WEB3 Technology B.V.

POLICY DOCUMENT

Whistleblowing Policy

Trading as “RGLTD.com” | Netherlands-Licensed CASP | AFM Authorisation No. 41000022

Regulatory Framework

DORA (EU) 2022/2554 · MiCA (EU) 2023/1114 · GDPR (EU) 2016/679

Document Control

Field	Detail
Document Title	Whistleblowing Policy
Document Owner	Chief Risk and Compliance Officer
Applies To	All employees (all the Company’s directors, officers, agents, staff, temporary workers, interns, consultants, contractors, or any other person who works for the Company regardless of contract type or duration) and third parties; all locations, roles and seniority levels
Regulatory Basis	DORA Regulation (EU) 2022/2554 and its associated Regulatory Technical Standards (RTS) on ICT Risk Management Framework; NIS 2 Directive (EU) 2022/2555; GDPR (EU) 2016/679
Version	v.26_9.0
Effective Date	27.10.2026
Review Cycle	Annual, or sooner upon significant changes to the organisation, legal and regulatory requirements
Approved By	Board of Directors
Classification	Internal
Company	“Company” means WEB3 Technology B.V., a private limited company (besloten vennootschap) incorporated under Dutch law, registered office at Prins Hendrikkade 21E, 1012 TL Amsterdam, the Netherlands, Chamber of Commerce (KvK) number 95206604, authorised as a crypto-asset service provider by the AFM under authorisation No. 41000022.

Table of contents

Document Control....1
Table of contents....2
1. Introduction....3
1.1 What is the purpose of this policy?....3
1.2 Why do we need this policy?....3
1.3 What is the scope of this policy?....4
1.4 Definitions....4
1.5 Roles and responsibilities....5
2. Policy Principles and Rules....5
2.1 When to report?....5
2.2 What to report?....5
2.3 Key principles....8
3. Filing a Whistleblowing Report....10
3.1 Reporting channels for employees....10
3.2 Procedures for Handling Reports....10
3.3 Considerations Relative To Whether the Compliance Officer or Board of Directors Should Investigate a Report....11
4. The Investigation Process....13
4.1 Conditions in assessing and weighing information....13
5. Retention Periods....14
6. Feedback....14
7. Privacy Rights....15
8. External Reporting....15
9. Mandatory trainings....16
10. Document control....17
10.1 Approval, review and deviations....17
10.2. Version history....18
Schedule 1 - Report....19

1. Introduction

1.1 What is the purpose of this policy?

This policy states the Company's framework on whistleblowing as a channel of last resort to report issues that (potentially) affect the integrity of the organisation and the reputation of the Company and any of its related parties (hereinafter jointly referred to as 'the Company'). The policy fits in the core values of the Company and the company's wider integrity structure. Irregularities negatively affect the integrity of the Company and could have serious consequences for individuals or society. It is important for the Company to be aware of any (potential or suspected) abuses and irregularities in order to address, mitigate and prevent them. The whistleblowing channels of the Company are open to all employees as well as third parties. The policy provides clear insight about the Company's key principles on whistleblowing, the various reporting channels, the investigation process and the different roles and responsibilities within that process.

1.2 Why do we need this policy?

It is important for the Company to have clear procedures and policies in place regarding whistleblowing for several reasons.

For employees it is important to know that the Company provides a channel where they can disclose information about suspected Irregularities which they feel unable to address within the regular reporting structure or other **Speak Up** channels.

The Company recognises that certain barriers exist in speaking up, especially when loyalty is at play or if you are afraid of personal or professional consequences. It is therefore important to know that employees who report irregularities in good faith are protected by the whistleblower status and our non-retaliation principle. Reports may be filed anonymously, though it is important to note that the identity of the reporting person is kept confidential for all reports (see paragraph 2.3).

This policy is very important for the Company as an organisation as well. The integrity and reputation of the Company are of utmost importance for the company, unreported Irregularities may jeopardise this. The Company and its employees are under a statutory and/or regulatory obligation in many jurisdictions to report particular types of Irregularities, such as financial crime and other criminal offences, to the regulatory or government authorities.

A consistent and effective mechanism must be in place to facilitate such reporting. The Company encourages employees and third parties to report any Irregularities, even when the rules or regulations do not require them to do so. Having a culture in place which promotes employees to speak up will ensure that disclosures pertaining to possible Irregularities are properly investigated and relevant information reaches senior management in good time when necessary. Early detection allows the Company to address (potential or suspected) Irregularities

before a situation escalates. Gathering information on the issues raised through the whistleblowing channel allows the organisation to detect patterns and make improvements to our policies, procedures and address conduct issues in order to prevent future problems. It also allows management to identify where more resources are needed to reduce risk exposure.

The policy gives effect to the latest regulations and legislation on whistleblowing and aims to adopt best practices in the field of whistleblowing protection and internal alert handling. In preparation for this policy, we have ensured compliance with the Dutch Whistleblower Protection Act (in Dutch: *Wet bescherming klokkenluiders, Wbk*)

1.3 What is the scope of this policy?

This policy applies to everyone working for or on behalf of any of the legal entities within the Company group. The policy also applies to all employees (all the Company's directors, officers, agents, staff, temporary workers, interns, consultants, contractors or any other person who is employed by the Company or otherwise works for the Company, regardless of the duration of their employment contract or other type of relationship) and third parties. This policy applies everywhere, for all locations, roles and seniority levels.

1.4 Definitions

Capitalised terms and expressions used in this policy shall have the meaning given to them in the below list of definitions:

Irregularities means (1) a (risk of) Breach of Union law, or (2) an act or omission involving the public interest (*maatschappelijk belang*) in respect of: (i) a breach or risk of breach of a statutory regulation or internal policies containing a concrete obligation and established by the Company pursuant to a statutory regulation; or (ii) a danger to public health, to the safety of persons, to the impairment of the environment or to the proper functioning of the public service or an enterprise as a result of improper conduct or failure to act. The public interest is in any case at stake if the act or omission does not only affect personal interests and there is either a pattern or structural character or the act or omission is serious or extensive.

Breach of Union law means the act or omission which: (1) is unlawful and relates to Union acts and policies falling within the material scope referred to in Article 2 of the Directive; or (2) undermines the purpose or application of the rules in the Union acts and policy areas falling within the material scope referred to in Article 2 of the Directive.
Directive means 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, when reporting a Breach of Union law, as amended from time to time.

1.5 Roles and responsibilities

This section sets forth the roles and responsibilities of relevant parties as the roles apply to this policy.

Role:	Responsibility:
Compliance Officer	1. Annual review, opinion and management of procedure review. 2. Maintaining an up-to-date description of the actions, procedures and stages under this whistleblowing policy.
Board of Directors	3. Approve procedure and annual reviews.

2. Policy Principles and Rules

2.1 When to report?

The whistleblowing channel of the company is open to all employees to report Irregularities which they cannot, or do not feel comfortable to, report to their manager or compliance officer. The whistleblowing channel complements the normal reporting channels and **Speak Up** channels. The whistleblowing channel is also open to third parties to report Irregularities concerning the Company or its employees. Potential and suspected Irregularities can be reported under all circumstances. It is important to note however that there are several conditions which impair the likeliness that the report can be investigated. Paragraph 4.1 lists examples of conditions which can be used in assessing and weighing information provided in whistleblowing reports and the decision to start an investigation into the matter.

You should be fully aware that you have full discretion and permission to engage an advisor on a confidential basis about the suspected Irregularity.

2.2 What to report?

This policy is designed to allow employees and third parties to report its suspicion that there are Irregularities within the Company (or at another organisation if he or she has come into contact with this organisation in the performance of their work), insofar as the suspicion is based on reasonable grounds arising from his or her knowledge at the Company or the knowledge acquired through his or her work at another company or organisation.

This reporting procedure is not meant for reporting individual problems between the reporter and (other individuals working at) the Company.

Irregularities amongst others includes:

2.3.1 Dishonest, fraudulent, inappropriate, illegal or negligent professional activity or behaviour by another person;

2.3.2 Failure by another person to act appropriately, with propriety or in accordance with the law when carrying out their duties.

2.3.3 Internal breaches of the Wwft, including (but not limited to) failures in customer due diligence, transaction monitoring, or reporting of unusual transactions.

Examples of Irregularities include (but are not limited to):

Money Laundering/ Terrorism Financing concerns/ Sanctions violations
Transfer of illegally generated money or assets into the legal financial and commercial cycle. Examples: Transfer of money via a „tax haven“; desire of a business partner to complete a transaction in whole or in part in cash; evidence of proximity of the business partner to criminal or terrorist organisations; doubts about a customer’s identity or suspicions that a customer is acting as a straw man for others.
Corruption/ Bribery/ Breach of Trust
Offering or accepting inappropriate advantages of any kind in a business context; claiming or accepting of inappropriate advantages by using one’s own official position. Examples: Offering or accepting of commissions or money gifts; invitation from or through business partners which seemingly serves to influence a business relationship. Breach of Trust: Abuse of authority over third-party assets or violation of the duty to safeguard asset interests of third parties.
Fraud/ Embezzlement/ Theft
Offences against property to the detriment of the company or a third party. - Fraud & Embezzlement - False pretences or suppression of the truth in order to obtain an illegal financial advantage for oneself or a third party. - Examples: Issuing of excessive bills to keep the surplus; credit fraud; subsidy fraud;

- insurance fraud; forging of identification documents, keys, transponders or other means of identification; manipulation of machines or test methods.
- Bypassing of directives for granting of credit; withholding of company funds or of insolvency money.
- Theft
- Unauthorised removal of foreign objects or money for personal use or to send them to a third party.
- Examples: Theft of goods from the warehouse; withholding of company funds or work materials.

Bullying, harassment, discrimination and victimisation

Behaviours of employees or leaders, as well as company guidelines that are perceived as acts of bullying, harassment, discriminatory or victimising. Any acts that can be seen as offensive, intimidating, malicious, insulting or victimising. Excluding or treating somebody less favourably because they've complained about bullying, harassment or discrimination.

Violation of Data Protection/ Data Privacy/ Data Security Provisions

Violations of provisions for the protection of personal data; serious breaches of secrecy of telecommunication; violation of policies aiming to protect data against falsification, destruction and unauthorized disclosure.

Health, Safety, Security and Wellbeing

Violations or unsafe acts in the physical working environment, posing a threat to physical safety and wellbeing. Alarming damages or faults with equipment and office facilities or practices that could be considered damaging to mental or psychological health.

Examples: Unsafe working conditions and environment, violations on global health and safety practices, psychological and physical wellbeing.

In order to report an Irregularity via the Company whistleblowing channel:

- the Irregularity should be directly related to the Company or any of its related parties;
- information provided should be as accurate and complete as possible;
- demonstrating evidence of the Irregularity is preferred but not necessary, reporting persons should nevertheless have reasonable grounds to suspect the Irregularity has taken place (or will take place).

It is important to note that the information included in the whistleblowing report can be an important factor in determining to launch an investigation.

2.3 Key principles

The Whistleblowing Policy of the Company is structured around five key principles:

1. protection of confidentiality;
2. non-retaliation;
3. anonymous reporting & confidential reporting;
4. reporting in good faith; and
5. protection of accused persons.

These five principles are laid down below in more detail.

Protection of confidentiality

The principle of confidentiality is a cornerstone of the Whistleblowing Policy. The recipient of the whistleblowing report and all others involved in the whistleblowing process treat the information confidentially and with utmost care. The data is saved digitally and physically only accessible to the officers directly involved in the reporting and investigation process on a 'need to know' basis.

The identity of the reporting person and other details of the report are treated confidentially and are protected through all stages of the investigation process. The identity of the reporting person who has filed a whistleblowing report is not revealed without first obtaining the person's explicit consent, unless its disclosure is required by a court order in the context of subsequent judicial proceedings.

Non-retaliation

This protection against retaliation also extends to:

- Facilitators who assist a reporting person in the reporting process in a work-related context;
- Any persons who are connected with the reporting person such as colleagues or relatives of the reporting person and who could suffer retaliation in a work-related context, on the part of their employer, their client or the beneficiary of their services; and
- Legal entities that the reporting person controls, works for or is otherwise connected with in a work-related context (e.g., personal service companies, suppliers, distributors etc.)

The reporting person who has made a valid report is protected against detriment. Detriment occurs if the Company treats you worse by making a report than if you had not made a report. Examples of detriment include dismissal, involuntary transfer, refusal of a promotion, a negative assessment or a written reprimand. In addition, the Company must ensure that your manager and colleagues do not disadvantage you, for example by bullying, ignoring or intimidating you.

Anonymous reporting or Confidential reporting

Following the Company's strong commitment to protect the identity of those who made reports in good faith and the Company's non-retaliation principle, as described above, a strong framework is in place to protect employees who file a report under this policy. As anonymous reporting can seriously hinder the possibility to investigate the claim, the Company encourages reporting persons to disclose their identity via a confidential report when reporting a concern or to at least provide contact details to facilitate any follow-up. Anonymous reporting is nevertheless a possibility under the Company Whistleblowing Policy as the Company would rather receive anonymous reports than not having the concern reported at all.

While the Company does provide the possibility to raise concerns anonymously there are some drawbacks. The ability to investigate, ask follow up questions or to provide feedback will be reduced if the individual cannot be contacted. It will also be more difficult to ensure the individual is protected if their identity is not known.

Reporting in good faith

This policy protects whistleblowers who report in good faith. A report is considered to be made in good faith if the individual had reasonable grounds to believe the information was true at the time of the reporting. If it later turns out the information was not true but the report was made in good faith, the whistleblower is still protected from retaliation. Those who deliberately and knowingly report wrong or misleading information do not enjoy protection, which serves as a safeguard against malicious or abusive reports. Making malicious or false claims is incompatible with the Company's core values and deliberate misuse of the Company whistleblowing channel may result in disciplinary action.

Protection of accused persons

The protection of the employee is of utmost importance to the company. In case a natural person is allegedly responsible for the Irregularity, their employment rights and right to privacy will need to be carefully considered. The person who is the subject of an investigation will be informed about the cause of the investigation if appropriate given the circumstances. When the investigation finds no evidence that justifies taking measures against the person who has been reported, that person should be protected from any negative effects. The same protection should apply for persons who are subjected to reports made in bad faith. If evidence is found and measures are taken, the person concerned should be protected from unintended negative effects that go beyond the objective of the measure taken.

3. Filing a Whistleblowing Report

A whistleblowing report can be filed via the designated whistleblowing channel or via alternative channels described below. The reporting mechanism and subsequent investigative procedures ensure the protection of the personal data of both the person who reports the Irregularity and if relevant the natural person who is allegedly responsible for the Irregularity.

3.1 Reporting channels for employees

The Compliance Officer is responsible for the intake, registration, assessment and subsequent investigation of reported Irregularities under this policy.

Employees can report any Irregularities under this policy through the internal whistleblowing channel “RGLTD Whistleblower Reporting Link” in the ClickUp Channel. This item holds the link to the reporting tool and the current policy. For employees currently employed by the Company, this channel is active and in use.

Employees are under no obligation to use the contact form to raise their concerns regarding alleged Irregularities, but using this designated whistleblowing channel guarantees that the report is submitted directly and without delay for assessing the reported Irregularity. Alternatively, if, for any reason, an employee should feel uncomfortable using this route, they can file a report with their manager, their manager’s manager, the HR business partner, the compliance officer, a trusted person, or a representative of the employee's choice, the senior management. Concerns can be reported in writing and by telephone at [number to be inserted]. Employees are expected to specify that they are filing a report under this policy. If a (potential or suspected) abuse or irregularity is reported to a line manager or the HR business partner, the compliance officer, a trusted person, or a representative of the employee's choice, or the senior management, the recipient is required to contact the Board of Directors without delay for further guidance.

3.2 Procedures for Handling Reports

Any report that is made directly to a line manager or the HR business partner, the compliance officer, a trusted person, or a representative of the employee's choice, or the senior management shall be promptly reported to the Compliance Officer by the recipient.

Each report forwarded to the Compliance Officer by the recipient and each report that is made directly to the Compliance Officer shall be reviewed by the Compliance Officer.

The Compliance Officer may, at its discretion, consult with any member of the senior management who is not the subject of the allegation and who may have appropriate expertise to assist the Compliance Officer.

The Compliance Officer shall determine whether the Compliance Officer or the Board of Directors should investigate the report, taking into account the considerations set forth below in 3.3. If the Compliance Officer determines that senior management should investigate the report, the Compliance Officer shall notify the company's chief executive officer of that determination. The senior management shall thereafter promptly investigate the report and shall report the results of its investigation to the Compliance Officer. Unless the Compliance Officer directs otherwise, senior management shall be free in its discretion to engage outside auditors, counsel or other experts to assist in the investigation and in the analysis of the results thereof.

If the Compliance Officer determines that the Compliance Officer should investigate the report, the Compliance Officer shall promptly determine what professional assistance, if any, it needs in order to conduct the investigation. The Compliance Officer shall be free in its discretion to engage outside auditors, counsel or other experts to assist in the investigation and in the analysis of the results thereof.

If the Compliance Officer so directs, a summary of reports received and/or investigated shall be provided to the full Board of Directors.

The Compliance Officer will send a confirmation of the report of suspected Irregularity to the reporter within seven days after receipt of the report. The acknowledgement will contain, at a minimum, a business description of the report, the date it was received, and a copy of the report.

Within three months after sending the confirmation of receipt of the report, the Compliance Officer will inform the reporter in writing of its position regarding the reported suspected Irregularity.

3.3 Considerations Relative To Whether the Compliance Officer or Board of Directors Should Investigate a Report

In determining whether the Board of Directors or the Compliance Officer should investigate a report, the Compliance Officer shall consider, among any other factors that are appropriate under the circumstances, the following:

1. ***Who is the alleged Irregularity doer?***

   If a financial officer, executive officer, or other high management official of the company is alleged to have engaged in the Irregularity, that factor alone may militate in favor of the Compliance Officer conducting the investigation.

2. ***How serious is the alleged Irregularity?***

   The more serious the alleged Irregularity, the more appropriate that the Compliance Officer should undertake the investigation. If the alleged Irregularity would constitute a

crime involving the integrity of the financial statements of the company, that factor alone may militate in favor of the Compliance Officer conducting the investigation.

3. ***How credible is the allegation of Irregularity?***

   The more credible the allegation, the more appropriate that the Compliance Officer should undertake the investigation. In assessing credibility, the Compliance Officer should consider all facts surrounding the allegation, including, but not limited to, whether similar allegations have been made in the press or by analysts.

Reporting channels third parties

The Company whistleblowing channels are also open to third parties. Third parties include clients, suppliers, agents, etc. Former employees, who no longer work for the Company, are also treated as third parties.This policy is not designed for clients who wish to file a complaint. These clients are kindly requested to follow the complaints procedure.

Third parties can report any Irregularities under this policy email to compliance@rgltd.com which only the Compliance Officer reads. The Compliance Officer registers the report in the internal whistleblowing reporting tool and handles and investigates it under this policy like any other report. The Company does not publish a whistleblowing reporting form on its website. The website publishes this policy.

The five key principles of the Company's Whistleblowing Policy referred to in paragraph 2.3 are also applicable to third parties making use of the policy.

Substantiating report

In order for the Company to properly assess and investigate the reported Irregularity, it is recommended to substantiate the report by providing documents or other details. The Company may refrain from investigating or other follow-up measures if a report contains unsubstantiated allegations and/or if it is not possible to gather further information because the report was submitted anonymously. A claim template can be found in Schedule 1. Paragraph 4.1 lists the conditions for assessing the information provided.

4. The Investigation Process

It is the Company's policy to investigate reports of Irregularities thoroughly, fairly and in a timely manner, with appropriate technical and investigative expertise. The Company is committed to conduct an investigation that is fair to all parties involved and to use all its appropriate resources to address Irregularities that have occurred or are occurring.

All reports falling within the remit of the Whistleblowing Policy are dealt with in a manner which aims to protect the reporting person from any retaliation caused by their decision to make the disclosure.

4.1 Conditions in assessing and weighing information

- Overall criteria to proceed with an investigation include:
- Assessment of proper use of the Whistleblowing Policy;
- First assessment trustworthiness whistleblowing report (based on content and documentation or details of the report), its materiality to the Company and likeliness the reported Irregularity may continue;
- Information already known or available regarding the complaint;
- Availability of investigation leads;
- Timeframe mentioned in whistleblowing report (there are limitations in the access of data when the Irregularity took place long ago);
- Professional judgement of the Compliance Officer (in consultation with its advisers);
- Possibility to accomplish contact and/or remain in contact with whistleblower for follow-up questions;
- The ability to protect the identity of the whistleblower throughout the process;
- Willingness of the reporting person to proceed with the process (note that relevant signals might be investigated by the Compliance Officer without compromising the whistleblower);
- In general developing jurisprudence around proportionality and subsidiarity in forensic investigations are taken into account in accordance with the Legal Counsel and HR.

5. Retention Periods

Upon its receipt in a register set up for that purpose and registers a report upon its receipt in a register set up for that purpose and which meets the requirements of the General Data Protection Regulation (**GDPR**). This will include, in any case: (a) information regarding the date the report was received; (b) a description of the report; (c) the reporter (if provided); and (d) the status and disposition of an investigation of the report. Access to the register is maintained on a least-privileged basis.

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the reporting person, the subjects of the report and any third parties mentioned in the report, taking into account the time required for any further investigations. In particular, personal data relating to out-of-scope reports will be destroyed without undue delay.

6. Feedback

If contact details are provided, the reporting person will be contacted to be informed if their report is in scope of this policy and if so about whistleblower protection and next steps.

It is important to strike a balance between the legitimate interest of the reporting person to receive information about the status of the investigation and the need to keep the investigation process and outcome confidential to protect the course of the investigation, the rights of the accused person or the confidential nature of any follow-up measure. The Company endeavours to keep anyone who raises concerns under this policy abreast of how their concerns are being addressed. For legal or practical reasons this is not always feasible: for example, the fact that disciplinary action has been taken against an individual can generally not be shared because of privacy issues and an investigation by a regulator or law enforcement agency will usually be confidential in itself. Where a report has been filed in good faith and subsequently leads to regulatory or court hearings, the employee who filed the initial report may be expected to serve as a witness. Where this occurs, the Company will provide appropriate assistance and support, including any necessary legal advice to the employee in the run-up to and during the hearing.

7. Privacy Rights

Pursuant to applicable law, the reporting person has the right to:

(a) request access to their personal data;

(b) request rectification of their personal data;

(c) request erasure of their personal data ("the right to be forgotten");

(d) request restriction of processing of their personal data;

(e) data portability where applicable (such as where processing is based on consent);

(f) object to the processing of their personal data while the Company verifies their processing; and

(g) where applicable, to withdraw their consent at any time.

The Company will not make use of automated decision-making, including profiling. The reporting person can exercise these rights by submitting an email to dpo@rgltd.com

The Company will respond to such requests in accordance with applicable data protection law.

For more information about the processing of your personal data, please refer to the relevant Privacy Notice applicable to your relation with the Company.

8. External Reporting

The Company strongly encourages reports to be made internally so that any concerns can be resolved. However, should reporting persons decide to report their concerns externally in compliance with applicable provisions, this can be done with the following competent authorities for the Netherlands.

(a) Authority for Consumer & Markets, ACM (in Dutch: "*Autoriteit Consument en Markt*");

(b) Authority for Financial Markets, AFM (in Dutch: "*Autoriteit Financiële Markten*");

(c) Data Protection Authority (in Dutch: "*Autoriteit Persoonsgegevens*");

(d) Dutch Whistleblowers Authority (in Dutch: "*Huis voor Klokkenluiders*");

(e) Health and Youth Care Inspectorate, IGJ (in Dutch: "*Inspectie gezondheidszorg en jeugd*");

(f) Dutch Healthcare Authority, NZa (in Dutch: "*Nederlandse Zorgautoriteit*");

(g) Nuclear Safety and Radiation Protection Authority (in Dutch: "*de Autoriteit Nucleaire Veiligheid en Stralingsbescherming*");

(h) Other authorities appointed by the minister or statute.

The relevant modalities can be found on the websites of each of the competent authorities concerned. It is also possible to seek advice on a confidential basis from the Advice Department of the Dutch Whistleblowers Authority before making a report (*advies@huisvoorklokkenluiders.nl*).

9. Mandatory trainings

The Company's employees must follow the training courses assigned to them in relation to this policy.

10. Document control

10.1 Approval, review and deviations

This policy has been approved by the Board of the Company and is subject to annual review by the Compliance Officer. Deviations from this policy are only allowed with prior approval of the Board of Directors.

Should there be significant changes to the organisation or significant legal developments, the Compliance Officer reviews and, if needed, updated this policy prior to the annual review.

Amendments to this policy are subject to approval by the Board of Directors.

10.2. Version history

Version	Date of Change	Revisor	Summary of Change
1.0	16.10.2024	Compliance Officer	Baseline document – AFM licence application
2.0	11.03.2025	Compliance Officer	Revised and approved following AFM information request
3.0	11.07.2025	Compliance Officer	Revised and approved following AFM information request
3.10	12.08.2026	Compliance Department	Rebranded and redesigned to the RGLTD.com template and visual identity, following the trading-name migration from ARI10 to RGLTD.com. No substantive content was revised, added, or deleted; document structure, headings, tables, and regulatory content are unchanged from v1.0.
4.0	27.10.2026	Compliance Department	Entity-neutral wording: references to brand replaced with defined term “Company”. Company definition added. The versioning history was updated to reflect the current structure as v.26_9.0. Public whistleblowing reporting form removed from the website. Third parties report by email to the Compliance Officer, who registers and investigates the report in the internal reporting tool. Current employees use the internal channel with the link to the tool. Former employees are treated as third parties. Scope of reporting persons unchanged. Board approval pending.

© WEB3 Technology B.V. — All rights reserved. This document is confidential and intended solely for internal use.

Schedule 1 - Report

A whistleblowing report needs to include sufficient details about the reported or suspected abuses and irregularities.

Please help us by including answers to the following questions:

(i) What happened?

(j) Who is involved in the incident?

(k) Where did it happen?

(l) When did it happen?

(m) What evidence do you have or can be used for discovery to help the reviewer?

(n) Why are you making this report (any critical items you would like to draw attention to)?