WHISTLEBLOWING POLICY

METASWAP sp. z o.o.

June 2025
V1.

VERSION CONTROL

Version	Version Description	Author	Reviewer	Date Approved	Description
1.0	Creation of Policy & Procedure				Initial creation of document

1. INTRODUCTION

1.1. This Whistleblowing Policy (hereinafter referred to as the **"Policy"**) establishes that **METASWAP sp. z o.o.**, a company registered in the Republic of Poland (hereinafter referred to as the **"Company"**), registration code: 0001143298, address: ul. STANISŁAWA PRZYBYSZEWSKIEGO 91-99/15, 93-126, ŁÓDŹ, Poland, is committed to strengthening its integrity system and support protected whistleblowing activities. The Policy is designed in compliance with the Whistleblower Protection Act of 14 June 2024 (Journal of Laws, item 928) [1] (hereinafter referred to as the **"Act")**. The Company ensures the confidentiality, protection, and fair treatment of whistleblowers in compliance with the Act, which prohibits retaliation against whistleblowers and is committed to establish an internal whistleblowing system, ensuring that employees and stakeholders have secure and accessible channels for misconduct.

1.2. This Policy defines the rights and obligations of the Company's employees, board members, external stakeholders, and witnesses in relation to reporting violations and unethical conduct within the organization. The primary objective of reporting violations is to protect the public interest and prevent unlawful activities, including but not limited to, violations of financial regulations, taxation laws, and AML compliance; consumer rights infringements; breach of workplace safety and product quality standards; environmental violations; data protection breaches and cybersecurity threats; violations affecting public security and order.

1.3. In accordance with Act, reports regarding violations should pertain to the following areas, as outlined in Art. 3 (1) of the Act:

i) Corruption, bribery, and abuse of power
ii) Public procurement violations and unfair competition
iii) Financial services, products, and markets, including securities and investment fraud
iv) Anti-money laundering (AML) and countering the financing of terrorism (CFT)
v) Product safety, quality standards, and compliance with regulatory requirements
vi) Transport safety, including road, air, and maritime regulations
vii) Environmental protection, climate regulations, and sustainable development policies; viii) Radiological protection, nuclear safety, and hazardous materials management.
ix) Food and feed safety, including production, distribution, and labeling compliance.
x) Animal health, welfare, and ethical treatment.
xi) Public health, occupational safety, and healthcare system compliance; xii) Consumer protection, fair trade, and prevention of deceptive business practices; xiii) Protection of privacy, personal data, and cybersecurity regulations

[1] Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów, Dz.U. 2024 poz. 928. https://orka.sejm.gov.pl/opinie10.nsf/nazwa/317_u/$file/317_u.pdf

xii) Security of networks, ICT systems, and critical infrastructure

xiii) Protection of financial interests of the Czech Republic, local government units, and the European Union

xiv) Regulations governing the internal market of the European Union, including competition law, state aid, and corporate taxation

xv) Fundamental human rights and constitutional freedoms in interactions between individuals, businesses, and public authorities.

The Company treats all reports of potential misconduct with the utmost seriousness, ensuring strict confidentiality and compliance with the Act, which protects whistleblowers from retaliation. Reports that meet the legal criteria outlined in the Act will be reviewed and investigated in accordance with the established internal procedures and legal obligations.

2. DEFINITIONS

2.1. **COMPANY INTERNAL CHANNEL** - refers to a secure, designated reporting system within the Company that allows employees, external parties, and others associated with the Company to report potential violations. The system ensures confidentiality, protects the whistleblower's identity, and allows the Company to address the issue efficiently. It is key to maintaining integrity and ensuring prompt resolution of reported issues.

2.2. **COMPANY PERSONNEL** - refers to any individual employed by or contracted with the Company, including an employee, a person providing work on a basis other than an employment relationship, including on the basis of a civil law contract, also a job applicant, as well as contractors and third-party service providers.

2.3. **CONFIDENTIALITY** - ensures that a whistleblower's identity and the details of their report are protected from unauthorized access or disclosure. This is crucial for maintaining trust in the system and encourages reporting by safeguarding the whistleblower from retaliation. Confidentiality extends to all individuals mentioned in the report, including witnesses and affected parties

2.4. **CREDIBILITY** - refers to the reliability and trustworthiness of the information provided in a whistleblowing report. For a report to be considered valid, the whistleblower must provide verifiable facts supported by evidence.

2.5. **FALSE REPORT** - refers to a whistleblowing report made with the intention of misleading, deceiving, or fabricating claims of violations. False reports can harm the integrity of the process and may result in disciplinary actions against the reporter.

2.6. **GOOD FAITH** - means reporting violations with honest intent, aimed at protecting the public interest, rather than seeking personal gain or causing harm. Whistleblowers

reporting in good faith are protected under Company policies, even if their report turns out to be inaccurate, provided the intention was genuine.

2.7. **INVESTIGATION** - is the formal process undertaken by the Company to validate a reported violation, involving the collection of evidence, interviews, and assessment to determine the nature of the violation and necessary corrective actions.

2.8. **NON-RETALIATION POLICY** - ensures that individuals who report violations will not face retaliation in any form, such as dismissal, harassment, or discrimination. Retaliation is strictly prohibited and may result in disciplinary action.

2.9. **RZECZNIK PRAW OBYWATELSKICH (OMBUDSMAN)** - the Ombudsman in Poland plays a crucial role in the external reporting mechanism for whistleblowers. According to the law, a whistleblower may submit an external report to the Ombudsman without first submitting an internal report. The Ombudsman is responsible for receiving external reports of legal violations, conducting an initial verification, and forwarding them to the appropriate public authority for further action. The Ombudsman serves as an independent authority and ensures the protection of the whistleblower's rights by maintaining confidentiality, safeguarding against retaliation, and providing advice regarding legal protections. The Ombudsman also has the responsibility of informing the public and whistleblowers about their rights and the protective measures available to them.Under Article 30 and Article 31 of the Act, the Ombudsman handles external reports in specific fields and provides access to information about legal protections against retaliatory actions

2.10. **RELATED PERSONS** - individuals who are directly or indirectly connected to a reported violation, including family members, colleagues, or business partners. Their actions may be relevant to the investigation.

2.11. **REPORTING** - is the act of submitting information regarding a violation through the Company's designated internal channels. Reports include descriptions of the violation, involved parties, evidence, and possible consequences.

2.12. **RETALIATION** - refers to negative actions taken against someone for reporting violations or assisting in an investigation. This includes firing, demotion, or creating a hostile work environment. Retaliation is prohibited and may lead to disciplinary action.

2.13. **VIOLATION** - refers to any criminal act, administrative offense, misconduct, or breach of duties within the Company, including serious ethical violations, cover-ups, or illegal acts threatening public interest.

2.14. **WHISTLEBLOWER** - an individual who reports violations of laws, regulations, or Company policies, often based on information acquired through employment or contractual relationships with the Company.

2.15. **WHISTLEBLOWER MANAGER (or COMPLIANCE OFFICER)** - the designated person responsible for handling and responding to whistleblowing reports, ensuring compliance with legal and internal policies, and protecting the whistleblower throughout the process.

2.16. **WHISTLEBLOWING PROCEDURE** - is a formal and structured process developed by our company, to facilitate the reporting of misconduct, violations, or unethical behavior by employees, contractors, or other stakeholders. This procedure is a

critical part of our commitment to transparency, accountability, and compliance with relevant laws and regulations. It is designed to ensure that individuals feel safe and supported in raising concerns, without fear of retaliation.

2.17. **WITNESS** - individuals who have direct knowledge of or have observed the violation. Their testimonies can provide crucial evidence during an investigation.

2.18. **VERIFIABILITY** - the ability to substantiate the accuracy of a whistleblower's report through available evidence such as documents, emails, or records.

2.19. **ANONYMITY** - the option for whistleblowers to report violations without revealing their identity, ensuring protection from potential retaliation.

2.20. **WHISTLEBLOWER PROTECTION**- encompasses legal safeguards and internal policies designed to protect individuals from retaliation or harm for reporting violations.

2.21. **WRONGDOING**- refers to any act of misconduct, illegal activity, or violation of Company policies, laws, or ethical standards that could harm the Company or its stakeholders, whether it is an act already committed, or one being planned.

3. LEGAL BASIS AND APPLICABILITY

3.1. The Whistle-blower Protection Directive (EU) 2019/1937[2], adopted by the European Parliament and Council, establishes common standards for safeguarding individuals who report breaches of EU law. Its primary goal is to strengthen whistle-blower protection throughout the European Union, promote transparency and integrity within both the public and private sectors, and prevent retaliation against those who report irregularities. The directive covers a broad spectrum of violations, including those related to product safety, environmental protection, public health, consumer rights, and personal data.

3.2. Poland has incorporated the requirements of Directive (EU) 2019/1937 into its national legal system through the *Act of 14 June 2024 on the Protection of Whistleblowers* (Journal of Laws 2024, item 928), adopted by the Parliament of the Republic of Poland. This Act ensures that whistleblower protections are fully aligned with EU standards, providing legal safeguards against retaliation and ensuring that reports of violations are handled with confidentiality and due diligence.

3.3. This Policy is based on the provisions outlined in the Act, which aims to establish a comprehensive framework for the protection of individuals who report breaches of the law, ethical misconduct, or other violations in the workplace and beyond. This legal framework ensures that whistleblowers are protected from retaliation and that their disclosures are handled with confidentiality and due diligence. The Act allows whistleblowers to submit external reports without the obligation to first submit an internal report. This ensures that individuals can bypass internal channels when they perceive such channels to be ineffective or unsafe.

[2] European Parliament & Council of the European Union. (2019). Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. *Official Journal of the European Union.* Retrieved from https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937

3.4. The processing of personal data related to whistleblowing reports must comply with the provisions of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)[3] and the Act, ensuring that all personal data is handled securely, lawfully, and responsibly. Personal data of whistleblowers and any individuals involved in reports must be protected from unauthorized access, disclosure, or misuse.

3.5. Whistleblowers have the right to submit external reports directly to the competent authorities without first reporting internally. The Ombudsman is responsible for receiving and processing external reports, providing guidance on whistleblower rights and protections, ensuring compliance with whistleblower protection regulations, preventing retaliation against whistleblowers.

3.6. This policy applies to all individuals within the organization, including employees, contractors, suppliers, and any other third parties who interact with the organization and may have witnessed or become aware of any violations, misconduct, or legal breaches.

i) Internal Reporting Mechanisms – Whistleblowers are encouraged to use internal reporting channels first, unless they have reasonable grounds to believe that such channels would not lead to an effective resolution.

The internal reporting mechanism should comply with the requirements of the Act.

ii) External Reporting Mechanisms – whistleblowers have the right to submit reports directly to the Ombudsmen or other relevant public authorities without the obligation to report internally. The external reporting mechanisms are intended to offer an alternative when internal reporting may not be viable or when the whistleblower fears retaliation. iii) Public Sector and Private Sector Applicability – the protections and procedures outlined in the Act apply to both the public and private sectors, ensuring uniform standards of protection for whistleblowers across various industries and organizational structures. iv) Non-Retaliation – this Policy applies to ensure the protection of whistleblowers from any form of retaliation, including but not limited to discrimination, harassment, negative employment consequences, such as reduced benefits or denial of promotions, legal threats or unjustified legal action.

The Company ensures strict enforcement of non-retaliation measures, providing whistleblowers with legal protection, confidentiality, and access to legal remedies if retaliation occurs.

4. MANAGEMENT OF REPORTS AND REPORTING CHANNELS

4.1. Internal Reporting Channels

[3] European Parliament & Council of the European Union. (2016). 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 (General Data Protection Regulation, GDPR). *Official Journal of the European Union*. Retrieved from https://eurlex.europa.eu/eli/reg/2016/679/oj/eng

Employees, contractors, and other relevant stakeholders can report any concerns, suspicions, or allegations of wrongdoing through the internal reporting channels provided by the company. These channels include:

Reports can be submitted via a specific email address dmitrii.mand@macpay.io

i) designated solely for whistleblowing purposes. The Compliance Officer will review and act upon the submissions.
ii) An online form available on the company's intranet, enabling the submission of detailed concerns in a secure and confidential manner.
iii) Employees may report concerns directly to their immediate supervisor or manager, who will ensure the proper escalation of the issue to the relevant department.

All reports will be acknowledged within 7 days, assessed within 30 days (extendable to 90 days in complex cases), and handled with strict confidentiality and protection against retaliation.

4.2. **External Reporting Procedure**

Whistleblowers have the option to submit a report externally, either independently or after using internal channels. External reports may be directed to the Ombudsmen or any relevant public authority as per applicable law. The decision to report externally does not require prior submission of an internal report.

The Ombudsmen or the public authority handling the external report is independently responsible for managing the personal data contained in the report. These authorities will act in compliance with legal provisions concerning data protection and following of the relevant law.

Whistleblowers can submit external reports through various official channels. Submission Methods:
i) Written Requests: The complainant may submit the report in writing through various means: ii) By post, addressed to the Ombudsmen or public authority at the designated correspondence address. iii) Electronically, by sending an email to the designated email address or using an electronic service provided by the Ombudsmen or public authority for receiving reports.
iv) Through an online form or application approved by the competent public authority for electronic submissions.
v) Oral Reports: Whistleblowers can also submit their reports orally, either in person or by phone, as specified by the Ombudsmen or public authority.
Upon receiving an external report, the Ombudsmen or public authority will acknowledge receipt of the report within 7 days. If the complainant has requested otherwise or if confirming receipt could jeopardize the confidentiality of the complainant’s identity, no acknowledgment will be issued.

The Ombudsmen or public authority may request clarification or additional information from the whistleblower at the contact address provided, should further details be required. If such

a request could compromise the protection of the whistleblower's identity, no such request will be made.
The Ombudsmen or public authority will, without undue delay, forward the information contained in the external report to the relevant European Union institutions, bodies, offices, or agencies for further action, as required by law.

4.3. The Company guarantees the protection of the whistleblower's identity, ensuring confidentiality and, where possible, anonymity throughout the process. Reports will only be disclosed to authorized personnel who are involved in investigating the matter, and any information provided will be handled with the utmost care to protect the whistleblower from retaliation.

4.4. The Company ensures that no retaliatory actions will be taken against individuals who report concerns in good faith through the established reporting channels. Any acts of retaliation will be treated as serious violations of the Company's policies and will be investigated promptly. Employees who experience retaliation have the right to seek legal protection under the Act.

4.5. Whistleblowers can seek guidance from the Compliance Department on how to report a concern or obtain further clarification on the process. In addition, support services, including legal and psychological assistance, will be provided where necessary to ensure the well-being of the whistleblower during the reporting process. The Company is committed to fostering a transparent, ethical, and secure environment where individuals can report violations without fear of retaliation.

5. VERIFICATION PROCESS

5.1. Upon receiving a whistleblower report, the Compliance Officer is responsible for logging the report in a secure, confidential register. The report will then be reviewed for initial verification to determine if it contains sufficient information regarding a potential violation. If the report is clear and actionable, it will proceed for further processing. If additional information is needed, the report will be flagged for further review. Unauthorized disclosure of a whistleblower's identity or report details is prohibited and subject to penalties under the legislation.

5.2. The Company accepts anonymous reports, provided they meet the criteria for handling as outlined in this procedure. Anonymous reports will be processed with the same care and attention as non-anonymous reports, ensuring the confidentiality of the whistleblower is maintained. If a report is deemed insufficient for further investigation, the whistleblower's anonymity will remain protected during the decision-making process.

5.3. The report will be analyzed to determine whether it is credible and falls within the scope of the Company policies and relevant laws. The Compliance Officer will assess

the validity of the report, gather additional facts if necessary, and decide whether an investigation is warranted. If the report is verified as valid, it will proceed to the next stage of investigation. If not, the whistleblower will be informed of the decision (if possible), and the report will be archived.

5.4. If the report passes the initial verification, an internal investigation will be initiated by the designated team or department. The investigation will follow the Company's standard procedures, ensuring fairness, impartiality, and confidentiality for all parties involved, including the whistleblower and the reported person. The investigative team will gather evidence, interview witnesses, and review relevant documentation to confirm or refute the allegations made in the report. Based on the findings, corrective actions or other necessary measures will be implemented. The investigation will be completed within a reasonable timeframe, and all parties involved will be kept informed of its progress.

5.5. The whistleblower will be informed about the acceptance of their report and the initiation of an investigation (if applicable). Throughout the investigation, the whistleblower will receive periodic updates on the status, provided that confidentiality and legal requirements permit. Once the investigation is concluded, the whistleblower will be informed of the final outcome, including any actions taken or decisions made based on the findings.

5.6. All actions taken throughout the process will prioritize the protection of the whistleblower's identity and ensure that retaliation is prevented in accordance with the Act. If retaliation or discrimination against the whistleblower is reported, the Company will take immediate corrective action to address the issue. Violations of whistleblower protection provisions will be considered serious misconduct and may result in disciplinary or legal consequences for the responsible parties.

6. PROCEDURE FOR HANDLING INFORMATION ON VIOLATIONS REPORTED ANONYMOUSLY

6.1. The Company recognizes the importance of allowing whistleblowers to submit reports anonymously to encourage the reporting of violations without fear of retaliation. Anonymous reports will be accepted and processed with the same level of diligence and confidentiality as non-anonymous reports, provided they contain sufficient detail for investigation.

6.2. The company ensures that any anonymous report of a violation will be accepted and registered for further investigation. Th Compliance Officer will review each anonymous report to determine if it contains enough details (e.g. Specific incidents, involved parties, supporting evidence) to proceed with an investigation.

6.3. In cases where an anonymous report is accepted, the investigation will proceed without revealing the identity of the whistleblower. If additional information is needed, the Company may attempt to gather further details without compromising the

anonymity of the reporter. Should the anonymity be at risk, no further clarification will be sought.

6.4. Due to the anonymous nature of the report, providing feedback to the whistleblower is not always possible. However, the company will ensure that the investigation is conducted thoroughly, and any actions taken will be documented internally.

6.5. The company guarantees that the anonymity of the whistleblower will be protected throughout the investigation process. All reports, including anonymous ones, will be handled with the utmost care to prevent any potential retaliation or breaches of confidentiality.

7. STORAGE OF INFORMATION

7.1. The Company is committed to ensuring the protection of whistleblowers' personal data, including their identity, throughout the entire reporting and investigation process. All personal data submitted by whistleblowers, whether through internal or external channels, will be handled with the utmost care and in compliance with applicable data protection laws and the Company's policies.

7.2. Personal data, including any information that could potentially identify the whistleblower, is subject to strict confidentiality and will only be accessible to those involved in the management of the report, in accordance with the Company's internal procedures. This includes the Report Manager, Compliance Officer, investigative teams, and other relevant personnel, all of whom are bound by confidentiality obligations.

7.3. In cases where the disclosure of the whistleblower's identity is legally required in the context of proceedings conducted by public authorities, the Company will inform the whistleblower about this requirement and explain the reasons for such disclosure. This will only occur if such a legal obligation exists, and the Company will ensure transparency in the process.

7.4. Personal data collected in connection with the acceptance of a whistleblower report will be retained for a period of up to three years after the completion of the follow-up actions, or one year from the conclusion of the investigation or corrective measures. The retention period ensures that any necessary records are available for audit or review, while respecting the whistleblower's right to privacy.

7.5. The Company guarantees that all measures are taken to ensure the security of stored personal data, with access granted only to authorized individuals who require it for legitimate purposes. Any data retention or processing will be in line with the company's data protection policy and applicable legislation on personal data protection.

8. ARCHIVING OF REPORTS

8.1. The Company is committed to maintaining an internal register of all whistleblower reports, ensuring proper administration of the data contained within the register in compliance with our policies and applicable legal requirements. This register will be securely stored and managed, with access granted only to authorized personnel involved in the handling and processing of reports.

8.2. The internal register will include the following essential details for each whistleblower report:

i) A unique reference number for the report.

ii) A brief description of the alleged breach or issue.

iii) The personal and contact details of the whistleblower (if provided).

iv) The date the report was received.

v) Information regarding any follow-up actions taken during the investigation process.

vi) The date on which the report was closed, including the outcome of any actions taken.

8.3. The Company recognizes the importance of maintaining transparency in the whistleblowing process. As such, all records will be kept in accordance with the data retention policy, which ensures that the information is securely stored for the required period. The mandatory retention period for the whistleblower report records is three years, starting from one year after the completion of follow-up actions or closure of the investigation.

8.4. During this retention period, all records will be easily accessible for audit, review, or further legal purposes if required. After the retention period has elapsed, all records will be securely archived or destroyed in accordance with the Company's data protection policy, ensuring that personal data is handled with care and in compliance with relevant privacy regulations.

8.5. This archiving process allows the Company to maintain a comprehensive and secure record of all whistleblower reports, ensures compliance with legal and regulatory obligations, and protects the confidentiality of the whistleblower and all parties involved in the process. The Company is committed to upholding the highest standards of transparency and security while safeguarding the privacy of all individuals involved in the whistleblowing procedure.

9. MAXIMUM PERIOD FOR FEEDBACK TO THE COMPLAINANT

9.1. The Company is committed to providing timely responses to internal complaints in accordance with legal requirements and best practices. The following procedure outlines the maximum period for providing feedback to the complainant:

9.2. Upon receiving an internal complaint, the company is required to acknowledge receipt of the complaint within 7 days. The acknowledgment will confirm the receipt of the complaint and provide an overview of the next steps in the process.

9.3. The maximum period for providing feedback to the complainant regarding the outcome of the internal complaint is 3 months. This period starts from the date of acknowledgment of receipt of the internal complaint.

9.4. If the acknowledgment is not sent to the complainant within 7 days (due to a lack of provided contact information), the 3-month period for feedback will begin after 7 days have elapsed from the date of the internal complaint.

9.5. In cases where the complainant has not provided the necessary contact details (postal address or email address), the company will make reasonable efforts to contact the complainant. However, feedback may be delayed if no contact information is available, and it will not be considered the Company's responsibility if the complainant does not provide such details.

9.6. The Company will make every effort to ensure that feedback is provided within the 3-month period. In cases where additional time is required, the complainant will be informed promptly and provided with an explanation for the delay.

10. WHISTLEBLOWING AND LIABILITY

10.1. The Company is committed to providing protection for whistleblowers who report misconduct or violations in good faith. In line with the Company's internal policies and relevant legal frameworks, whistleblowers are protected from retaliation and should they face any adverse actions as a result of their report, they are entitled to appropriate compensation.

10.2. If a whistleblower faces retaliatory actions—such as demotion, harassment, discrimination, or termination of employment—due to their report, they are entitled to compensation. The amount of compensation will be no less than the average monthly remuneration in the national economy for the previous year. This ensures that whistleblowers are protected and not penalized for their decision to report violations in the workplace. Compensation claims may be submitted through relevant authorities, including the Ministry of Justice.

10.3. While the Company encourages the reporting of any potential violations or misconduct, it is also essential that whistleblowers ensure the accuracy of the information they provide. In cases where a whistleblower intentionally submits false or misleading reports, or makes false public disclosures, the person who has suffered harm due to the false report or disclosure is entitled to compensation for the damage done to their personal rights. This compensation may be sought directly from the whistleblower responsible for making the false report.

10.4. In the event that a whistleblower claims retaliation, it is presumed that any action taken by the Company, such as disciplinary measures or adverse changes to their work conditions, may constitute retaliation. The burden of proof then shifts to the

Company. The Company must demonstrate that the action was taken for objective and justifiable reasons, unrelated to the whistleblower's report.

10.5. The Company is committed to ensuring that all whistleblowers can report in good faith without fear of retaliation. Any retaliation is not tolerated and will be met with corrective action. At the same time, the Company acknowledges the potential risks involved in false reporting and emphasize that malicious, false reports may result in legal and financial consequences for the whistleblower.

10.6. The Company ensures that any claims of retaliation or false reporting will be thoroughly investigated with the highest level of impartiality, and the Company will uphold both the rights of the whistleblower and those potentially affected by the report.

By implementing these measures, the Company guarantees a transparent, legally compliant, and fair whistleblowing framework, ensuring protection for whistleblowers while preventing abuse of the system.

11. CONFIDENTIALITY

11.1. The Company is committed to maintaining the highest level of confidentiality in the whistleblowing process, in accordance with the Act. This includes safeguarding the personal data and identities of the whistleblower, the affected person, and any third parties mentioned in the report. We take necessary measures to prevent unauthorized access to any sensitive information related to the whistleblowing procedure.

11.2. Only individuals specifically authorized by the Company, in writing, are permitted to receive, verify, monitor, or process internal reports. These authorized personnel are entrusted with handling sensitive data and are required to maintain strict confidentiality regarding the information and personal data obtained during the whistleblowing process. This duty of confidentiality extends even beyond the termination of their employment or legal relationship with the Company.

11.3. All personal data and information related to a report, including the identity of the whistleblower, the affected party, and any third parties, shall be securely stored and only accessible to authorized individuals. This data will be retained for the minimum period required by law and as specified in the Company's internal procedures.

11.4. To ensure that unauthorized individuals do not have access to whistleblowing information, the Company has implemented various security measures, including encrypted communication channels and restricted access to digital and physical records. Any breach of confidentiality will be investigated promptly, and appropriate measures will be taken to prevent future occurrences.

11.5. The Company commits to protecting the identity of the whistleblower throughout the investigation process. The information contained within the report will only be disclosed to other parties if required by law, such as for criminal investigations, or

where explicit consent has been given by the whistleblower. In such cases, the whistleblower will be informed and provided with a clear explanation regarding the disclosure of their identity.

11.6. The authorized personnel who handle whistleblowing reports are obliged to maintain confidentiality regarding the information and personal data obtained in the course of the reporting process. They must refrain from disclosing any sensitive information unless legally mandated or when disclosure is essential for the purposes of the investigation. This confidentiality obligation continues even after the termination of the employee's or authorized individual's relationship with the company.

11.7. All employees involved in receiving, processing, or investigating reports are required to undergo regular training on the importance of confidentiality and data protection. This training includes a clear understanding of the legal requirements surrounding whistleblowing and the responsibilities of those involved in the process to protect sensitive information. Employees are also reminded of the serious legal and ethical consequences of breaching confidentiality.

11.8. The Company ensures that the whistleblower's identity is protected throughout the process to prevent retaliation or harm. If retaliation or discrimination against the whistleblower is reported, the Company will take immediate corrective action. The whistleblower is provided with reassurance that their identity will be kept confidential and that their protection is a priority.

11.9. By implementing these confidentiality measures, the Company demonstrates its commitment to creating a safe environment for whistleblowers, ensuring that their concerns are addressed while protecting the privacy and rights of all parties involved.

12. POLICY UPDATES AND REVISIONS

12.1. The Director of the Company approves this Policy, and the Compliance Officer oversees its updates. The Compliance Officer is also responsible for ensuring that the Policy is communicated to all Company's executives and employees, external stakeholders, contractors, and third parties, provides updates to reflect changes in legislation or best practices, oversees the implementation of this Policy, and ensures compliance with applicable whistleblower protection laws. The Policy will be made available on the Company's website for easy access. Should there be any questions or concerns about compliance with this Policy, employees are encouraged to reach out to the Compliance Officer for further assistance and clarification.

END OF POLICY