PROCEDURE FOR REPORTING WORK-RELATED BREACHES IN MAINOR GROUP

This document describes the principles and guidelines implemented in Mainor Group (parent company AS Mainor and group companies AS Mainor Ülemiste, AS Eesti Ettevõtluskõrgkool Mainor (Estonian Entrepreneurship University of Applied Sciences), OÜ Tallinn International School, and AS Dvigatel-Energeetika, hereinafter referred to as Mainor Group) that ensure the possibility to safely and confidentially report any misconduct and/or breach related to work activities, providing protection to the reporting person based on Act on Protection of Persons Who Report Work-Related Breaches of European Union Law[1].

1 BREACH

1.1 The principles and guidelines provided in this procedure apply to all employees of Mainor Group, members of the management and supervisory boards, and other persons listed in § 3 (1) of the Act on Protection of Persons Who Report Work-Related Breaches of European Union Law, who have a work-related connection with Mainor Group, regardless of their position or status (e.g., temporary employees, interns, external consultants, and service providers operating under authorisation agreement, contract, or other agreement).

1.2 Misconduct and breach (including potential misconduct and breach) refer primarily to the breach of applicable laws by the persons listed in point 1.1., or actions that are contrary to the purpose of the law or the internal rules of Mainor Group (hereinafter collectively referred to as work-related breach).

1.3 Reports can be made about any work-related breach, regardless of whether it is directly related to the breach of European Union Law. Reports can include, for example, topics such as:

- misuse or appropriation of company resources;
- fraud, forgery, corruption, and offering, giving, receiving, or soliciting bribes;
- breach of occupational health and safety requirements, endangering or harming someone's life and health;
- any crime or failure to fulfill lawful obligations by the organization;
- breach of privacy and personal data protection;
- tax fraud and breach of internal market rules;
- breach of public procurement rules;
- financial services, products, and markets, including prevention of money laundering and terrorist financing;
- breach of product safety and compliance requirements.

1.4 The reporting person must act in good faith and sincerely and reasonably believe that the information provided and the allegations contained therein are true – the reporting person must have justification and/or evidence that the information about the work-related breach is true.

[1] https://www.riigiteataja.ee/en/eli/520092024001/consolide

1.5 The procedure for reporting work-related breaches is not intended for resolving labor disputes or submitting false or malicious information.

1.6 Obstructing the reporting of breaches or knowingly providing false information is prohibited and punishable.

2 REPORTING

2.1 The reporting person can submit a report about a work-related breaches (hereinafter referred to as breach report) through the following channels:

- email address: vihje@mainor.ee;
- web form (anonymous option): https://forms.office.com/e/BZwTAyUdqn
- face-to-face meeting, which can be arranged by sending an email to vihje@mainor.ee.

2.2 When reporting a work-related breach, the following must be provided:

- the content of the incident, specifying as concretely and accurately as possible all possible facts and any possible (emerging) damage;
- the time and place of the incident (if the exact date is unknown, then approximate time);
- persons involved in the incident (name, position, company);
- evidence (photos, documents, correspondence, or similar) if available;
- how the information reached the reporting person and the reporting person's connection to the incident.

2.3 The content of the breach report is disclosed and used only for the purpose of identifying and taking follow-up measures regarding the work-related breach.

3 RIGHTS OF THE REPORTING PERSON

3.1 The identity of the reporting person and the information provided are kept confidential and the reporting person is protected as effectively as possible from any retaliation.

3.2 If the reporting person's identity needs to be disclosed to third parties (e.g., Police and Border Guard Board) for processing, this will only be done with the reporting person's written consent. If criminal or misdemeanor proceedings are initiated based on the breach report, confidentiality of the reporting is ensured according to the specific provisions of the relevant procedural law.

3.3 A non-anonymous reporting person has the right to receive confirmation of the receipt of the breach report and feedback on follow-up measures.

3.4 Mainor Group operates on the principle that the reporting person is acting in good faith until proven otherwise. This ensures that the reporting person's protection remains even if they mistakenly provide false information but did so in good faith. The right to reporting person protection remains on the condition that new information is provided to Mainor Group as soon as possible. Persons who do not act in the interests of Mainor Group and/or knowingly provide misleading, malicious, or false statements are not considered reporting persons under this procedure. If it is found that a Mainor Group employee has used retaliation or harassment measures against the reporting person, attempted to do so, or

threatened with retaliation, the incident will be investigated and necessary measures will be taken.

3.5 An employee responsible for retaliation is accountable for their actions according to the law. A reporting person who believes they have been subjected to retaliation or has a valid reason to believe they are threatened by retaliation must report this immediately.

4 PROCESSING OF REPORTS

4.1 The processors of breach reports received by Mainor Group are the talent manager of AS Mainor, the HR specialist of AS Mainor Ülemiste, the HR partner of Estonian Entrepreneurship University of Applied Sciences, and the deputy director of Tallinn International School OÜ, who are responsible for:

- informing employees and other related parties about the principles and guidelines provided in this procedure (including the rights of the reporting person);
- managing reporting channels and receiving and processing work-related breach reports;
- maintaining contact with the reporting person and providing feedback and requesting additional information if necessary;
- implementing appropriate follow-up measures to identify and eliminate work-related breaches;
- informing about the implementation of follow-up measures;
- forwarding the work-related breach report to the competent state authority if necessary.

4.2 In situations where the processor listed in point 4.1. cannot process the breach report according to the legal requirements (e.g. the report is made about them), they will recuse themselves from the process.

4.3 A non-anonymous reporting person will receive confirmation of the receipt of the work-related breach report within 7 (seven) days from the date of reporting.

4.4 If the processors of Mainor Group lack the competence to process the work-related breach report, they will forward the breach report to the competent authority immediately, but no later than the 5th (fifth) working day after receiving it. The non-anonymous reporting person will also be informed about the forwarding of the breach report.

4.5 Work-related breach reports are processed thoroughly. If necessary, additional explanations about the work-related breach will be requested from the reporting person or related persons.

4.6 Feedback on the implementation of follow-up measures will be provided to the non-anonymous reporting person as soon as possible, but no later than 3 (three) months (in the case of external reporting no later than 6 (six) months) after receiving the work-related breach report. The non-anonymous reporting person will also be provided with feedback on the final outcome of the breach process.

4.7 Feedback will not be provided if the breach report is anonymous or if the reporting person explicitly prohibited sending the acknowledgement or there is a reason to believe that this would jeopardise the confidentiality of the reporting person.

4.8 If the information provided in the work-related breach report raises suspicion that a legal breach has been committed or is planned to be committed, in addition to other legal measures, a crime report may be submitted to the prosecutor's office and the police.

4.9 For the interests of a possible or ongoing investigation, the reporting person may be required not to disclose information about the reporting, investigation, or progress of the breach.

5 OTHER

5.1 Breach reports are retained for 3 (three) years from the date of feedback. The retention of breach reports is carried out according to the regulation of the Government of the Republic.

5.2 Additional information and explanations about the procedure for reporting breaches and the rights of the reporting person can be obtained by emailing vihje@mainor.ee and contacting the processors listed in point 4.1.

5.3 Mainor Group ensures the protection and confidentiality of the reporting person according to the law.