| | |
|---|---|
| Normative internal legal act title | **Standard for the implementation and management of the Group's internal whistleblowing channels** |
| Process title | Setting up and management of internal violation reporting channels |
| Process owner (unit) | Business safety |
| Approving company | AB Ignitis grupė |
| Position/body of the certifying officer | Business Resilience Manager |
| Effective date | Coincides with the date of approval |

# STANDARD FOR IMPLEMENTATION AND MANAGEMENT OF THE GROUP'S INTERNAL CHANNELS FOR REPORTING VIOLATIONS

## 1. PURPOSE AND SCOPE

1.1. Purpose – to establish the procedures for reporting possible violations being prepared, committed, or ongoing within the Group, receiving such reports through the internal reporting channel (hereinafter referred to as the Trust Line), evaluating the information, and making decisions..

1.2. Applicable to all Group companies and their employees.

## 2. DEFINITIONS

2.1. General terms of the glossary: Group of companies/group, employee, company.

2.2. **Whistleblower** – a natural person providing information about a violation within an organisation, learned from their current or past service, work, or contractual relationships (such as consultancy, contracting, subcontracting, internships, practical training, volunteer work, etc.) with the organisation, or during pre-contractual relations, including self-employed persons, shareholders, members of the company's administrative, management, or supervisory bodies (including non-executive members, volunteers, and paid or unpaid interns), or any natural person working under the supervision and direction of contractors, subcontractors, and/or suppliers.

2.3. Law – the Republic of Lithuania Law on the Protection of Whistleblowers.

2.4. **Competent Entity (Person)** – a person, group of persons or special unit within the Group designated by the Group to manage the internal Whistleblowing Channel, to receive, evaluate and process the information received through it, and to ensure the confidentiality of the person submitting the Whistleblowing Information.

2.5. **Competent authority** is the Prosecutor General's Office of the Republic of Lithuania, which, in accordance with the Law on the Protection of Whistleblowers, recognises persons who provide information about a violation as whistleblowers, receives, examines or transmits to other authorities, within the scope of its competence, reports or information about violations for examination.

2.6. **Confidentiality** – a principle of activities of the Group's Employees, which ensures that the data and other directly or indirectly identifiable information of the person who has provided the information on the infringement are processed only for the purpose of carrying out their work functions, and that this information is not disclosed to third parties, except in the cases provided for in the Law on the Protection of Whistleblowers or in other legal acts.

2.7. **Violation** – a criminal offence, administrative offence, official misconduct or breach of employment duties that may be being prepared, committed or committed within the Group of Companies, as well as a serious violation of mandatory standards of professional conduct, an attempt to conceal the offence in question, or any other offence which threatens or infringes the public interest, which come to the knowledge of the person who has disclosed the infringement through their service, employment or contractual relationship (consultancy, contract, subcontract, traineeship, internship, voluntary activity, etc.) with the institution or in the course of recruitment or other pre-contractual relationships.

2.8. **Whistleblower** – a person who has provided information about a possible violation of the Group Employee's legislation and has been recognised as a whistleblower by the competent authority.

2.9. **Report** – any information about a Violation submitted by the reporting person through the Internal Reporting Channel in any form (verbally, in writing, by phone, or by email) that meets the criteria set forth in the Law. Providing information solely to protect personal interests is not considered a

report meeting the criteria established in the Republic of Lithuania Law on the Protection of Whistleblowers (hereinafter the Law).

2.10. Other terms used in the Standard shall be understood as defined in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter referred to as the "Regulation"), in the Republic of Lithuania Law on the Legal Protection of Personal Data, in the Republic of Lithuania Law on the Protection of Whistleblowers, and in the Description of the Procedures of the Establishment of the Internal Channels of Information on Violations and Ensuring their Functioning, as approved by the Government of the Republic of Lithuania in 2018. "On the implementation of the Republic of Lithuania Law on the Protection of Whistleblowers".

## 3. GENERAL PROVISIONS

3.1. This Standard is prepared in accordance with:

3.1.1. The Republic of Lithuania Law on the Prevention of Corruption;

3.1.2. The Republic of Lithuania Law on the Protection of Whistleblowers;

3.1.3. the Description of the Procedure for the Implementation and Functioning of the Internal Information Channels for the Provision of Information on Violations, approved by Resolution of the Government of the Republic of Lithuania No 1133 of 14 November 2018 "On the Implementation of the Republic of Lithuania Law on the Protection of Whistleblowers" (the Government's Description);

3.1.4. Standard LST ISO 37001:2017 "Anti-Corruption Management Systems. Requirements and Guidelines for Use."

3.2. The Trust Line is a necessary good practice tool for promoting violation prevention and transparency, strengthening violation prevention, and increasing employee and public trust in the Group of Companies.

3.3. Information about the Trust Line is provided on the Group's external and internal websites.

## 4. PURPOSE OF THE INTERNAL WHISTLEBLOWING CHANNEL

4.1. To enable persons who are or were connected with the Group through employment or contractual relationships to provide information about violations within the Group, in accordance with the provisions of the Law.

4.2. To implement the requirements of the Law and the provisions for whistleblower protection.

4.3. To promptly forward information about violations to the competent authority for review and to make a decision regarding the whistleblower status.

4.4. To prevent possible illegal actions by Group Employees and to take action for applying liability measures to Employees who have committed violations.

4.5. The internal whistleblowing channel can be used to report the following violations identified within the Group for:

4.5.1. offences of a corrupt nature (administrative offences, breaches of employment obligations committed through abuse of power and directly or indirectly for the purpose of benefiting oneself or another person, as well as criminal offences of a corrupt nature).

4.5.2. breaches of the Anti-Corruption Policy, the provisions of the Code of Conduct for Employees, and the requirements of the Anti-Corruption Management System.

4.5.3. breaches of procurement.

4.5.4. improper performance or non-performance of staff members' job duties.

4.5.5. infringements of the rules on declaration of private interests.

4.5.6. cases of fraud and deception.

4.5.7. other irregularities.

## 5. SUBMISSION, RECEIPT, REGISTRATION, AND FORWARDING OF INFORMATION ABOUT VIOLATIONS

5.1. A person can submit a report through the internal channel in the following ways:
- 5.1.1. Send a report to Ignitis Group's email address pasitikejimolinija@ignitis.lt;
- 5.1.2. Leave a message on the Trust Line voicemail (tel. +370 640 88889);
- 5.1.3. Fill out the Violation Report **Form**.
- 5.1.4. Visit Ignitis Group during official working hours and report directly to the competent entity.
- 5.1.5. Send a signed report by mail to Ignitis Group.Laisvės pr. 10, LT-04215 Vilnius. When sending a report by mail, the envelope should be marked with "To be delivered in person to the Competent Entity" under the Ignitis Group name.

5.2. A person can submit a violation report by:
- 5.2.1. Completing and signing the Violation Report Form as specified in Annex 1 of the Standard.
- 5.2.2. Providing a signed free-form report indicating it is submitted in accordance with the Law.

5.3. A person submitting a free-form violation reports must specify in the reports:
- 5.3.1. Their name, surname, personal code, workplace, and other contact details (email address, phone number, correspondence address as chosen by the person).
- 5.3.2. Known information about who, when, how, and what violation was committed, is being committed, or is being prepared. the date and circumstances of learning of the infringement; whether the infringement has already been notified; if notified, who was notified and whether a reply was received;
- 5.3.3. any other documents, data or information available to the Commission which may reveal the elements of a possible infringement.

5.4. Reports of breaches received by the Trust Line shall be registered by the competent entity, which administers the internal channel within the Group and is responsible for the enforcement of the requirements of the Law. The competent entity transfers the incoming reports to a computerised workstation and stores them on a network disk with restricted access rights.

5.5. Upon receiving a report, the competent entity must immediately, but no later than 2 business days from the date of receipt, forward the information to the authorised investigating institution without the consent of the person who submitted the information and informs the person about it. The competent entity must take a decision on the examination of the submitted information complying with the provisions of the Law within 5 business days from the date of receipt of the information and inform the person who submitted the information about the Infringement in writing.

5.6. The competent entity decides whether to examine or refuse to examine the report submitted through the internal channel. Upon deciding to examine the report, the competent entity creates a task in the JIRA system, specifying the responsible executor(s).

5.7. The competent entity or another Group employee, based on their competence, is appointed as the responsible executor to examine reports on violations that meet the criteria of this Standard. The responsible executor(s) must adhere to the provisions of the Law and the Standard.

5.8. If a report about a violation, meeting the requirements of the Law, is received by the Group via an email address other than that specified in clause 5.1.1 of the Standard, or by mail, it is not registered and is immediately forwarded to the email address specified in clause 5.1.1 of the Standard or handed over to the competent entity without disclosing the received information to third parties. Information about the violation received and/or forwarded via another email address must be immediately deleted.

5.9. Information is provided to persons who submitted reports only if their contact details are provided.

5.10. Where the information provided is the subject of a pre-trial investigation, an investigation into a possible disciplinary offence, an investigation into misconduct in office, procedures for controlling the recording and management of the Information received, and in any other cases provided for by law, the Information received may be copied, listened to or reviewed. The competent entity registering this information notes these actions in the remarks field of the virtual repository where the information is kept.

5.11. Information about a violation is not registered or investigated if:
    5.11.1. The information cannot be read or is improperly submitted, i.e., it is impossible to understand, read, or listen to the content;
    5.11.2. The information is obscene or offensive;
    5.11.3. The content of the information is meaningless or related to advertising;
    5.11.4. Information relating to personal interest.
5.12. Information about whistleblowers cannot be provided to persons not participating in the investigation.
5.13. Information received via the Trust Line is stored for one year and deleted after this period unless otherwise stipulated by law.

## 6. GROUP'S COMPETENT ENTITY

6.1. The Group's competent entity, in implementing the requirements of the Standard, shall perform the following functions:
    6.1.1. analyse and investigate information about violations received via the Trust Line;
    6.1.2. ensure the confidentiality of the person who submitted the information about the violation via the Trust Line;
    6.1.3. cooperate with the Group's Employees and structural units, competent authorities, and/or other institutions or agencies investigating violations, providing and/or receiving necessary information;
    6.1.4. collects and compiles personalised statistics on the number of reports received and the outcome of their processing;
    6.1.5. ensure that information about violations reported via the Group's Trust Line is collected and stored in the JIRA system, where necessary information can be found.
    6.1.6. perform other functions described in the Standard.
6.2. The Group's Competent Entity must not be influenced or otherwise obstructed in performing the functions assigned to it by this Standard. In carrying out the functions set forth in the Standard, the Group's Competent Entity shall have the right to:
    6.2.1. receive necessary information and data from other Group Employees and structural units;
    6.2.2. interview employees and other persons related to the verified information and obtain their explanations;
    6.2.3. consult with specialists and obtain their conclusions;
    6.2.4. in accordance with legal requirements, review documents related to the verified information and obtain copies thereof;
    6.2.5. make decisions related to the investigation of information received through the Trust Line, which are binding on all Group employees and structural units;
    6.2.6. perform other necessary actions permitted by legal acts.
6.3. Once a year, the Group's Competent Entity shall summarise the data on the receipt and examination of information about violations received during the previous year and publish statistical data on the effectiveness of the Trust Line (such as the amount of information about violations submitted via the Trust Line, how much information was examined, and how much was forwarded to competent authorities) and other relevant information related to the submission and examination of information about violations within the Group on the Group's website.
6.4. The Group's Competent Entity and/or Employee is prohibited from evaluating and examining the submitted information about the violation if it creates a potential conflict of interest.
6.5. Letters transmitting the received information about the violation to competent authorities, other state or municipal institutions or agencies, and responses to persons who have submitted information about the violation under the Law on the Protection of Whistleblowers, etc., shall be signed by the Group's Business Resilience Manager.
6.6. If the behaviour of the person or their representative providing information about the violation orally is inappropriate or shows obvious signs of a crime, criminal offense, or administrative offense, the

Group's Competent Entity shall have the right not to serve such a person and must immediately report the person's behaviour to their direct supervisor.

## 7. ASSESSMENT AND DECISION-MAKING REGARDING SUBMITTED INFORMATION ABOUT VIOLATIONS

7.1. The Group's competent entity evaluates the information about the violation received via the Trust Line to determine:

7.1.1. Whether there are deficiencies in the information submission, as outlined in clause 5.12 of the Standard, which would prevent the information from being registered;

7.1.2. Whether the information provided through the Trust Line meets the content requirements of a report and pertains to violations specified in Article 3 (2) of the Law on the Protection of Whistleblowers, and whether the person seeks whistleblower status. If it is unclear from the submitted information whether the person seeks whistleblower status, the competent entity promptly contacts the person using the provided contact details to clarify this circumstance;

7.1.3. Whether the report received via the Trust Line is anonymous and/or unsigned;

7.1.4. Whether the Group is competent to investigate the received information about the violation. If it is not entirely clear, the Group's competent entity undertakes initial information clarification actions and determines this circumstance.

7.1.5. In order to assess whether the information about the breach complies with the provisions of the Law on the Protection of Whistleblowers or falls within the Group's competence, the Group's Competent Entity may submit a request to any employee of the Group, depending on their job functions and the information at their disposal, who shall be obliged to provide the information necessary for the examination of the information about the breach without delay, and at the latest within the time limit specified by the Group's Competent Entity.

7.2. The Group's competent entity, after evaluating the submitted and registered information about the violation, makes one of the following decisions:

7.2.1. to examine the submitted information on a breach;

7.2.2. if it is established that a person has submitted a report in the form prescribed by the Government Description or a free-form report containing the information referred to in clauses 5.3 to 5.3 of the Standard, to forward the information on the reports to the competent authority to make a decision on the granting of the whistleblower status to the person, and, in case the Group is in a position to investigate the reports submitted by the person (relating to ethical breaches, disciplinary breaches, etc.), to start the examination of the information on the violation and to inform the person who has provided the information about it;

7.2.3. if it is established that a person has submitted a reports in the form prescribed by the Government's Description, or a free-form reports containing the information specified in points 5.3 – 5.4 of the Standard, but the Group is not competent to examine it (when the reports provides information on a criminal offence, an administrative offence outside the Group's competence, a disciplinary offence committed by an employee of another enterprise, institution, etc.)), within 2 business days from the date of receipt of the report, forward the information about the report to the competent authority and inform the person who submitted the information about it;

7.2.4. If it is found that the information about the violation is not related to the purpose of the Trust Line but falls within the Group's competence (e.g., discrepancies in electricity contracts, possible electricity theft, etc.), this information is forwarded to the responsible entity and noted in the JIRA system.

7.2.5. If it is determined that the information about the violation reasonably suggests that a criminal act, administrative offense, or other violation, which is not within the Group's

competence, is being prepared, committed, or has been committed, the information about the possible violations must be forwarded to the authorised state or municipal institution or agency within 2 working days from the date of receipt without the consent of the person who provided the information about the violation, and the person is informed (if their contact information is known).

7.3. The Group's competent entity may terminate the examination of the submitted information about the violation if it is found that:
  7.3.1. the report is based on information which is manifestly untrue;
  7.3.2. The information is abstract, based on the general statements or personal opinions of the person who provided it, and cannot be verified;
  7.3.3. The report is vague, i.e., it does not specify the complained actions (or inactions) and the factual circumstances or data supporting them, the content is unclear, and therefore the report cannot be examined.
  7.3.4. The information provided about the violation has already been reviewed and a decision has been made or it is still under review. If new legal or factual circumstances arise that were not present or known at the time of the decision not to examine the provided information about the violation, the Group's competent entity may decide to review the submitted information.
  7.3.5. another institution is reviewing the information about the violation.
  7.3.6. The information is not related to the purpose of the Trust Line and must be examined under the Law on Public Administration or other special laws.
  7.3.7. The information provided about the violation is not within the Group's competence and there is no other entity to which the received information can be forwarded for examination;
  7.3.8. other justified reasons.

7.4. The Group's competent entity informs the person who submitted the information about the violation in writing of the decision to examine or refuse to examine the report received via the Trust Line no later than 10 business days from the date of receipt of the information about the violation.

7.5. If the verification of the information on the violation reveals indications of a possible breach by a Group Employee, the competent entity shall, by notification, propose to the Group's Business Resilience Manager to initiate an investigation into the potential violation by the Employee.

7.6. It is prohibited to forward the information about the violation received via the Trust Line to the Employee whose actions are being complained about.

7.7. If the person who submitted the information about the violation did not receive a response or if no action was taken by the Group in response to the submitted information about the violation, they have the right to directly contact the competent authority and submit a report in the prescribed form about the violation in accordance with Article 4 (4) (4) of the Law on the Protection of Whistleblowers.

## 8. ENSURING CONFIDENTIALITY

8.1. The Group's competent entity ensures the confidentiality of the person who submitted the information about the violation, except in cases specified by the Law on the Protection of Whistleblowers or when the person themselves requests in writing or if the provided information is knowingly false.

8.2. Confidentiality is ensured from the moment the information about the violation is received, regardless of the outcome of the investigation into the received information about the violation. The provision of data and other information about the person who submitted the information about the violation to pre-trial investigation or other competent institutions or agencies, employees, without disclosing these data to persons not involved in the investigation of the violation, is not considered a breach of confidentiality.

8.3. The Group implements measures to ensure that access to the information and documents received via the Trust Line and stored by the Group, which contain data allowing the identification of the person who submitted the information about the violation, is restricted to the Group's competent entity, and that the data of the person who submitted the information about the violation, allowing their identification, are provided only to persons examining the information about the violation and conducting the investigation of the received information about the violation.
8.4. The confidentiality of the person or whistleblower who submitted the information about the violation must be ensured during public administration, investigation of work duty violations, or administrative proceedings, as far as is objectively possible considering the submitted data and its connection to the person or whistleblower providing the information about the violation.
8.5. Employees who, due to their duties, become aware of the personal data of the person who submitted the information about the violation or the content of such information, must ensure the confidentiality of this information and personal data both during their employment with the Group and after the termination of their employment.
8.6. Information about the violation submitted via the Trust Line is collected and stored in a separate section of the JIRA system, where necessary information related to the violation can be found. Access to this part of the JIRA system is granted only to the competent entity.
8.7. The JIRA system section also stores recorded conversations, if such recordings are made, minutes of meetings, and other information related to the reported violation, involving the person providing the information and the competent entity. Information about violations is stored for five years from the date of the last decision made during the review of this information. The storage period of information about violations in the Group may be extended by a justified order from a competent authority.
8.8. Employees can be granted access to certain parts of the information only with a justified and necessary basis. The decision to grant access is made by the business security manager.
8.9. Employees who, due to their functions, may become aware of the data of the person who submitted the information, are made aware of their responsibility for violating whistleblower protection requirements as stipulated in the Law on the Protection of Whistleblowers and/or other legal acts, and commit not to disclose such information or data to third parties (Annex 2).

## 9. FINAL PROVISIONS

9.1. The Group's website publishes information about the designated Group Competent Entity, their contact details, procedures for submitting and examining information about violations within the Group via the Trust Line, legal protection measures for the person who submitted the information about the violation, which protect against adverse actions as specified in Article 11 (3) and (5) of the Law on the Protection of Whistleblowers, ways to provide confidential consultations to persons considering and having submitted information about the violation, and other relevant information related to the submission and examination of information about violations within the Group.
9.2. Before any action is taken against the person who provided information about the violation or the whistleblower, or persons associated with them, it is prohibited from the day of information submission to undertake, threaten to undertake, or attempt to undertake any adverse actions as specified in Article 10 (1) and (3) of the Law on the Protection of Whistleblowers. This prohibition applies to the employer and other Group employees.
9.3. If certain issues related to the administration, registration, examination, or decision-making regarding the information about violations are not regulated by the Standard, the provisions of the laws of the Republic of Lithuania shall apply.
9.4. The Standard is approved, amended as necessary, or declared void by the Group's Business Resilience Manager. The Standard is reviewed as needed or when there are changes in legal requirements, but not less frequently than every two years. The Group's Business Security Manager is responsible for the implementation, oversight, and control of the Standard.

9.5. This Standard is publicly available on the Group’s website and intranet.