

Whistleblowing policy for Ferroamp AB (publ)

1. Adoption

This Whistleblowing policy for Ferroamp AB (publ) (Ferroamp) is revised annually or if changes require a special revision. The Whistleblowing policy was adopted at the Board meeting on 10/5/2023.

1.1 Purpose

Ferroamp strives to have a transparent business climate and a high level of business ethics. Our whistleblowing function provides an opportunity to communicate any suspicions of impropriety confidentially. The function is important for reducing risks and maintaining confidence in our operations, by enabling us to detect and rectify suspected irregularities at an early stage.

2. Whistleblowing

The whistleblowing function can be used to warn of serious risks of misconduct that may affect people, our organisation, society or the environment.

2.1 When can you whistleblow?

Things reported may include information on criminal acts, irregularities and infringements or other acts that breach EU or national law in a work-related context, and where it is in the public interest that they come to light, such as:

- Corruption and financial crimes, such as bribery, extortion, unfair competition, money laundering, theft, fraud and forgery, accounting offences and conflicts of interest.
- Crimes that affect the life and health of individuals, such as serious environmental crimes, major deficiencies in workplace safety and very serious forms of discrimination and harassment that are contrary to the law.

For cases such as workplace dissatisfaction or related issues, a supervisor or manager must be involved, because these issues cannot be treated as whistleblowing cases.

A person who submits a report through the whistleblowing function does not need to have proof of their suspicions. However, no accusation may be made with malicious intent or with the knowledge that the accusation is false. Misuse of the whistleblowing system is a serious disciplinary offence.

2.2 Who can whistleblow?

The whistleblowing function can be used by all employees (regardless of form of employment) in Ferroamp. Customers, suppliers or other stakeholders can also use the system.

2.3 How do you whistleblow?

For written reporting, we use Visslan, which is our digital whistleblowing channel. It is always available through <https://ferroamp.visslan-report.se> On the website, you choose to "report" in order to then be able to describe your suspected misconduct.

Please describe what happened as thoroughly as possible, so that we can ensure that adequate measures can be applied. It is also possible to attach additional evidence, in the form of, for example, written documents, pictures or audio files, even though this is not a requirement.

2.4 Sensitive personal data

Please do not include sensitive personal information about people mentioned in your report unless it is necessary to be able to describe your case. Sensitive personal data is information about; ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, a person's sexual life or sexual orientation, genetic data, biometric data used to uniquely identify a person.

2.5 Anonymity

You can be anonymous throughout the process without affecting your legal protection, but you also have the opportunity to confess your identity under strict confidentiality. Anonymity can in some cases complicate the report's follow-up possibilities and the measures we can take, but in such a case we can also later ask you to reveal your identity later, again in strict confidentiality to the Case Manager(s).

2.6 Follow-up & login

After you have reported, you will receive a sixteen-digit code, which you will in future be able to log in to Visslan with from <https://ferroamp.visslan-report.se> It is very important that you save the code as otherwise, you will not be able to access your report again.

If you lose the code, you can submit a new report referring to the previous report.

Within **seven days**, you will receive a confirmation that the Case Manager(s) has received your report. The Case Manager(s) is/are the independent and autonomous party that receives reports in the reporting channel, whose contact information is attached in "6.1 Contact information for Case Manager(s)". In case of questions or concerns, you and the Case Manager(s) can communicate through the platform's built-in and anonymous chat function. You will receive feedback within **three months** on any measures planned or implemented due to the reporting.

It is important that you, with your sixteen-digit code, log in regularly to answer any follow-up questions Case Manager(s) may have. In some cases, the report can not be taken forward without answers to such follow-up questions from you as the reporting person.

2.7 Verbal reporting

In addition, it is also possible to conduct a verbal report by uploading an audio file as an attachment when creating a report at <https://ferroamp.visslan-report.se> You do this by selecting that you have evidence for the report, and uploading an audio file there. In the audio file, you describe the same facts and details as you had done in a written case.

In addition, a physical meeting with the Case Manager(s) can be requested via Visslan. This is most easily done by either requesting it in an existing report, or creating a new report asking for a physical meeting.

3. What are my rights?

3.1 Right to confidentiality

During the handling of the report, it will be ensured that your identity as a reporting person is treated confidentially and that access to the case is prevented for unauthorized personnel, i.e. Case Manager(s). We will not disclose your identity without your consent if applicable law does not compel us to, and we will ensure that you are not subjected to retaliation.

3.2 Protection against reprisals or retaliation

In the event of a report, there is protection against negative consequences from having reported misconduct in the form of a ban on reprisals and retaliation. The protection against this also applies in relevant cases to persons in the workplace who assist the reporting person, your colleagues and relatives in the workplace, and legal entities that you own, work for or are otherwise related to.

This means that threats of retaliation and attempts at retaliation are not permitted. Examples of such are if you were to be fired, have been forced to change tasks, imposed disciplinary measures, threatened, discriminated against, blacklisted in your industry, or the like due to reporting.

Even if you were to be identified and subjected to reprisals, you would still be covered by the protection as long as you had reasonable grounds to believe that the misconduct reported was true and within the scope of the Whistleblower Act. Note, however, that protection is not obtained if it is a crime in itself to acquire or have access to the information reported.

The protection against retaliation also applies in legal proceedings, including defamation, copyright infringement, breach of confidentiality, breach of data protection rules, disclosure of trade secrets or claims for damages based on private law, public law or collective labour law, and you shall not be held liable in any way a consequence of reports or disclosures provided that you had reasonable grounds to believe that it was necessary to report or publish such information in order to expose a misconduct.

3.3 Publication of information

The protection also applies to the publication of information. It is then assumed that you have reported internally within the company and externally to a government authority, or directly externally, and no appropriate action has been taken within three months (in justified cases six months). Protection is also obtained when you have had reasonable grounds to believe that there may be an obvious danger to the public interest if it is not made public, for example in an emergency. The same applies when there is a risk of retaliation in the case of external reporting or that it is unlikely that the misconduct will be remedied in an effective manner, for example in the event that there is a risk that evidence may be concealed or destroyed.