Whistleblowing Policy

Itiviti Group AB

Table of Content

Summary

Itiviti is committed to comply with all applicable laws and regulations and believes that the ability of employees to report a suspected breach is vital in achieving this goal. As a result, Itiviti has established procedures to enable employees to report concerns about wrongdoings or alleged breaches of a general, operational and financial nature. The Chief Compliance Officer reports on whistleblowing cases to the Chairman of the Board of Directors.

Itiviti ensures that employees who report concerns in good faith are free to do so without fear of retaliation.

Employees can report alleged breaches:

- ✓ Directly to their management (their manager or another manager whom the employee trusts),
- ✓ To the Human Resources Department,
- ✓ To the Chief Compliance Officer,
- ✓ To the Chairman of the Board under specific circumstances.

Alternatively, employees can also report concerns using Itiviti's anonymised Whistleblowing System via the following third-party website: https://report.whistleb.com/ITIVITI. This provides the ability to report alleged misconduct anonymously.

Misconduct that pertain to accounting and auditing matters will be investigated by the Finance Department under the direction and oversight of the Board. Other alleged wrongdoings will be investigated initially by the Chief Compliance Officer, under the direction and oversight of the Board. Any misconduct of the Chief Compliance Officer should be reported directly to the CEO.

This Policy is global and applies to all Itiviti employees.

For more information about this policy, please contact your Chief Compliance Officer or send an email to: legal@itiviti.com

Introduction

This Whistleblowing Policy is a vital part of Itiviti's Corporate Compliance Program.

Employees are often the first to discover misconduct in the workplace, and it is important that an employee who discovers wrongdoing 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 Itiviti.

This policy applies to everyone at Itiviti – all employees, managers, consultants, 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 review the Whistleblowing Manual.

The Anonymised Whistleblowing System

In order to allow employees to raise concerns about wrongdoing, Itiviti has established an anonymised Whistleblowing System managed by a third party ("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 (including insider trading, false expenses claims,…),
- Conflicts of interests, or the offering or acceptance of bribes (or similar schemes where an employee uses his/her position to obtain a personal gain without disclosure to or the prior approval of the Company),
- Environmental risks or crimes,
- Misuse of personal data,
- Intellectual Property infringement,
- Unfair competition or competition law violations,
- Security vulnerabilities which constitute a risk for employees' or customers' health or safety,
- Harassment or discrimination, or
- Violations of the Company's Code of Conduct.

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 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 will systematically conduct initial inquiries to assess a concern and report to the Board. The Board will request a full investigation if the initial inquiry reveals evidence of misconduct. The initial inquiry will generally be conducted by the Chief Compliance Officer.

However, 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 the CFO if pertaining to accounting crimes, or
- 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.

No individual targeted by or involved in a reported concern will investigate or assess 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

Initial inquiries into reported concern will start from the date they are reported and be conducted, with due diligence and discretion, until evidence of the likelihood of a wrongdoing has been established, in which case the matter will be escalated to be fully investigated.

Because of the fact that individuals are concerned and consequences may be grave, including on a reputational level, initial inquiries will be undertaken in a manner that preserves the rights of individuals to the maximum extent possible. As a result, initial inquiries may take time. In some cases, it may be necessary to refer a matter to an external advisor, which may result in an extension of the process.

The seriousness and complexity of a complaint will also have an impact on the time needed to fully investigate the matter.

Itiviti acknowledges that any person who raises a concern will need assurance that the concern has been addressed. All concerns will be the subject of initial inquiries and will generate a report. 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 or the Standard Reporting Channels to report a concern regarding a potential wrongdoing. Any such retaliation will lead to disciplinary action by Itiviti, up to and including termination of employment.

Anonymity

To ensure anonymity, Itiviti has created a Whistleblowing System using a third party provider. Concerns may be reported using this system in complete anonymity.

However, reporters of concerns must understand that not having their name or other relevant information may slow the inquiry process down substantially.

Therefore, where possible, Itiviti encourages employees to provide documentation, name and contact details when reporting a complaint.

For further information, please view your office Employee Manual/Handbook.

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 and the Standard Reporting Channels 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 or persons 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 report on potential wrongdoing and the individual to whom such report relates, as well as any witnesses or other individuals affected.
- Details of the misconduct attributed to the person suspected of wrongdoing.

Itiviti will only process personal data which is strictly relevant to the investigation. 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 in the context of this policy.

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.

For further information, please consult the Data Protection Policy and Manual.

Any personal data collected via the Whistleblowing System or the Standard Reporting Channels will be processed for the purpose of administering and investigating reported concerns, and dealing with discovered misconduct, as described in this Policy and related Manual. All exchanges in relation to inquiries and investigations will be deleted from the mail servers once such have ended and archived together with relevant reports on a secure archival server either held by Itiviti or by a specialized third party. The stored information will be kept for a period of 5 years unless otherwise required by law or legal claims.

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 inquiry and investigation at Itiviti. In addition and exceptionally, 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.

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 and using protections afforded under the GDPR.

When personal data pertaining to an individual is collected via the Whistleblowing System, the individual targeted by the report will 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.

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 can always report their concerns using the Standard Reporting Channels. They can do this:

- ✓ directly to their management (their manager or another manager whom the employee trusts),
- ✓ to the Human Resources Department,
- ✓ to the Chief Compliance Officer,
- ✓ to the Chairman of the Board under specific circumstances.

For wrongdoings such as fraud or other criminal conducts involving the top management of the company, employees should report their concern either through the Whistleblowing System or directly to the Chairman of the Board.

For further information, please view your office Employee Manual/Handbook.

Related Documents

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

- Whistleblowing Manual
- Code of Conduct
- Data Protection Policy
- Data Protection Implementation Manual
- Anti-Corruption and Anti-Bribery policy
- Office Employee Manual/Handbook

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 Office Employee Manual/Handbook.

Owner

Chief Compliance Officer / Chief Legal Officer.

* *

*

Version: 2.0
Effective as Itiviti Group Policy: December 2018
Last updated: November 2018
By: Legal Department