**Whistleblowing Policy**

**Background and Applicability of Policy**

People who work for or are otherwise in professional contact with a company are often the first to become aware of breaches directed to, involving or taking place in the operations of such company. By reporting breaches of law harming the public interest, such persons act as "*whistleblowers*" and in that way play an important role in detecting and preventing harmful breaches of law. However, potential whistleblowers are often discouraged from reporting their concerns for fear of retaliation.

Largely for these reasons, European Union has passed legislation, namely the so-called Whistleblowing Directive (EU) 2019/1937 (**Directive**), to set EU-wide minimum standards for the effective protection of whistleblowers reporting breaches of particularly important EU-level legislation. In turn, the EU member states have implemented these minimum standards in their national laws. In Finland the implementation has been carried out by passing so-called Whistleblowing Act i.e. "*Laki Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta*" (**Act**) (Directive and Act are jointly referred to as the **Legislation**).

This Policy and WithSecure's Whistleblowing Channel have been prepared in accordance with Legislation. This Policy applies to and our Whistleblowing Channel is used by both WithSecure Corporation (having its principal place of business in Finland) and also other legal entities in the same group of companies (also having their principal place of business outside Finland) (jointly **WithSecure**). In case of legal entities having their principal place of business outside Finland also the other applicable national mandatory legislation is complied with in receipt of and handling of the reports received through the Whistleblowing Channel.

**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.

**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)**. The Breaches to be reported do not include 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.

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. 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 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**

Under the Legislation persons eligible to act as whistleblowers, submit a report concerning WithSecure and to whom protection is provided both by WithSecure and in accordance with the Legislation are for instance all persons who have acquired information on Breaches within work or in work-related context while being in a following position at WithSecure: employee, director, self-employed person, agency worker, volunteer worker, trainee, shareholder who plays an active role within WithSecure, member of board of directors or administrative board, or managing director of WithSecure. The above-mentioned covers also persons who have acquired the information during the negotiations preceding the work referred to above or during such work that has subsequently ended (such as job applicants and former employees). The 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.

In addition to persons eligible to act as whistleblowers, submit a report concerning WithSecure and to whom protection is provided in accordance with the Legislation, WithSecure accepts reports concerning WithSecure also from employees and directors of customers, contractors and suppliers of WithSecure, handles such reports and itself offers the protection to such whistleblowers in accordance with this Policy. Please note, however, such whistleblowers beyond the scope of the Legislation will not be entitled to any other protection under the Legislation.

**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 will 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 persons designated to receive and handle your report ("**Handlers**").

*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 and to see any follow-up questions the Handlers may

have had. You cannot be identified through this link. The link is provided 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 Handlers 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 submit a report to the Whistleblowing Channel without disclosing your name, identity or providing your email address at all. In this case the Handlers 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 Handlers, 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 WithSecure's 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 Handlers will receive this information. The Handlers will keep your name and identity confidential unless they are entitled to or authorized under the Legislation to disclose the information (e.g. if the information needs to be provided to the police or other authorities) or if 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.

As a whistleblower you have the right to be informed in advance if your identity will be disclosed, unless such disclosure would obstruct the purpose of assessing the accuracy of the report, preliminary judicial investigation or litigation.

**Offered Protection**

You will receive protection against retaliation, i.e. negative consequences, threats and attempts of retaliation that may result from your report:

- if you are eligible whistleblower as specified above in this Policy; and

- if you have reasonable grounds to believe that the information you report is true and falls within the scope of the Breaches at the time of reporting; and

- if you have reported the Breach in accordance with the so called three-step system. In order to comply with the three-step system you must primarily use WithSecure's Whistleblowing Channel to report the Breach.

In addition, if you are employed by WithSecure at the time of reporting, please note that in order to comply with your statutory duty of loyalty towards WithSecure as your employer, you must primarily use WithSecure's Whistleblowing Channel to report Breaches (first step in the three-step system).

However, you do not need to use WithSecure's Whistleblowing Channel to get protection if:

- you are not provided an opportunity to report through WithSecure's Whistleblowing Channel; or

- you have reasonable grounds to believe that WithSecure has not taken actions required primarily within three (3) months from the receipt of your report e.g. WithSecure has not provided you any follow-up on the actions performed primarily within three (3) months from the receipt of your report; or

- you have reasonable grounds to believe that WithSecure is not able to intervene efficiently with the Breach e.g. when using our Whistleblowing Channel could endanger the investigation of the Breach or the Breach requires urgent action to protect, for example, human life, health or safety or the environment; or

- you have reasonable grounds to believe that you run the risk of retaliation due to your report e.g. the object of your report has started to threaten you with retaliation already when you are preparing your report.

In such situations you are also entitled to report the Breach through the public channel provided by the authority (in Finland the Office of the Chancellor of Justice is responsible for maintaining centralized channel) and still receive protection (second step of the three-step system). When using the public channel, you cannot file your report anonymously. Note that this reference to public means specific public whistleblowing channel maintained by an authority (in Finland the Office of the Chancellor of Justice or other regulated authority), not public disclosure of information to the general public, such as online or to newspapers (this is only the third possible step of the three-step system and thus primarily the last alternative).

The public disclosure of information to the general public is justified only in rare situations. Such situation may be at hand e.g. if you have reasonable grounds to believe that Breach can with a high probability cause immediate danger to general interests such as to people's life or health (such as a Breach related to nuclear and radiation safety). For avoidance of doubt, contacting your trade union regarding issues related to your employment or requesting legal assistance from your trade union lawyer in relation to reporting procedure is not deemed as general disclosure of information to the general public.

Please note that you are not obliged to first report through our Whistleblowing Channel or through the public channel provided by an authority in order to receive protection if you report Breach directly to EU institution or body.

In short the protection provided to you includes:

- identity protection; and

- protection from retaliation and possible reversal of the burden of proof in the handling of claim related to retaliation in the courts and other authorities; and

- possible compensation and remedies e.g. due to retaliation; and

- possible protection against civil, criminal and administrative liability.

Please note that you do not need to prove your suspicions or allegations correct. If you have been eligible whistleblower, you have had reasonable grounds to believe that the matters reported by you are true at the time of reporting and fall in within the scope of Breaches and you have complied with the three-step system, 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. Please also note that no protection is available if you report on information that has already been published.

Filing a knowingly false report is a breach of 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 such as obligation to pay damages.

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. Further, such persons may be entitled to compensation due to deliberate false report.

**Receiving and Initial Handling of Report**

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

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 Handlers of 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 primarily 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.

All received reports are recorded in the case management register or registered otherwise.

WithSecure has unilateral right to decide on the change of the Service Provider to another service provider by informing on such change.

**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 two (2) Handlers of WithSecure. The report will be treated as confidential in accordance with this Policy. The chosen representatives at WithSecure Corporation are:

- Chief People Officer;
- 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.

Since this Policy and the Whistleblowing Channel cover all legal entities in WithSecure group of companies, in addition to persons listed above, each affiliated legal entity has appointed its own representatives (acting in same or similar position as the ones listed above) to act as representatives of such legal entity. The Service Provider will take into consideration as to which legal entity the report concerns when deciding the correct to whom information related to the report will be delivered.

The Service Provider will make the decision whether the report is further investigated and to whom at WithSecure 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.

WithSecure reviews the performance, expertise, experience and impartiality of the Handlers on a regular basis and has unilateral right to change these Handlers merely by informing on such changes. WithSecure has unilateral right to decide on qualification requirements as well as scope of

the tasks and powers of the Handlers. The Company also has unilateral right to decide on changes to these merely by informing on the changes.

**Data Protection**

The Whistleblowing Channel is subject to data protection legislation. Please see WithSecure's Privacy Notice for Whistleblowing Channel. WithSecure has conducted a data protection impact assessment as required by the Legislation.

**Raising concerns about Actions taken by WithSecure**

If you are concerned that:

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

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 WithSecure's chosen representative and you. Also, as explained in section "Offered Protection", you have in certain situations also right to report the matter using specific public whistleblowing channel provided by authorities or even publish your information.

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.

**Informing and Training**

WithSecure will provide information and training related to the Whistleblowing Channel as and to the extent deemed necessary by it. WithSecure has a unilateral right to choose the way of organizing the informing and training. WithSecure may for instance choose to organize informing and training by internal training, by a website or by using outside service provider.

**Security of the Whistleblowing Channel**

WithSecure and its Service Provider are committed to monitor the information security of the Whistleblowing Channel on a regular basis in accordance with the Legislation.

**Amendments**

WithSecure reserves the right to amend and change this Policy unilaterally at any time excluding such matters for which cooperation negotiations are required under the applicable mandatory laws.