

WHISTLEBLOWING POLICY

Organization and scope:	Aqilion AB (the ” Company ”)
Version:	1.0
Established by:	The Board of Directors
Date for establishment:	2024-03-12
Legal basis:	2021:890 Act on the Protection of Persons Reporting Irregularities
Owner:	CEO

1. Introduction, purpose and scope

The Company strives for a healthy business environment and is committed to transparency and accountability throughout its operations. The Company is aware that organizations can be subject to mismanagement and other abuses. Through this whistleblower policy (the "**Policy**"), the Company informs about and encourages the reporting of actual or suspected irregularities of public interest within the Company.

Furthermore, the Policy aims to establish a standard for reporting irregularities of public interest within the organization. An individual who wants to report irregularities ("**Whistleblower**") should feel safe and know that he or she can report irregularities of public interest without risk of retaliation and that reports are handled in a professional and confidential manner.

The Policy covers the entire operation. Everyone who is part of the Company's whistleblower circle has the opportunity to report under this Policy. Those included in this circle are those who are in contact with the Company in a work context, such as employees, consultants, trainees or volunteers.

2. Responsibility and accountability

The Company's Board of Directors is ultimately responsible for ensuring that the Company complies with the regulations governing the right to whistleblowing and protection against retaliation, etc.

The CEO is responsible for the ongoing work within the Company and for compliance with the Policy.

All employees are expected to be familiar with this Policy and the whistleblowing instructions applicable from time to time, and to make use of the opportunity to report irregularities under the Policy if necessary.

3. Reporting of irregularities

Irregularities are events of public interest, such as violations of laws and regulations or of the Company's own policies, or other misconducts for which there is a public interest in disclosure.

Some examples of activities or events that the Company considers to be irregularities in the public interest are:

- i) Bribery, theft, fraud, accounting fraud, tax evasion and other criminal acts,
- ii) serious breaches of internal governance documents,
- iii) activities that may cause damage to persons or property,
- iv) failure to rectify, or to report, events that could result in significant costs or losses,
- v) abuse of power or position,
- vi) discrimination on the grounds of age, race, gender, religion, sexual orientation, marital status, parental status, political opinion or ethnic origin in employment or use of services,
- vii) corruption and conflicts of interest; or
- viii) violations of the fundamental rights and freedoms of any person.

Report to your manager

Anyone who discovers or suspects irregularities is encouraged to report it to their manager. Reports of irregularities can also always be made to the Company's CEO or Chairman of the Board, directly or anonymously.

Internal reporting channel

Reports can also be made through an internal reporting channel. Information on the internal reporting channel is available on the Company's website/intranet. The Company provides a web-based service for receiving, handling and investigation of reports regarding irregularities. Reporting is made to an appointed third party, which then reports directly to the Company's Whistleblower Committee. If necessary due to the nature of the irregularity, the Chairman of the Board may be informed under secrecy. Information on the internal reporting channel is on the Company's website/intranet.

External reporting channels and publication:

Those who wish to report an irregularity can also do so by using an external reporting channel through which reports are made to the competent authority. Information on how to report to competent authorities via an external reporting channel can be found on the Company's website. In some cases, it is possible to be covered by the protection of the law also when publishing information regarding an irregularity.

Investigation and response

Irregularities should be investigated as expeditiously as the circumstances require and within applicable time limits. The Company has appointed a Whistleblower Committee which is responsible for the internal management of reports received through the internal reporting channel. The Whistleblower Committee is subject to a special confidentiality obligation. This means, among other things, that they may not reveal the identity of a reporting person or the content of a report to anyone else in the organization except as set out in this Policy.

It is important that any individual who makes a report genuinely suspects that an irregularity of public interest exists.

The Company may enlist the support of an external party in handling and investigating reports received.

Notwithstanding the above, the Whistleblower shall, no later than seven days after receipt of a report, receive confirmation that the report has been received. Within three months of confirmation, the Whistleblower should receive reasonable feedback on any action taken or planned, and the reasons for it. If the deadline may be extended for specific reasons, the Whistleblower will be informed accordingly.

Annual follow-up and reporting to the Board

Once a year, a summary of incoming reports is prepared, indicating the type of reports but no details and whether the case has been resolved or not. This summary is sent to the Board.

4. Protection when reporting

A whistleblower must be protected from all types of retaliation. The protection follows from 2021:890 Act on the Protection of Persons Reporting Irregularities. The protection applies provided that the Whistleblower has had reasonable grounds to assume that the information in the report is true and that he or she is not guilty of a crime by obtaining the information. The same applies to a person who assists the Whistleblower in reporting, such as a shop steward or a safety representative. The disclosure of documents in connection with reporting is not covered by the protection.

Examples of retaliation from which whistleblowers should be protected are:

- i) termination, dismissal, reassignment,
- ii) lack of pay increase, reduction in benefits,
- iii) unjustified poor performance; and
- iv) lack of promotion, ostracism and any other retaliation related to the reporting.

The Company shall not retaliate against anyone for approaching their workers' organization for consultation on the issue of reporting. Nor should the Company obstruct or attempt to obstruct such consultation.

A Whistleblower is also protected when he or she chooses to report to a competent authority through an external reporting channel, provided that no reasonable follow-up action has been taken by the Company after internal reporting or if the Whistleblower has not received confirmation of receipt of the report within seven days or has not received feedback within three months. The protection for external reporting also applies when the Whistleblower has reasonable grounds to believe that there is an irregularity that involves an imminent or obvious danger or if internal reporting can be assumed to entail a risk of retaliation or failure to remedy the irregularity.

Whistleblowers are protected from investigation, which means that the Company may not investigate the identity of the person who made a report. Nor may the Company obstruct or attempt to obstruct reporting.

5. Confidentiality, data protection and documentation

Confidentiality

A report of irregularities or suspected irregularities must be handled confidentially. Information that could lead to the identification of the reporting person may be disclosed, for example in the context of a police report, provided that it does not hinder or impede the purpose of the follow-up of the report.

The Whistleblower Committee is bound by a special confidentiality commitment as stated above.

Data protection

Personal data are processed in the context of follow-up cases, for the purpose of taking action, for reports to be used as evidence in legal proceedings or otherwise in accordance with law or regulation. Personal data processed in the context of a follow-up case and the taking of measures following a follow-up case may be processed for a maximum of two

years after the case has been closed. Personal data that is clearly irrelevant to the processing of a case may not be collected and will be deleted as soon as possible. More information on the Company's processing of personal data relating to employees can be found in our privacy policy for employees, or if you are not an employee, in our privacy policy.

Documentation

The case shall be documented in an appropriate manner.

Written documentation and reports should be kept for as long as necessary, but not more than two years after the case has been closed.

6. Review

This Policy is regularly reviewed and updated where necessary.