Whistleblowing Policy

General

At WithSecure we are committed to a high level of ethics and integrity in conducting our business operations. We understand that this is crucial to our continued success and reputation. Our values, principles and policies guide our everyday business operations. We have a professional responsibility to speak up, report any possible corrupt, illegal or other undesirable conduct and take required actions after such conduct is discovered. This WithSecure's Whistleblowing Policy (**Policy**) is an important tool in discovering such conduct. WithSecure strongly encourages you to speak up if you suspect or witness any such behaviour, activities or conduct. WithSecure will take all reports made under this Policy seriously.

If you make a whistleblowing report in accordance with this Policy, we have a responsibility to protect you, including not disclosing your identity and ensuring you are not subject to any retaliation.

This Policy sets out how WithSecure provides you with an effective, objective, confidential and secure reporting channel, Whistleblowing-channel (**Whistleblowing Channel),** allowing you to express your concerns or suspicions openly and safely. On the Whistleblowing Channel you are also advised how to make a report, how you are informed on the follow-up actions and how you are protected. WithSecure reviews the Policy and the Whistleblowing Channel from time to time in order to ensure their accuracy and proper and reliable functioning.

The Whistleblowing Channel is not for reporting your personal work-related grievances such as grievances that relate to your employment contract or to occupational safety and health. Other WithSecure policies and ways to report apply to such. Accordingly, the Whistleblowing Channel is not to be used for giving general feedback to WithSecure.

Concerns and Suspicions to be Reported

The breaches to be reported through the Whistleblowing Channel include actual or potential crimes, serious omissions or misconduct, as well as other breaches of the applicable laws and regulations. All such infringements are later referred to as **Breach(es)**.

When you have information or reasonable suspicion about an actual or potential Breach and such Breach has occurred or is very likely to occur in WithSecure or about an attempt to conceal such Breach, kindly report this through the Whistleblowing Channel. Through the Whistleblowing Channel you can also request a separate meeting where you can provide information on such Breach.

If you are uncertain, you can also send first a question through the Whistleblowing Channel to ask whether the type of information you intend to disclose falls within the scope of the regulation and can be disclosed through the Whistleblowing Channel. In such case kindly remember to provide at least your email address in connection with the filing so that the person handling your request is able to answer to you through the Whistleblowing Channel.

The Whistleblowing Channel is available to you 24/7 at https://lantero.report/new/hhpartners. The questions presented in the Whistleblowing Channel in connection with filing of your report will guide you to give information that is necessary for investigating and handling your report. Kindly answer to all questions as accurately as possible.

Eligible Whistleblower

Persons who are eligible to act as a whistleblower and file a report concerning WithSecure include all persons who by virtue of their work-related activities, irrespective of the nature of such activities and of whether they are paid or not, have access to information on Breaches, including but without limitation, WithSecure's all current and former partners, directors, officers, freelancers, employees, secondees, contractors, suppliers (or their employees or subcontractors), agency workers, job applicants, volunteers and trainees as well as shareholders (who have an active role within WithSecure) and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members.

Your right to report on the Breaches is unlimited and cannot be, for instance, restricted or waived by any agreement, policy or form or conditions of your employment.

Anonymity

You can file a report on suspected Breach and its potential perpetrator anonymously through our Whistleblowing Channel. All reports coming through the Whistleblowing Channel are confidential meaning that WithSecure has the obligation to protect and keep your identity and the identity of any third party possibly mentioned in your report confidential. The reporting service is entirely independent of the organization to ensure that it is impossible to find out who is behind a report, for example by tracking IP addresses.

Levels of Anonymity

When submitting a report to the Whistleblowing Channel, you must first choose whether you want to do so anonymously or whether you want to disclose your identity fully to the ones authorized to receive and handle your report.

Submitting a report anonymously

When you submit a report in the Whistleblowing Channel, you will always receive a unique report-specific link to see the status of your report or any follow-up questions the ones authorized to receive and handle your report may have had. You cannot be identified through this link. It is only for the purposes to contact you anonymously when needed. If you have chosen to submit a report to the Whistleblowing Channel anonymously, you must choose between the following two levels of anonymity:

1. Providing an e-mail address to receive notifications of new questions or information

   When submitting your report, you can choose to provide your email address to the Whistleblowing Channel through which you will receive an email notification if a question or a notification has been left for you in relation to your report. Your email address is only used by the technical platform of the Whistleblowing Channel and will serve as a technical tool to notify you of new events. WithSecure and the ones authorized to receive and handle your report do not see or receive information of your email address. All information related to a report is erased from the Whistleblowing Channel when the report has been processed, so that no sensitive information is stored unnecessarily. This normally takes a maximum of three months.

2. Full anonymity

   You may also leave a report in the Whistleblowing Channel without disclosing your name, identity or providing your email address at all. In this case, the ones authorized to receive and handle your report will still be able to contact you through the link you received after submitting the report, but you yourself are responsible for remembering the link and reviewing it from time to time to see if there are any updates or follow-up questions to your report. You will not be notified of these through your email. If you choose not to disclose your name/identity and provide email address to the person(s) authorized to receive and handle the report, this may prevent the handling of your report and performing follow-up actions as effectively as WithSecure would like to. Correspondingly, this may prevent ensuring that there exists no conflict of interest between you and the representatives chosen to review the report.

Submitting a report by fully disclosing your identity

When you provide your name/identity in addition to your email address in the Whistleblowing Channel, only the ones authorized to receive and handle your report will receive this information. The ones authorized to receive and handle your report, are obliged to keep your name and identity confidential unless you give an explicit consent to reveal your name and identity. In this case information on your name and identity and your email address are also deleted from the technical platform of the Whistleblowing

Channel permanently after the handling of your report in the Whistleblowing Channel is concluded.

Offered Protection

In case you have reasonable grounds to believe, in light of the circumstances and the information available to you at the time of reporting, that the matters reported by you are true and fall within the scope of Breaches, you will be given protection against retaliation i.e. any negative consequences or threats and attempts of retaliation due to your report.

In order to receive protection, you shall primarily use our Whistleblowing Channel to file your report. Further, if you are employed by WithSecure, please note, in order to comply with your statutory duty of loyalty towards your employer under the law, you should primarily use our Whistleblowing Channel to file the reports.

However, you do not need to use our Whistleblowing Channel to receive protection, if you have reasonable grounds to believe that:

- our Whistleblowing Channel and handling of reports are not credible wherefore there may be retaliation against you e.g. due to breach of confidentiality;
- the Breach or related evidence could be destroyed when using our Whistleblowing Channel; or
- the Breach requires urgent actions to safeguard e.g. the life, health or safety of persons or to protect the environment.

In such situations you are entitled to file your report also through the public channel (in Finland to the Chancellor of Justice, once such channel becomes available) and still receive protection. When using the public channel, you cannot file your report anonymously. Note that this reference to public means this specific public channel, not revealing the information to the general public.

In practice the protection provided to you includes:

- identity protection;
- protection from retaliation;
- possible compensation and remedies e.g. due to retaliation; and
- civil, criminal and administrative liability protection.

Please note that you do not need to prove your suspicions or allegations correct. If you have had reasonable grounds to believe that the matters reported by you are true and fall in within the scope of Breaches, you are entitled to protection even if your disclosure later turns out to be incorrect. Please note that a mere allegation or hearsay with no supporting information is unlikely to meet the required standard of reasonable grounds.

Filing a knowingly false report is a breach of the whistleblowing legislation and our Code of Conduct and may result in disciplinary action. There may also be other legal consequences if you make a knowingly false report.

In addition to protection provided to the whistleblower, WithSecure provides protection also to person(s) who are suspected of having committed the Breach. Such protection includes, for instance, that such person is treated in an equal and non-discriminating manner and the consequences of the Breach are based on WithSecure's policies and the applicable laws. Such person is also granted a possibility to review and comment the alleged Breach and the relevant material.

Receiving and Initial Handling of a Report

Our Whistleblowing Channel is designed, established and operated in a secure manner that ensures confidentiality of your identity and any third party possibly mentioned in your report. Access to your report is prevented from persons who are not authorized to receive and handle the reports.

In order to create a credible channel for filing whistleblowing reports, to ensure objectivity of handling of reports and to avoid the possibility that the report would be handled by a person somehow connected to the reported Breach, WithSecure has chosen to use the following third-party service providers to provide and maintain the Whistleblowing Channel:

(a) Lantero AB, a professional provider of whistleblower systems; and

(b) HH Partners Attorneys-at-law Ltd. acting as initial handler of the whistleblowing reports

(jointly **Service Provider**).

Due to this chosen third party service provider arrangement the persons who are authorized to receive and perform the initial handling of your report are impartial, independent and professional.

All whistleblowers will receive confirmation of receipt of their reports as soon as their reports have been received and at the latest within seven (7) days of delivery of their reports. Please note that only those who have provided their email address when submitting the report will receive a notification of this by email. Others are responsible for checking the status of their report via the link provided when submitting the report.

The persons authorized to receive and handle the reports may also request further information from whistleblowers through the Whistleblowing Channel. You as whistleblower are not obliged to provide further information, however, this would be highly appreciated. Please note that only those who have provided their email address when submitting the report will receive a notification of this by email. Others are

responsible for checking the status of their report via the link provided when submitting the report.

Whistleblowers will receive feedback concerning their reports within three (3) months from the confirmation of receipt. Feedback means information on the follow-up actions envisaged or taken by WithSecure and the grounds for the choice of those follow-up actions. Please note that WithSecure may be unable to disclose details in its feedback, especially due to possibly applicable mandatory legal requirements. Again, please note that only those who have provided their email address when submitting the report will receive a notification of this by email. Others are responsible for checking the status of their report via the link provided when submitting the report.

Internal Handling of Report

After your report has been initially received and handled by the Service Provider, the Service Provider may further report the case to at least one of the chosen representatives of WithSecure. The report will be treated as confidential in accordance with this Policy. The chosen representatives are:

- Head of People Operations & Culture;
- Chief Financial Officer;
- Data Protection Officer;
- Chief Legal Officer;
- Chief Executive Officer; and
- Chairman of Board of Directors and/or other member of Board of Directors, if necessary.

The Service Provider will make the decision whether the report is further investigated and to whom such report is then delivered with the objective that there cannot exist any conflict of interest between the chosen representative of WithSecure, you and the person(s) mentioned in your report or related the possible Breaches mentioned in your report.

The chosen representative(s) of WithSecure will decide on the required further investigations and actions to be taken by WithSecure. All such investigations and possible follow-up actions will be performed diligently and by preserving confidentiality. In case criminal activity is revealed, WithSecure will report it to the police.

The Audit Committee will also receive regular reports on the whistleblowing process, including statistics and information on a general level on the reported topics, and depending on the case, may be involved in reviewing individual cases when it is deemed necessary.

Data Protection

Data protection legislation is applied in relation to our Whistleblowing Channel.

The collected data depends on the information you have chosen to provide in connection with filing of your report. The collected data can be divided to content data, system data, your name and email address. The content data includes the content of your report and timing of your report, excluding your name and email address. The system data includes technical logs on the usage of the Whistleblowing Channel, excluding your name and email address.

Data is handled for the purposes of managing the Whistleblowing Channel, processing reports and proving fulfilment of legal requirements. In case a report leads to further inquiry, the related content data is passed on to the inquiry. The legal basis for processing the data is law and our legitimate interests.

The content data is recorded. Content data shall be stored for no longer than it is necessary and proportionate in order for WithSecure to comply with its applicable legal requirements. The retention period is based on whether the applicable legal grounds persist. The applicable legal grounds are: proving compliance until the relevant limitation of time has passed, submitting complaints/information to relevant authorities and managing possibly arising legal processes. In case there is an on-going inquiry or legal case when the retention period would be exceeded, the retention period will be prolonged to the end of the inquiry and any legal case.

The system data will not be part of the stored content data, and system data will be deleted when the processing of your report in the Whistleblowing Channel system ends. Typically, this happens when you are informed of the follow-up actions taken by WithSecure, which normally happens within three (3) months of your initial report.

Your name and email address, if you have disclosed your identity, will be deleted together with the system data, which normally happens within three (3) months of your initial report. In other cases, your name and email address are deleted once there is no longer any need to process the name or email address. That may be in connection with deleting the system data, or later, depending on case-by-case appraisal on a need to process basis. At the latest, your name and email address will be deleted when content data is deleted.

See our internal data protection policy at Human resources personal data records. WithSecure has conducted a data protection impact assessment as required by the applicable whistleblowing legislation.

Raising concerns about Actions taken by WithSecure

If you are concerned that:

- you may be, are being, or have been subjected to retaliation;
- there has been a disclosure of your identity contrary to this Policy; or
- your report has not been handled in compliance with this Policy;

we kindly ask you to proceed as follows.

Kindly send a new report to Whistleblowing Channel with a clear reference "*Concerns about Actions taken*". The Service Provider will after receiving such report make the decision to whom the report is delivered with the objective that there cannot exist any conflict of interest between the chosen representative of WithSecure and you. The chosen representatives are defined above in this Policy. Also, as explained in section "Offered Protection**"**, you have in certain situations also right to report the matter using other external channels besides WithSecure's Whistleblowing Channel.

Please note that by choosing to keep your identity confidential in the situation where you are concerned that you may be, are being, or have been subject to retaliation, WithSecure may not be able to investigate and respond to the suspected retaliation against you as effectively as WithSecure would like to.