



ITIVITI

Whistleblowing Policy

Itiviti Group AB



Introduction

This whistleblowing policy, which is drafted in line with the principles in Itiviti Group's policies, is a vital part of Itiviti's Corporate Compliance Program.

Employees are often the first to discover misconduct at their workplace, and it is important that an employee who discovers wrongdoing by the company or any of its employees, consultants, contractors, or suppliers is able to report it without risk of retaliation or discrimination.

The purpose of this policy is to encourage employees to raise concerns about matters occurring within or related to Itiviti, rather than overlooking a problem or seeking a resolution of the problem outside the Itiviti.

This policy applies to everyone at Itiviti – all employees, managers, executive officers, and members of the board of directors (all of whom are included in the term "employees" as used in the remainder of this policy).

For further details on the Whistleblowing System and the Standard Reporting Channels, please visit the Whistleblowing Manual.



The Whistleblowing System

In order to allow employees to raise concerns about wrongdoing, Itiviti has established a whistleblowing system that serves as a contact interface designed specifically for receiving and handling employees' reports on suspected misconduct.

However, laws and regulations on protection of personal data set limitations on the circumstances under which Itiviti may process information indicating that one of its employees has been involved in suspected misconduct.

For this reason, the whistleblowing system may only be used in the following circumstances:

First, **only serious misconduct may be reported** through the whistleblowing system. Serious misconduct involves irregularities or improper actions concerning Itiviti's vital interests or individuals' health and safety. This may for example include:

- financial crime and accounting irregularities.
- the offering or acceptance of bribes.
- environmental risks or crimes.
- security vulnerabilities which constitute a risk for employees' or customers' health or safety.
- serious forms of harassment or discrimination; or
- violations of the Company's Code of Conduct.

Second, **only misconduct by persons in a key or leading position within Itiviti may be reported** via the whistleblowing system. This means that only misconduct by Itiviti's board of directors, executive officers, or individuals responsible for major purchases or other key business functions may be reported through the whistleblowing system.

Third, the whistleblowing system **may only be used to the extent that it is justified not to turn to Itiviti's standard information and reporting channels**, as described in the last section of this policy. This may for example be the case when the reported person is part of the management or the suspected misconduct, for that or other reasons, runs the risk of not being properly handled.

The whistleblowing system complements the Itiviti's standard internal information and reporting channels and is available for use on a voluntary basis. The standard reporting channels are always available for reporting of any and all concerns, see the section below on Standard Reporting Channels.

How to Report a Concern Through the Whistleblowing System

To report a concern related to an issue which fits the description above, please review the local Whistleblowing Manual for guidance.

The whistleblowing system is accessed via: <https://report.whistleb.com/ITIVITI>

For Russian employees the whistleblowing system is accessed via:
<https://report.whistleb.com/ITIVITIRussia>



Process

Itiviti will act upon any concerns raised. Please note that Itiviti can assess a concern only after having conducted an initial inquiry and, most likely, after properly investigating the matter in question.

Where appropriate, matters raised may:

- be investigated by management, the board of directors, internal audit, or through the disciplinary process.
- be referred to the police or other law enforcement authorities.
- be referred to an independent auditor; or
- become the subject of an independent inquiry.

In order to protect the individuals involved and those suspected of the alleged wrong-doing, an initial inquiry will be made to decide whether an investigation is appropriate and, if so, what form it should take. If urgent action is required, it will be taken before any investigation is conducted.

Where a concern is directed at, or involves, an individual handling the reported concerns, that individual will not be involved in investigating or assessing the matter.

Where a concern is directed at, or involves, the CEO, the Chairman of the Board will lead the investigation and assessment of the matter.

All reported concerns will be filed and saved.

Timing

Concerns will be investigated as quickly as is practicable. It may be necessary to refer a matter to an external advisor, which may result in an extension of the investigative process. The seriousness and complexity of a complaint will also have an impact on the time needed to investigate the matter.

Itiviti acknowledges that any person who raises a concern will need assurance that the concern has been addressed. Subject to legal constraints, Itiviti will provide the person raising the concern with information about the outcome of any investigation.

Prevention of Retaliation

Itiviti will not tolerate any attempt to penalize, or discriminate against, an employee who has used the whistleblowing system to report a genuine concern regarding wrongdoing. Any such retaliation may be subject to disciplinary action by Itiviti, up to and including termination of employment.

Anonymity

Complaints can be made anonymously through the whistleblowing system. However, it normally facilitates any subsequent investigation and handling of the matter if contact details have been provided. Therefore, Itiviti encourages employees to provide name and contact details when reporting a complaint. For further information please view the Employee Manual.



False and Malicious Allegations

Itiviti strives to meet the highest standards of honesty and integrity and will ensure that sufficient resources are put into investigating any complaint received.

However, it is important for any employee considering making allegations to ensure that they are sincere. The making of any deliberately false or malicious allegations may result in disciplinary action.

Processing of Personal Data

Reports made through the whistleblowing system are likely to contain personal data – data which directly or indirectly pertains to an identified or identifiable individual. The personal data may pertain to the person who has made the notification, and/or to a person suspected of the alleged wrongdoing. The types of personal data which may be processed in conjunction with an investigation are typically the following:

- The name, position, and contact details (for example e-mail and telephone number) of the employee who submitted the complaint and the individual to whom the complaint relates, as well as any witnesses or other individuals affected.
- Details of the misconduct of which the person reported is suspected.

Itiviti will only process personal data which is correct and relevant to the investigation. Superfluous personal data will not be processed. Sensitive personal data, such as an individual's race or ethnic origin, political views, religious or philosophical conviction, membership of a trade union, or data relating to an individual's health or sex life, will, as a general rule, not be processed by Itiviti.

Itiviti is the data controller of any personal data collected via the whistleblowing system, and is responsible to ensure that the personal data collected is processed in accordance with applicable laws and regulations on data protection.

The details of Itiviti for purposes of its role as data controller are as follows:

Itiviti Group AB
Org. nr. 556313-4583
Kungsgatan 36, Box 7742, SE 103 95 Stockholm, Sweden
info@itiviti.com
+46 (0)8 506 477 00

Any personal data collected via the whistleblowing system will be processed for the purpose of administering and investigating allegations raised, and dealing with discovered misconduct, as described in this manual. Itiviti takes both technical and organizational security measures to protect the personal data processed. The personal data collected will be processed only by those individuals at Itiviti who are involved in the investigation. In this context, personal data may be transferred to a department within Itiviti (such as internal audit), management, the board of directors, or other persons closely related to Itiviti. In addition, personal data may be transferred to the police or other law enforcement authorities, forensic companies, or independent auditors. To the extent deemed necessary, it may also be transferred to the Itiviti's affiliates or joint venture partners.



If it is necessary to transfer personal data to individuals or companies in countries outside the European Union or European Economic Area (EEA), which may not provide the same level of protection as in an individual's home country, the transfer will be made in accordance with applicable law.

The personal data which is compiled and processed will not be retained longer than is necessary. Complaints, reports, and information regarding misconduct which have been investigated will be deleted within two months of the conclusion of the investigation or, if the investigation results in action being taken against the individual who has been reported, when the information is no longer needed for the purpose of carrying out an investigation and taking action. If it is decided that no investigation will be initiated, the information will be deleted immediately after such decision has been made.

When personal data pertaining to an individual is collected via the whistleblowing system, the individual must be informed. If it is not possible to inform the individual immediately, for example if such information could jeopardize Itiviti's investigation, information will be provided at a point of time where it would no longer constitute a risk to the investigation.

Subject to the limitations stated above, Itiviti will provide, free of charge to every person who requests it, notification once per annum of whether personal data concerning the applicant is processed or not. An application for such information shall be made in writing, signed by the applicant, and sent to Itiviti using the contact details provided in this section.

Itiviti will, at the request of a registered person, rectify, block, or erase personal data that is incorrect or that has otherwise not been processed in accordance with applicable laws and regulations.

Standard Reporting Channels

Employees with a concern related to a person or issue which does not fit the description of matters which may be reported through the whistleblowing system should not use the whistleblowing system. Instead, employees should raise these issues through their standard reporting channel, which consists of the employee's direct manager, another manager whom the employee trusts, or the Human Resources department. For further information, please view the Employee Manual.

Related Documents

This policy should be read in connection with the following documents.

- Whistleblowing Manual
- Code of Conduct
- Data Protection Policy
- Data Protection Manual
- Employee Manual

Applicability

This policy applies to all employees of Itiviti Group AB and its subsidiaries. In cases where national regulations cause difficulties regarding the implementation of or differs from the content of this policy,



national regulations shall rule in those areas. Other parts of this policy shall still be valid. For further information on local applicability, please view the Employee Manual.

Owner

Chief Compliance Officer.