

**Contents**

Introduction..... 2

Who can use the Whistleblower channel?..... 2

What is covered ? ..... 3

When to report a concern?..... 4

How to report a concern?..... 4

    Regular reporting lines ..... 4

    Internal reporting channels..... 4

    Whistleblower channel..... 5

    Reporting externally..... 6

How are concerns reported to the Whistleblower channel dealt with? ..... 6

    Process..... 6

    Anonymity & Confidentiality..... 7

    Protection of personal data..... 7

    Non-retaliation & Protection against unfair treatment..... 8

    Recording & Management reporting ..... 9

## Introduction

Imec is a world-leading research and innovation hub in nanoelectronics and digital technologies, headquartered in Leuven, Belgium.<sup>1</sup> We are committed to conduct our activities based on our corporate values of integrity, connectedness, passion and excellence, thereby respecting relevant laws and regulations. Those values define how we treat each other at imec, but also what behavior is expected from and towards our customers and partners, and towards the broader community. These values and expectations have been translated more explicitly in imec's internal Ethics Code of Conduct ("Ethics Code")<sup>2</sup> and the Code of Conduct for imec's business partners ("Business Code")<sup>3</sup>.

Despite this commitment, you may observe conduct that possibly violates a law or regulation, the Ethics Code, the Business Code, or imec's policies and procedures. If you observe or suspect any misconduct, you are strongly encouraged to raise your concern internally through the regular reporting lines and internal reporting channels. However, if this is not possible or if you don't feel comfortable in doing so, you can use the Whistleblower channel. By doing so, you give imec the opportunity to correct or deal with the situation pro-actively. Any concerns reported will be treated confidentially and, if desired, anonymously and you will not be retaliated against for raising concerns in good faith about suspected misconduct.

The purpose of this policy ("Policy") is to explain when and how you can report a concern. It also describes what you may expect from imec and what steps will be taken after you report a concern.

## Who can use the Whistleblower channel?

The Policy is applicable to all imec employees and everyone who carries out work for or on behalf of imec worldwide (including contractors, consultants, students and postdocs).

The Whistleblower channel is also available to any person with whom imec has or has had an involvement or business relationship (such as former employees, business partners, suppliers, and stakeholders in general) and wishes to raise a concern about possible misconduct within imec.

For employees of imec entities<sup>4</sup> that are located in jurisdictions where, further to local regulations, a specific whistleblowing or speak up policy has been implemented, such specific policy shall prevail over this Policy and must be adhered to.

For employees of imec Belgium, this policy shall be read in conjunction with the Belgian law of 28 November 2022<sup>5</sup> implementing the European Directive (2019/1937) of 23 October 2019 on the protection of persons who report breaches of Union law (the "Whistleblower Law"). The provisions of the Whistleblower Law shall be supplementary to this policy for situations that are not explicitly mentioned herein. In case of discrepancies between this policy and the Whistleblower Law, the law shall prevail.

---

<sup>1</sup> Imec consists of distributed R&D groups at several Flemish universities and has affiliates and offices in the Netherlands, USA, China, India, and Japan. Reference to "imec" in this policy means the imec group except where otherwise indicated.

<sup>2</sup> For employees, the Ethics Code can be consulted at the Employee Center.

<sup>3</sup> The Business Code can be consulted at the imec website ([www.imec-int.com](http://www.imec-int.com)).

<sup>4</sup> Specific policies are currently in place for employees located in the Netherlands and in the USA.

<sup>5</sup> "Wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector, B.S. 15 december 2022"

## What is covered ?

The Policy should only be used to report concerns about suspected misconduct within imec with respect to any (possible) violation of

- laws and regulations
- the Ethics Code
- the Business Code
- imec policies and procedures.

Examples of concerns that can be reported using this policy are:

- disclosure of confidential information
- improper use of company resources
- irregularities of a financial nature, including concerns regarding (questionable) accounting controls and auditing matters, or inadequate financial or non-financial recordkeeping
- irregularities in procurement
- violations of regulations to prevent money laundering and terrorist financing
- fraud and fraudulent (financial) reporting, including tax and social fraud and tax evasion
- discrimination or (sexual) harassment
- conflicts of interest
- violations of regulations and policies to protect privacy and personal data
- issues related to information security
- bribery and corruption
- breaches of competition law and state aid regulation
- environmental, health and safety issues, including product safety, food safety, public health, nuclear safety and animal welfare.

This Policy should NOT be used:

- for issues or grievances you may have in relation to HR related matters (e.g. your terms of employment or performance related issues)<sup>6</sup>
- for events presenting an immediate threat to life or property<sup>7</sup>
- to settle personal disputes
- to make accusations with malicious intent, which you know are false or that cannot be substantiated; and
- to obtain answers to questions or to provide comments on imec policies/procedures or interpretation of their applicability<sup>8</sup>.

---

<sup>6</sup> For HR related matters, your direct manager and/or your HR business partner are the primary points of contact.

<sup>7</sup> Imec has a Crisis Management Plan in place covering crisis situations. Contact [crisis@imec.be](mailto:crisis@imec.be)

<sup>8</sup> You should contact the relevant internal owner for policy/procedure related questions.

## When to report a concern?

We encourage you to report a concern as soon as possible, ideally when the potential misconduct can still be prevented, or a situation escalates.

If you know about or suspect misconduct, report your concern with the facts that are known to you. We do not expect you to have all the answers and ask you to never start investigating any concern yourself. There are various options for support and advice available within our organization, as listed below.

By reporting internally, you enable imec to carefully investigate the matter, take appropriate action if necessary, and give you the support needed.

It should be noted that no disciplinary measures will be taken against you if your genuine and good faith concern turns out to be unfounded.

## How to report a concern?

If you suspect any misconduct, imec encourages you to address this directly with the person(s) involved.

If this is not possible or you do not feel comfortable in doing so, you can raise questions and concerns either through the regular reporting lines, through one of the available internal reporting channels or through the Whistleblower channel established as part of this Policy.

### Regular reporting lines

This Policy does not replace imec's regular reporting lines. The first person for an imec employee to approach when raising a concern is his/her direct manager.

If this is not possible or you do not feel comfortable doing so, please feel free to raise questions to any of the available internal reporting channels described below.

If you are not an imec employee (i.e. supplier, customer etc.), you can contact your imec contact person. If this is not possible or you do not feel comfortable doing so, you can use the Whistleblower channel.

### Internal reporting channels

Imec has established several internal reporting channels to provide support and guidance on how to address or solve a problem, such as your HR business partner, the persons of trust or the external prevention advisor. They can be contacted to intervene depending on who is reporting an issue, on the subject and the sensitivity.<sup>9</sup>

If you have concerns related to specific areas of compliance, such as privacy, information security, export control regulation or environment, health & safety, you can always contact the competent department or compliance officer.<sup>10</sup>

---

<sup>9</sup> For employees, more information on the specific reporting channels at every entity of the imec group can be found on the Employee Center, e.g.

- US: Unlawful Harassment and Discrimination
- Belgium: Talking through problems with the right person

<sup>10</sup> For employees, contact details can be found on the Employee Center.

Issues related to research integrity can be addressed to the Commission on Scientific Integrity of imec. The Commission on Scientific Integrity<sup>11</sup> is responsible for overseeing imec's policy on research integrity.

The Ethics Commission<sup>12</sup> can be directly approached in the following circumstances:

- If you need assistance in discussing and resolving ethics questions and issues regarding acceptable conduct;
- If you need help when in doubt about compliance with or interpretation of the Ethics Code;
- If you believe that ethics and compliance issues are not being resolved;
- If you do not feel comfortable reporting through other channels.

### Whistleblower channel

In case you suspect misconduct and genuinely believe that the matter cannot be dealt with directly or through the regular reporting lines or any of the above channels or you do not feel comfortable doing so, you can use the Whistleblower channel. This gives you the opportunity to report concerns confidentially, and if necessary, anonymously. It should be noted that concerns reported anonymously are more difficult, and in some circumstances even impossible, to be adequately investigated.

Imec has appointed the Corporate Legal Counsel, the VP Human resources and the Enterprise Risk Officer as Reporting Officers<sup>13</sup> who are responsible for managing the Whistleblower channel by:

- receiving Concerns<sup>14</sup> from and communicating with the Reporter<sup>15</sup>
- conducting or instructing an investigation; and
- consulting and providing information to other persons on a strict 'need to know' basis (the "Authorized Persons").

Concerns can be addressed to the Reporting Officer in person, by letter<sup>16</sup> or by e-mail. It is also possible to ask a Reporting Officer for advice before formally reporting a Concern.

- Address: imec, to the attention of the Reporting Officer, Kapeldreef 75, 3001 Leuven, Belgium
- E-mail: [Whistleblowing@imec.be](mailto:Whistleblowing@imec.be)

The Reporting Officers shall inform and consult each other on each Concern they receive.

To adequately assess and investigate your Concern, please provide as much detailed information as possible, such as:

- the background, history and reason for the Concern;

---

<sup>11</sup> For employees, more information about the Commission on Scientific Integrity and the related policy can be found on the Employee Center.

<sup>12</sup> For employees, more information about the Ethics Commission can be found on the Employee Center.

<sup>13</sup> When written with a capital letter in this Policy, Reporting Officer shall also refer to the "meldingsbeheerder" as defined in the Whistleblower Law.

<sup>14</sup> When written with a capital letter in this Policy, Concern shall refer to a concern that has been formally submitted through the Whistleblower channel regardless of the concern is substantiated or will be further investigated, also referred to as "interne melding" in the Whistleblower Law.

<sup>15</sup> When written with a capital letter in this Policy, Reporter shall refer to the person who has submitted a Concern through the Whistleblower channel, also referred to as "melder" in the Whistleblower Law.

<sup>16</sup> If reported by letter, the envelope should be labeled as follows to indicate confidentiality: "To be opened by the Reporting Officer only. Being submitted pursuant to the imec Whistleblower policy"

- names, dates, places and other relevant information;
- any documents that may support your Concern.

A Concern can only be followed up if it contains sufficient information and there is a reasonable possibility of obtaining further information.

If the Concern relates to a Reporting Officer, you can report the Concern by sending a letter<sup>17</sup> to imec, to the attention of the Chairman of the Audit Committee, Kapeldreef 75, 3001 Leuven, Belgium.

### Reporting externally

Anyone raising a concern related to suspected misconduct should first report internally to any of the above channels. Only if this is not reasonably possible, reporting directly to a law or regulatory enforcement authority or thereto founded (semi) public authority could be an option.

## How are concerns reported to the Whistleblower channel dealt with?

### Process

#### Acknowledgment and information

The Reporting Officer must acknowledge receipt of the Concern to the Reporter and inform him/her of the next steps within 7 calendar days after the date of receipt.

The Reporting Officer must inform the Reporter whether the Concern is in scope of this Policy and, if so, about the next steps. This information specifically includes provisions regarding confidentiality, anonymity, protective measures and the processing of (personal) data.

In case the Reporter reported anonymously, the above cannot be reasonably expected from the Reporting Officer.

The Reporting Officer must inform the CEO about the receipt of a Concern, without disclosing the identity of the Reporter. If the CEO or a member of the Executive Board is the subject of the Concern, the Chairman of the Audit Committee must be informed instead of the CEO.

On a regular basis, the Reporter may request the Reporting Officer to provide him/her with an update by providing a general status report on the progress of the investigation, but not on the details of the investigation itself. The Reporting Officer can decide to refrain from providing an update on or certain details of the investigation, for example if the Reporting Officer believes that such information is confidential or could hinder the Investigation.

#### Preliminary investigation

If the reported Concern is in scope of this Policy, the Reporting Officer must perform a preliminary investigation to determine whether there are reasonable facts and/or circumstances to conclude that the reported Concern is sufficiently grounded.

Cooperation by employees, including members of (senior) management, is mandatory. The Reporting Officer may involve additional Authorized Persons when necessary. If the preliminary investigation indicates that the CEO or a member of the Executive Board is the subject of the Concern, the Reporting Officer must consult with the Chairman of the Audit Committee.

The preliminary investigation must be concluded, and the Reporter must be informed of the outcome thereof within 21 calendar days of the date of acknowledgment of the receipt of the reported Concern.

---

<sup>17</sup> The envelope should in this case be labeled as follows : “To be opened by the Chairman of the Audit Committee only. Being submitted pursuant to the imec Whistleblower policy.”

## Full investigation

If the reported Concern is sufficiently grounded, the Reporting Officer will advise the CEO to request a full investigation. If the CEO or a member of the Executive Board is the subject of the Concern, the reporting Officer will advise the Chairman of the Audit Committee.

The full investigation will be supervised by the Reporting Officer with the assistance of Authorized Persons and can be conducted by an independent party depending on the nature of the Concern.

Cooperation by employees, including members of (senior) management, is mandatory.

The full investigation must be concluded, and the Reporter must be informed of the final conclusions within 90 calendar days of acknowledgment of the receipt of the reported Concern.

## Anonymity & Confidentiality

The Reporting Officer and all other Authorized Persons must protect the identity of everyone involved in the Whistleblower process and other details of the Concern, as well as the details of an investigation, by sharing this information only on a strict 'need to know' basis.

An exception to the confidentiality principle is when imec is legally required by applicable law or regulation to disclose information related to a Concern, including the Reporter's identity and/or the identity of the accused person(s), to an external party who is legitimately authorized.

You can help us protect confidentiality by being discrete about the matter and not discussing your Concern with your colleagues or anyone else.

You can share your concerns anonymously when allowed by the laws or regulations of your country. We do however encourage you to reveal your identity as it is more difficult, and in some circumstances even impossible, for the Reporting Officer to adequately investigate Concerns that are made anonymously or to continue the dialogue with the Reporter.

## Protection of personal data

Imec is committed to protect the privacy of everyone involved in the Whistleblower process. We will take adequate measures to safeguard personal data from unauthorized access and processing. Any personal data obtained as part of this Policy will be processed in line with the imec privacy policy<sup>18</sup> and will only be used for the purposes explained in this policy, to comply with the law, or because of an important public interest.

Any personal data involved shall be processed confidentially and separated from employee files or information systems managing employee information.

Personal data related to Concerns that have been found unsubstantiated shall be removed within 30 calendar days after the Reporter has been informed that the Concern has been defined unsubstantiated.

Personal data relating to Concerns<sup>19</sup> about substantiated claims will at least be kept for the duration of the contractual relationship with the Reporter. If no contractual relationship exists (anymore), the data will be removed within thirteen months after the verification work of the investigators is completed, unless the investigators conclude that the Concern constitutes a breach of the law or disciplinary measures are taken.

---

<sup>18</sup> For employees, this policy can be consulted at the Employee Center.

<sup>19</sup> These data are name, function and contact details of the Reporter, everyone who is the subject of protective measures further to this Policy as well as the accused person(s).

If the Concern constitutes a breach of the law, the data will be kept until the later date of the expiration of the legal limitation period or the completion of the court proceedings (in highest instance). If disciplinary measures are taken, the data will be removed within thirteen months after the disciplinary measures have been completed.

### Non-retaliation & Protection against unfair treatment

Imec strictly prohibits retaliation against an employee who reports a Concern in good faith (either to the Whistleblower channel or directly to relevant governmental/regulatory authorities) if such retaliation can be linked to the fact that the employee has reported such Concern. Such prohibition also includes any attempt to or threatening with retaliation. Retaliation is also prohibited against an employee who provides information in an investigation under this Policy. Examples of retaliation are dismissal, early termination of a temporary contract, or failure to renew a contract.

Imec shall not treat an employee unfairly in connection with a Concern in good faith. Unfair treatment means taking any measure which can be linked to the fact that the employee has reported a Concern, having a negative effect on the employee. Such unfair treatment is also prohibited against an employee who provides information in an investigation under this Policy.

Examples of such measures are:

- compulsory appointment to another position
- extending or limiting employee's duties, except at employee's own request
- refusing a request by employee for a move or relocation
- changing employee's workplace or refusing a request to do so
- withholding a salary increase, incidental remuneration, bonus, or the award of allowances
- withholding opportunities for promotion.

Unfair treatment also applies if there are reasonable grounds to speak to the employee about his/her performance or to take a measure with a negative effect against the employee, but the measure taken by imec is disproportionate to those grounds.

If imec proceeds to take a measure with a negative effect against the employee within a short period following a Concern being made in good faith, imec shall give justification as to why the measure is considered necessary and why this measure is not connected with the Concern in good faith.

Imec shall ensure that the employee's manager(s) and colleagues refrain from any form of unfair treatment in connection with the Concern in good faith that interferes with the employee's ability to function either professionally or personally. Examples of such unfair treatment are:

- bullying, ignoring, and excluding the employee
- making unfounded or disproportionate allegations about employee's performance;
- intimidating the employee by threatening to take specific measures or actions if he/she proceeds with the Concern.

Anyone who suspects to have been retaliated against or treated unfair in violation of this Policy further to a Concern made in good faith must report this immediately to the Reporting Officer. The Reporting Officer may consult with one or more Authorized Persons on the next steps.

In case of unfair treatment this may include giving warning or take disciplinary measures against the colleagues who treated the employee unfair.



## Recording & Management reporting

The Reporting Officer must maintain a record of all activities, reports and information received pursuant to this Policy. Such records may include initial contact reports, transcripts from meetings and verbal conversations about the (suspected) Concerns and all facts from an investigation.

All records related to a reported Concern must be classified and handled as 'Strictly Confidential', in accordance with imec's Information Security Policy<sup>20</sup>.

The Reporting Officer provides an annual report to the Audit Committee and the Work Council of imec Belgium<sup>21</sup>. This report shall contain the following information:

- the total number of Concerns reported;
- the number of Concerns that have led to a preliminary investigation;
- the number of Concerns that have been fully investigated;
- the number of Concerns that have been found justified and triggered specific actions.

---

<sup>20</sup> For employees, this policy can be consulted at the Employee Center.

<sup>21</sup> The Work council of imec Belgium is only informed of Concerns reported under this policy related to the activities and employees of imec Belgium.