WHISTLEBLOWING POLICY

1. INTRODUCTION

1.1. At Mips Group we aim for the highest possible level of transparency, responsibility and business ethics. Our Code of Conduct, which covers all employees, maps out our approach to issues concerning a variety of areas, including business ethics. Our employees, as well as other collaborators, play a key role in identifying deviations from the Code of Conduct or other Group policies and therefore we encourage everyone who has serious concerns about our activities to make their voice heard and report their concerns.

1.2. The purpose of this whistleblowing policy is to handle reports filed under Mips Group's whistleblower function in Navex WhistleB. Under this policy, whistleblowers who are prepared to report misconduct are made aware that they are an important resource for Mips Group, and therefore Mips Group seeks to ensure a business environment in which whistleblowers feel that they can report misconduct safely and without fear of reprisals.

1.3. Our whistleblowing service offers an opportunity to report suspicions of serious misconduct in accordance with sections 3 and 4 below. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage. Reports can be submitted openly or anonymously.

2. WHO CAN USE THE WHISTLEBLOWER SERVICE AND WITH WHAT PROTECTION?

2.1. The whistleblower service can be used *by anyone* (including the public) provided that the report fulfils the general requirements and relates to specific misconduct or irregularities in accordance with sections 3 and 5 below. Individuals who are not employees or otherwise active in Mips AB in a work-related context and who file a report in accordance with this section 2.1 are hereinafter referred to as "External Whistleblowers".

2.2. Please note that the statutory protection against retaliation and against confidentiality obligations provided by the Swedish Whistleblower Act (2021:890) (described in in sections 2.4 - 2.6) only applies to whistleblowers who represent or are active in Mips AB in a work-related context. Nevertheless, Mips Group wants to emphasize that information about misconduct is taken seriously – regardless of who provides it – and gratefully receives reports of irregularities in accordance with this policy even if you do not belong to a category of persons who can whistleblow with Swedish statutory protection. Please note that External Whistleblowers may neither report to the authorities in accordance with section 9, or by publication in accordance with the conditions specified in section 10.

2.3. Anyone who in any way represents or is active in Mips AB in a work-related context may submit reports regarding misconduct or irregularities in accordance with sections 4 and 5 below. This includes board members, all employees (permanent employees, probationary employees, fixed-term employees, and full-time and part-time employees), trainees and temporary employees (crew personnel). Shareholders who are active in Mips AB, as well as people who are members of Mips AB's control bodies, may also file reports using the function. Individuals who file a report in accordance with this section 2.3 are hereinafter referred to as "Internal Whistleblowers".

2.4. Internal Whistleblowers who report misconduct that is subject to this policy (see sections 4 and 5 below) are protected from any reprisals, which means that the whistleblower or a related party may not suffer any negative consequences as a result of the person filing a whistleblower report. This protection is subject to the condition that the report was made in good faith, that the Internal Whistleblower had reasonable grounds to assume that the information concerning the misconduct was accurate, and that the report was made in one of the ways specified in this policy. The protection in accordance with this section not only covers the Internal Whistleblower, but also their colleagues, trade union representatives, or health and safety officers who provide assistance, as well as the Internal Whistleblower's employer or company if, for example, the Internal Whistleblower is temporary staff or a consultant at the company. If an Internal Whistleblower experiences reprisals as a consequence of misconduct reported by a person or any other party, the Internal Whistleblower should contact the HR department immediately. It should be noted that this protection does not prevent the Group from taking action against an Internal Whistleblower for *other reasons* than the whistleblower's report.

2.5. Internal Whistleblowers who report misconduct in accordance with section 4 of this policy will, in most cases, also be protected against sanctions due to the reporting constituting a potential breach of a confidentiality obligation, provided that there were reasonable grounds to believe that it was necessary to provide the information in question in order to disclose the misconduct. This protection does not include surplus information that is not reasonably required to be disclosed in order to reveal the misconduct. The protection applies irrespective of whether the duty of confidentiality is stipulated by agreement or law but does not include qualified confidentiality obligations. Examples of qualified confidentiality obligations that are not covered by the exemption from liability include breaches of confidentiality obligations to protect national security interests or concerning defense-sector inventions. Other confidentiality obligations that may not be breached on the basis of reference to whistleblower legislation are those intended to protect private individuals in healthcare and medical care, as well as several confidentiality obligations concerning educational activities. It should be noted that the protection from breach of confidentiality obligations does not entail any right to disclose papers or documents.

2.6. Moreover, it must be remembered that there is no protection from reprisals if an Internal Whistleblower report results in criminal liability. In order for the protection described in sections 2.4 -2.5 to apply, it is also a requirement that the whistleblower files the report through the whistleblower service in Navex WhistleB, as a report to the authorities in accordance with section 9, or by publication in accordance with the conditions specified in section 10.

3. WHAT CAN BE REPORTED BY EXTERNAL WHISTLEBLOWERS?

3.1. In order for a report to be filed by an External Whistleblower, there must be concrete suspicions of an incident that fulfils both criteria below:

1. it relates to a *serious irregularity* (see section 3.2 below), and
2. the irregularity was committed by a member *of Mips Group's management or by another key person* within the Group (see section 3.3 below).

3.2. *Serious irregularities* mean:

- economic crime such as bribery, corruption, theft, fraud and counterfeiting, corruption, accounting offences and other violations of accounting and tax laws; and
- other serious irregularities affecting the vital interests of a company within Mips Group or the life and health of individuals, such as, for example, serious environmental offences, major workplace safety failures, and very serious forms of discrimination and harassment.

3.3. *Mips Group's management and other key management personnel* mean the following and similar roles within the Group:

- Group executive management: the CEO and other C-level executives responsible for setting up and implementing strategic and operational objectives.
- directors: individuals who sit on the group's Board of Directors, which guides and oversees the company's strategic direction and business ethics.
- department managers: individuals who lead key departments such as production, sales, marketing, human resources, purchasing and IT, and who have a major influence on the company's operations and performance.
- key competences: specialists with unique expertise that is crucial to the group's business, such as top engineers, scientists, and IP experts.
- legal and compliance staff: those who manage the company's compliance with laws and regulations, which is critical to avoid legal risks and fines.
- sales directors and sales professionals: key individuals in sales who develop and implement sales strategies, build relationships with customers, and secure deals that contribute to company revenue and growth.
- purchasing managers and purchasing staff: those who manage the acquisition of goods and services necessary for the group's activities, negotiate prices and conditions, and ensure the reliability and quality of suppliers.

These roles and their equivalents may be considered critical to the success of Mips Group as they are responsible for decisions and functions that may directly affect the Group's financial performance, growth opportunities, and operational efficiency.

4. WHAT CAN BE REPORTED BY INTERNAL WHISTLEBLOWERS?

4.1. Internal Whistleblowers may file reports which concern incidents or circumstances within the framework of Mips Group's activities, or a concrete suspicion that such incidents or circumstances may arise, and which relate to:

- any misconduct which should be disclosed in the public interest (see section 4.2), or
- in certain cases, infringement of legislation in designated areas (see section 4.3).

4.2. Misconduct which should be disclosed in the public interest concerns misconduct which in the interests of the general public should be revealed and investigated, for example:

- corruption and financial irregularities; for example, bribes, unfair competition, money laundering, fraud, conflict of interest or irregularities related to accounting, internal accounting control, audits, banking and financial crime,

- serious health and safety violations; for example, workplace health and safety, product safety, serious discrimination and harassments that are against the law, or
- serious environmental violations; for example, illegal treatment of hazardous waste.

4.3. Infringement of legislation in the following areas may be considered to constitute circumstances entailing that a report is considered to be qualified – even if this cannot be deemed to be in the public interest:

- Public procurement
- Financing of terrorism
- Environmental protection
- Feed safety and animal health and well-being
- Protection of private life and personal data
- Competition rules
- Prevention of money laundering
- Product compliance
- Documents concerning the EU's financial interests
- Financial services, products and markets
- Product safety
- Transport safety
- Public health
- Network and information security
- Corporate tax rules
- Food safety
- Consumer protection
- Radiation safety and nuclear safety

5. GENERAL REQUIREMENTS AND WHAT A REPORT SHOULD CONTAIN

5.1. A report must be based on concrete suspicions. All whistleblowers must have reasonable grounds to believe that the information provided is accurate, but the whistleblower does not need to have evidence to support their suspicion. Reports that are filed solely on the basis of rumours or hearsay are not subject to any protection. As a general rule, the whistleblower must have first-hand information. No allegation may be made with malicious intent or with the knowledge that the allegation is false. False or malicious allegations can be a serious breach of the employment contract, and there is no protection from reprisals in the event of knowingly false or malicious reports.

5.2. In a report, the whistleblower should describe all the facts and allegations as carefully and in as much detail as possible. The report should describe anything that may be of relevance to the report and include, if possible, at least the following information:

- what the report concerns,
- who or what is involved,
- where the incident occurred,
- when the incident occurred,
- whether it was a one-off event or concerns an ongoing or recurring problem, and
- whether the whistleblower is an Internal or External Whistleblower.

5.3. Within the framework of Mips Group's internal regulations a report that fulfils the above criteria and, when reported by an External Whistleblower, relates to misconduct described in section 3, or, when reported by an Internal Whistleblower, relates to misconduct described in section 4, is referred to as a qualified report.

5.4. A report that does not meet the criteria to be filed under the whistleblower function in accordance with sections 3 or 4 and 5 above is referred to as an unqualified report. An unqualified report will not be treated as a whistleblower report. If an employee files an unqualified report, the employee will be informed accordingly, and the report will be deleted within three weeks.

5.5. Matters not covered by this policy include incidents of general dissatisfaction with how the business is run, or with leadership, salary, or other regular personnel matters. The same applies to workplace issues that are not of a very serious nature. Matters of other types than those described in sections 3 and 4 above should be handled by reporting to the immediate manager, to the manager's manager, or to another similar person in a managerial position, alternatively to a health and safety officer or a trade union representative, if the whistleblower is a union member.

6. HANDLING OF REPORTS

6.1. The whistleblower service is managed by WhistleB, an external provider that ensures anonymity. WhistleB does not save metadata and cannot trace the IP address of a whistleblower.

6.2. The weblink into the whistleblower service is accessible via Mips AB's website or by copying this link into your browser: report.whistleb.com/mipsprotection.

6.3. Reports filed are handled by Mips Group's whistleblowing team who are subject to strict confidentiality obligations. Mips Group's whistleblowing team includes:

- Mips Group's whistleblowing committee (which consists of the Chairman of the Board of Directors and the Chairman of the Audit Committee), as well as
- specially authorized individuals at Moll Wendén Law Firm.

If a report concerns any member of Mips Group's ordinary whistleblower committee, an alternative committee that does not include this individual will be appointed.

6.4. Only the whistleblowing team has access to reports submitted through our reporting channel for anonymous reporting. An investigation may include additional individuals who provide information or expertise. These individuals are also bound to secrecy.

6.5. Upon receipt of a report, the whistleblowing team decides whether to approve or reject the report in accordance with applicable legislation. If the report is approved, appropriate measures are taken for investigation. See section 7 below.

6.6. The whistleblowing team may reject a report if:
- the report does not fall within the scope of what may be reported in the whistleblower service (according to sections 3 or 4 above),
- the report has not been made in good faith or is malicious,
- there is insufficient information to investigate the matter, or
- the matter that the report concerns has already been addressed.

6.7. Within seven (7) days of filing a report, the whistleblower will receive an acknowledgment of receipt. If the report is filed through the whistleblower function, the receipt will be sent on the communication site of the whistleblower service.

6.8. Irrespective of whether the report is assessed to be qualified or unqualified, the whistleblower will receive feedback regarding the assessment. If the report is assessed to be qualified, the whistleblower will also receive feedback regarding the handling of the matter. Feedback will be made available no later than three (3) months after a filed report.

6.9. A report will be handled with respect, care, confidentiality, and due consideration of the integrity of all persons involved. A report will also be dealt with promptly and decisions on necessary measures will be taken as soon as possible, but never at the expense of quality or the legal protection of the individual or individuals who are the subject of the report.

6.10. We encourage anybody who shares their suspicions to be open with their identity. All messages received will be handled confidentially. Those who wish to report anonymously may do so in writing through the external web-based reporting channel. Reports and subsequent discussion between the whistleblowing team and the whistleblower are then encrypted and password protected, and the whistleblower remains anonymous. It is also possible to give an oral report through the reporting channel.

6.11. If the whistleblower chooses not to conceal their identity, this information will be treated confidentially and kept secret for as long as legally possible. In the event of a report that results in a police report or other legal action, Mips Group or Moll Wendén Law Firm may, however, be required to disclose the whistleblower's personal data (e.g., because the person may need to appear as a witness a trial). In such a situation, the whistleblower will as a rule be informed

before their personal data is disclosed, unless such information would jeopardize the related investigations or judicial proceedings.

7. INVESTIGATIONS

7.1. All qualified whistleblower reports are treated seriously and in accordance with this instruction:

- Reports are handled confidentially,
- A report is not investigated by anyone who is affected or involved in the case,
- If necessary, the whistleblowing team may send follow-up questions through the reporting channel for anonymous reporting to the whistleblower. The subsequent discussion will be anonymous,
- No one from the whistleblowing team, or anyone else participating in the investigation process, will try to identify the whistleblower, and
- Corporate or external expertise may be included in the investigation upon consent from whistleblower.

8. INFORMATION ON PROCESSING OF PERSONAL DATA

8.1. Personal data provided in the whistleblowing service (such as personal data on the person specified in a message, the person submitting the report (if not sent anonymously) and any third persons involved) is processed in accordance with the provisions of the General Data Protection Regulation, other applicable legislation, and Mips AB's from time to time personal data policy, which is available at https://mipscorp.com/sv/start-svenska/privacy-policy/.

8.2. Personal data occurring in reports may be subject to a statutory duty of confidentiality that prevents unauthorised disclosure. The duty of confidentiality does not prevent the authorised disclosure of personal data, such as when the personal data is required to be passed on to the police or another authority.

8.3. Personal data included in a whistleblower service is deleted upon completion of the investigation, with the exception of when personal data must be maintained according to other applicable laws. Deletion occurs within 30 days after completion of the investigation. The documentation from reports and investigations that are saved will be anonymized. They may not include personal data through which individuals can be directly or indirectly identified.

9. OPPORTUNITY TO REPORT MISCONDUCT TO AUTHORITIES

9.1. In addition to utilizing Mips Group's own internal whistleblowing channel, Internal Whistleblowers also have the opportunity to file a report to a government authority. This is called "External Reporting". When reporting externally, the

whistleblower can receive the same protection as if using the company's internal whistleblowing channel and thereby make reports about the same types of misconduct as described in section 4 above.

9.2. The main difference between using the Group's whistleblowing channel and the external reporting procedure is that when reporting externally, a government authority receives and follows-up on the report – not the company. Mips Group will therefore, as an outset, not access the report and it is up to the relevant authority to determine what information will be shared with the Group.

9.3. Different government authorities and agencies are responsible for handling reports about misconduct in various areas. E.g., the Swedish Authority for Privacy Protection is responsible for reports about breaches of rules on the protection of personal data. Which procedures that shall be used, and the available methods of filing a report, can vary depending on the authority or agency, but the whistleblower will always be able to report orally, in writing or via a physical meeting.

9.4. There are a lot of different authorities and agencies which are tasked with operating the external reporting procedures in different areas. For an exhaustive list of authorities and agencies which are responsible for different areas, as well as their contact details, can be found on the webpage of the Swedish Work Environment Authority: Myndigheter med ansvar vid visselblåsning - Arbetsmiljöverket.

10. OPPORTUNITY TO PUBLICLY DISCLOSE INFORMATION ABOUT MISCONDUCT

10.1. In certain cases, protection in the event of a report by an Internal Whistleblower in accordance with this policy (see sections 2.3-2.6 above) may also be obtained if an Internal Whistleblower publicly discloses information about such misconduct as referred to in the section 4 above. A public disclosure may, for example, consist of the whistleblower turning to the media with details of the misconduct, or publishing the information on a blog or on social media.

10.2. Protection as stipulated in sections 2.3-2.6 above will only be provided upon public disclosure if:

- The Internal Whistleblower reported the misconduct externally to an authority in accordance with section 9, without the authority taking any reasonable measures to rectify the misconduct, or if the whistleblower has not received feedback from the authority within the specified time;
- The Internal Whistleblower has good reason to believe that external reporting to the authority in accordance with section 9 above would result in the

whistleblower being a subject to reprisals or that the misconduct cannot be eliminated; or

- The Internal Whistleblower has good reason to believe that the misconduct poses a clear or imminent threat to someone's life, health or safety, or there is a substantial risk of environmental damage, or the whistleblower has other similar reasons for publishing the information.

10.3. We recommend that the whistleblower always seek the advice of a trade union representative or legal representative before publishing any information covered by the scope of this policy.

11. FREEDOM OF DISCLOSURE AND PROCUREMENT

11.1. In Sweden, the concept of 'Freedom of Disclosure' exists. This is an aspect of the Freedom of Expression and applies to all individuals who share information with the intent of it being published and made available to the public. Freedom of Disclosure ensures that public authorities – that is, the state, regions, and municipalities – cannot penalise anyone for disclosing information that gets published. Note that the Freedom of Disclosure as such does not prevent a private employer from acting on the disclosure of information. The freedom of disclosure only applies if the information is shared with the creators of books, newspapers, TV and radio programmes, or a similar publication media. For example, this may involve sharing information with a TV reporter, newspaper journalist or author. Freedom of Disclosure also applies if the information is shared with editorial teams or publishers, such as a news or newspaper editorial team. It is important to highlight that Freedom of Disclosure has its limitations – for instance, there is no impunity if someone discloses information in violation of so-called qualified confidentiality obligations.

11.2. In addition to the Freedom of Disclosure, Freedom of Procurement also applies. Freedom of Procurement means that anyone may search for information on any subject for the purpose of it being published or to utilise their Freedom of Disclosure, without a public authority – the state, regions, and municipalities – being able to penalise that person. The Freedom of Procurement is limited, however, in such a way that the information may not be procured through certain criminal acts – such as theft, unlawful interception, unlawful coercion, and data breaches. Freedom of Procurement does not prevent private employers from acting on the procurement of the information.