, such reports include information about suspected or actual violations of laws, regulations, the Bank's internal documents, ethical standards, abuse, fraud, corruption, conflicts of interest, concealment of information, circumvention of control procedures, violations in projects financed by the Bank, and other actions that could cause financial, legal, reputational, or operational damage to the Bank.

For the purposes of this Policy, the following are not considered messages, unless otherwise required by the nature of the matter:

(i) standard customer inquiries and complaints regarding quality of service, products, tariffs and terms of service, as well as technical failures in the absence of signs of abuse or violation;

(ii) personnel and other HR issues (working conditions, pay, leave, schedule, etc.) in the absence of signs of violation, discrimination, harassment, abuse, conflict of interest or persecution;

(iii) requests that are not related to the subject of the Policy, contain insufficient information that cannot be supplemented, duplicate previously considered requests without new facts, already considered in another established manner, do not contain signs of a violation, or are knowingly false or submitted in bad faith.

3.9. Retaliation - means any direct or indirect adverse action taken, recommended, or threatened against a whistleblower or any person engaged in protected activity, including, but not limited to, termination, demotion, disciplinary action, harassment, discrimination, intimidation, or other forms of adverse action.

3.10. Good faith is a reasonable belief, based on available information, that the reported information is reliable and relates to violations, regardless of whether the information is confirmed during a subsequent investigation.

3.11. External party - any individual or legal entity that is not an employee of the Bank, including but not limited to clients, contractors, consultants, suppliers, partners, other interested parties, and individuals or communities who may be affected by the activities or projects financed by the Bank, irrespective of whether a formal relationship with the Bank exists.

3.12. Bank staff - all employees of the Bank, including persons working on a permanent, temporary, contract or other basis, as well as the Bank's management.

3.13. Internal audits (investigations) are the process of reviewing and evaluating a received report and, if necessary, conducting investigations to establish its validity, materiality, and the presence of signs of a violation or practices subject to sanction, as well as taking appropriate measures in accordance with the Bank's internal regulatory documents.

3.14. SEAH - complaints related to sexual exploitation, violence and harassment.

4. BASIC PRINCIPLES

The implementation of this Policy is based on the following principles:

4.1. Confidentiality: All information related to reports of illegal activity is strictly confidential. The identity of the complainant will not be disclosed without their consent, except in cases required by law.

4.2. Protection from Retaliation: The Bank ensures that no person who reports in good faith possible violations will be subject to retaliation, including dismissal, demotion, harassment or other adverse action.

4.3. Good Faith in Reporting: Reports must be made honestly and with reasonable grounds to believe that the information contained in the report is true.

4.4. Accessibility: Channels for reporting illegal activities must be accessible to all stakeholders, including Bank employees, customers, partners and other external parties.

4.5. Impartiality and Objectivity: All reports will be reviewed and, where appropriate, investigated in an impartial and objective manner, without conflict of interest.

4.6. Timeliness: Reports will be reviewed and processed within a reasonable and clearly defined timeframe, ensuring a prompt response while respecting the principles of due process.

4.7. Accountability: The Bank ensures that appropriate action is taken following up on confirmed reports, including corrective and disciplinary action.

4.8. Right to external appeal: The Bank recognizes the right of any person to appeal to government agencies (the National Bank of the Kyrgyz Republic, law enforcement agencies) in the event of a justified mistrust of the objectivity of the internal investigation process or in the event of a threat to life/health.

5. SCOPE AND PROCEDURE FOR REPORTING VIOLATIONS

5.1. Scope of application.

This Policy applies to all Bank employees, including management, as well as external parties, such as clients, counterparties, consultants, contractors, partners, and other individuals, groups, or communities affected by the Bank’s activities. It covers any person who, in good faith, reports suspected wrongdoing, violations, misconduct, or unethical practices related to the Bank’s activities, including financed projects. The Policy also extends to employees and external parties whose actions or inactions may be subject to review, or investigation in connection to suspected violations or wrongdoing.

5.2. Reporting violations.

5.2.1. Bank employees and other persons covered by this Policy who become aware of suspected violations are encouraged to promptly report them through the channels provided for in this Policy, if there are reasonable grounds to believe that such information is reliable.

5.2.2. The whistleblowing channels provided for in this Policy are used to report suspected violations, including in cases where the matter involves a violation of the law, ethical standards or principles of good faith, when there are grounds to believe that the matter cannot be effectively addressed within the framework of the Bank's standard procedures, and also when an individual is subject to or reasonably fears persecution (retaliation) in connection with filing a report.

5.3. Channels for messages.

The Bank provides accessible, secure, and confidential channels for reporting violations and illegal activities. Reports can be submitted by Bank employees and external parties through internal and external communication channels.

5.3.1. Internal communication channels

- The Bank maintains dedicated internal reporting channels, including a Helpline, for Bank employees to report violations, unlawful actions, unethical behavior, and breaches of internal regulations.
- These channels ensure confidentiality, secure processing of information and protection of persons sending messages in good faith.
- Messages through internal channels can be sent either with the identity of the applicant or anonymously.
- Information about the Helpline is regularly communicated to Bank employees and can be accessed through internal communication channels doverie@eldik.kg , including access via QR code.
- An additional channel for submitting reports is also available - the Compliance Control Department's email address: risk_compliance@rsk.kg; risk_compliance@eldik.kg

5.3.2. External communication channels

External parties may report unlawful activity through the Bank's existing communication channels, which are also used to receive requests and complaints from applicants, including:

- oral channels (via hotline/ call center or in person);
- written appeals (submitted in person, by mail or through the Book of Registration of Complaints and Suggestions);
- electronic channels (including email, online chats, the “Feedback” section on the Bank’s official website and a mobile application);
- Bank's official pages on social networks.

External parties may report unlawful activity through the Bank's communication channels, including:

- General email address: info@eldik.kg
- Call center (24 hours): **9111;**
- WhatsApp communication channel: **+996 (706) 911111;**
- an online form for submitting a message, available on the Bank's official website: https://eldik.kg/en/feedback
- For counterparties: email ethics@rsk.kg; ethics@eldik.kg

Messages can be sent:

- openly (indicating the identity of the applicant);
- confidentially;
- anonymously.

To ensure effective consideration of communications, applicants are encouraged to provide as complete and accurate information as possible, including, where available:

- a description of the alleged violation or unlawful act;

- the date, location, and circumstances of the incident;
- information about how the alleged violation was committed;
- information about persons who may be involved in the violation;
- documents, materials, or other evidence supporting the stated facts.

Anonymous reports: The Bank accepts anonymous reports; however, the ability to provide feedback to the complainant regarding the status or outcome of the review may be limited due to the absence of contact information. Violation reports may also be sent directly to the relevant Bank departments. Such reports must be registered in the Service Quality Department's unified electronic log. The department that receives such reports directly is responsible for forwarding them to the Service Quality Department for subsequent registration.

5.4. Identification and redirection of messages to the relevant structural divisions of the Bank.

In cases where reports of illegal activities are sent via electronic channels, including the Bank's official website or e-mail, the Bank shall ensure the availability of a special classification mechanism (a separate category or function "Whistleblowing").

This mechanism ensures the identification and differentiation of reports of illegal activity from general inquiries and complaints, and their subsequent forwarding through the internal routing system to the appropriate Bank departments for further review, depending on the nature of the report. Initial receipt and registration of reports is carried out by the Bank's Service Quality Department.

During the initial review of the message, the Service Quality Department, guided by the internal regulatory document of the Bank establishing the procedure for reviewing appeals from applicants of Eldik Bank OJSC, classifies the received messages by violation categories and, in accordance with the established procedure, forwards them to the relevant structural divisions of the Bank for review according to their competence:

- issues related to combating the financing of criminal activities and the legalization (laundering) of criminal proceeds (AML/CFT) - to the Compliance Control Department;
- issues related to violation of professional and business ethics, conflicts of interest, abuse of office and other issues of labor discipline - to the HR Department;
- issues related to corruption, illegal actions, internal violations, irregularities in procurement and selection of suppliers, fraud, operational incidents, security issues, as well as cases that have resulted or potentially could result in material or reputational damage to the Bank are referred to the Security Department;
- issues related to fraud, operational incidents, as well as activities related to payment terminals and remote servicing of transactions - to the relevant authorized structural divisions of the Bank

The Bank ensures that information about reporting channels is posted on the Bank's official website, and that this information is communicated to Bank employees through internal communication channels.

5.5. Standards for objective review and conducting an internal investigation

The consideration of reports of violations and illegal actions, as well as the conduct of official inspections and investigations, are carried out based on the principles of objectivity, impartiality, confidentiality, respect for the rights of all parties involved, and the prevention of conflicts of interest.

The relevant structural divisions of the Bank, including, but not limited to, divisions responsible for reviewing individual categories of reports, when conducting internal audits and investigations, are guided by the internal regulatory documents of the Bank governing the relevant areas of activity, including, but not limited to:

- Compliance Control Department - the Bank's Anti-Corruption Policy, the Code of Business Ethics, internal policies and procedures in the area of compliance, anti-money laundering and

combating the financing of terrorism (AML/CFT), as well as other internal documents in the area of compliance and risk management;

- HR Department - the Bank's HR Policy, the Code of Business Ethics, the Gender Equality Policy, the Regulation on the Prevention and Response to Cases of Violence and Harassment in the Workplace, as well as other internal documents regulating issues of labor relations and professional ethics;
- The Security Department - internal regulatory documents of the Bank in the area of ensuring security, preventing and detecting fraud, conducting official audits, internal control, as well as other documents regulating the investigation of violations and illegal actions.

This Policy establishes uniform principles, requirements and procedures for the receipt, registration, consideration of reports of violations, protection of complainants, conducting inspections and monitoring.

5.5.1. Reports and complaints related to incidents of Sexual Exploitation, Abuse and Harassment (SEAH), including those submitted by third parties, clients, partners, contractors, and other stakeholders, shall be reviewed in accordance with this Policy, as well as the internal document of the Operational Control Service (OCS) 'Procedure for Handling Applicants' Complaints in Eldik Bank OJSC' and other applicable internal regulatory documents of the Bank.

The review of such complaints shall be carried out in compliance with the principles of confidentiality, objectivity, avoidance of conflicts of interest, and protection of complainants and survivors from retaliation or discrimination, while also ensuring timely response and appropriate support measures depending on the nature of the incident.

5.6. Procedure for conducting an official investigation (check)

An investigation (internal review) is conducted in cases where, based on the results of the initial assessment, it is established that the report contains signs of a violation, illegal actions or practices subject to sanction and requires further verification.

As part of the investigation, measures may be taken to establish the factual circumstances, including the analysis of documents and information, interviews with employees and other persons, requests for additional documents and information, interaction with the relevant structural divisions of the Bank, as well as other actions necessary for a comprehensive, complete, objective, independent and impartial consideration of the report.

Bank employees are obliged to facilitate the conduct of an internal investigation and, upon request, provide the necessary documents, information, and explanations within the scope of their job responsibilities and in accordance with the Bank's internal regulatory documents.

Based on the investigation's findings, a report is prepared. It must include a description of the report reviewed, information on the measures taken, the facts established, conclusions regarding the presence or absence of a violation, as well as information on the measures taken and recommendations for further action. The results of the internal investigation are sent to the Chairman of the Management Board and may be shared with other departments only by a corresponding resolution.

5.7. Taking action based on the results of reviewing reports

Based on the results of the investigation, the Bank takes appropriate measures depending on the nature and severity of the violation identified.

Such measures may include:

- disciplinary measures;
- corrective measures;
- strengthening internal control procedures;
- termination of an employment contract;
- termination of the contract with the counterparty;

- transfer of materials to law enforcement agencies;
- other measures in accordance with the internal documents of the Bank and the legislation of the Kyrgyz Republic.

All reports are reported to the Bank's management. Depending on their seriousness and scale, issues are submitted to management for review.

Information on the results of the review of the application is also communicated to the applicant after agreement with the relevant structural divisions and if his contact information is available.

5.8. Message review timeframes

The period for registering a message is no more than 1 (one) business day from the moment of its receipt.
The period for confirming receipt of a message (if contact information is available) shall not exceed 5 (five) working days from the date of registration of the message.
The investigation period shall be up to 30 (thirty) calendar days and may be extended if necessary, depending on the timeframes established in the relevant internal regulatory documents of the Bank.

6. PROTECTION OF INFORMANTS, CONFIDENTIALITY AND PROHIBITION ON RETALIATION

6.1. The Bank ensures the protection of complainants, witnesses and other persons involved in the consideration of reports from any form of retaliation, including dismissal, demotion, disciplinary measures, pressure, discrimination or other adverse consequences associated with the good faith reporting of violations or illegal actions.
Protection from retaliation extends not only to the whistleblower but also to anyone assisting in the reporting or investigation, including witnesses, representatives, support workers, and others who may be adversely affected by the reporting.

6.2. Any actions aimed at persecuting the applicant are considered a violation and may result in disciplinary or other measures in accordance with the Bank’s internal documents and the legislation of the Kyrgyz Republic.

6.3. The Bank ensures the confidentiality of information about the applicant's identity, as well as other information related to the message, and takes measures to protect such information from unauthorized access and disclosure.

6.4. Disclosure of information about the applicant's identity is permitted only:

- with the consent of the applicant;
- in cases stipulated by the legislation of the Kyrgyz Republic;
- to the extent strictly necessary to conduct an inspection or comply with legal requirements, with prior notice to the applicant, if this is possible and not prohibited by law, and does not create a risk to the investigation.

6.5. If facts of persecution are confirmed, the Bank takes measures to protect the applicant and restore his rights.

7. REGISTRY MAINTENANCE, INFORMATION STORAGE AND REPORTING

7.1. All reports of violations and illegal actions are subject to mandatory recording, registration in a single electronic journal and storage in accordance with the procedure established by the Bank.

7.2. The Bank maintains a single electronic journal (register) designed to record requests and messages from applicants.

7.3. The Service Quality Department receives messages, registers them, distributes them to the appropriate structural divisions, and then consolidates the information and maintains an electronic journal (register).
7.4. The electronic journal (register) records information on messages, including information on the channel of receipt, type of request, category, responsible department and other data in the volume determined by the Bank.
7.5. The electronic journal (register) is maintained on a permanent basis and is subject to storage in accordance with the Bank's internal regulatory documents, while observing the requirements of confidentiality and limited access.
7.6. Access to the electronic journal (register) is limited and provided only to authorized persons in compliance with the requirements of the Kyrgyz Republic legislation on personal data and banking secrecy.
7.7. Materials on received messages are stored in the Bank in accordance with the nomenclature of cases and applicable requirements of the legislation of the Kyrgyz Republic.

8. ROLES AND RESPONSIBILITIES

8.1. The Compliance Control Department is responsible for the overall oversight of the implementation of this Policy, as well as for the ongoing review, updating, and maintenance of this document.
8.2. The Service Quality Department receives, registers, and distributes messages to the relevant Bank divisions, ensures the consolidation of information based on their review, maintains an electronic message log (register), and ensures the completeness, relevance, and accuracy of the data entered into it. When necessary, the Service Quality Department generates downloads and summary information based on the registry data.
8.3. The Bank's structural divisions involved in the process of reviewing reports ensure that they are reviewed within the limits of their competence and are responsible for the timely, complete and accurate provision of information to the Service Quality Department on the results of the review of reports, including information on the details of the request, the measures taken and the final decisions.
8.4. Summarized information on received messages is generated by the Service Quality Department based on the data of the electronic journal (register) and is provided in the format established by the National Bank of the Kyrgyz Republic to the Bank's management, and can also be used for the purposes of preparing the Bank's non-financial reporting (including ESG, sustainable development and corporate governance), internal control, risk management and employee training.

9. FINAL PROVISIONS

9.1. This Policy shall enter into force upon approval by the Board of Directors and shall be subject to mandatory implementation by all structural divisions of the Bank and officials of the Bank who are participants in the described process.
9.2. In the event of a change in the organizational structure of the Bank/job titles, the functions of the divisions/specialists involved in this Policy shall be performed by the divisions/specialists to which these functions will be transferred in accordance with the new organizational structure.
9.3. If, as a result of changes in the current legislation of the Kyrgyz Republic, individual clauses of this Policy conflict with them, then until the relevant changes are made to the Policy, the provisions of the legislation of the Kyrgyz Republic shall apply.
9.4. In the event of any contradictions between the provisions of this Policy and other internal regulatory documents of the Bank regarding the procedure for reporting violations, protecting complainants,

registering reports, the procedure for their consideration and conducting inspections, the provisions of this Policy shall take precedence.

9.5. The heads of the Bank's structural divisions are responsible for organizing the timely familiarization, study, application and use of this Policy by employees.

9.6. This Policy shall be reviewed at least once a year, as well as unscheduled when new risks or vulnerabilities are identified, based on the results of internal and external audits, and as necessary, in order to bring the processes defined by the Policy into compliance with current requirements requiring updating the Policy.

9.7. Issues not regulated by this Policy are governed by the current legislation of the Kyrgyz Republic and regulatory legal acts, decisions of the Board of Directors of the Bank and other internal documents of the Bank.

9.8. This Policy shall be communicated to the Bank’s employees and posted on the Bank’s official website.