INCIDENT REPORTING-POLICY

AUSTRIAN INSTITUTE OF TECHNOLOGY

AIM OF THE INCIDENT REPORTING SYSTEM

AIT Austrian Institute of Technology GmbH and its full subsidiaries, LKR Leichtmetallkompetenzzentrum Ranshofen GmbH, Seibersdorf Labor GmbH and Nuclear Engineering Seibersdorf GmbH, have committed to acting with integrity and in a highly ethical manner. This is vital both for our commercial success and to uphold our national and international reputation. For that reason, the Incident Reporting System implemented at AIT in accordance with EU Directive 2019/1937 is an important tool for dealing with corrupt, illegal or other undesirable behaviour.

If you have a well-founded suspicion or are a witness to concerning incidents, we want to encourage you to use the Incident Reporting System to submit a report or query about the matter. We take all submissions seriously and will instigate steps as required to prevent similar incidents in the future.

Basic information about the Incident Reporting System
The Incident Reporting System is an external, web-based and encrypted web application. That means all the information is stored on high security servers in Germany, rather than on internal AIT servers. The system is designed so that neither the operator of the web application (BKMS®) nor AIT can determine the origin of the submitted information.

This Incident Reporting System is open to all our employees, former employees, trainees, PhD students and freelancers, and also to employees of business partners or collaboration partners.

For your protection, all processing and documentation is undertaken exclusively within the Incident Reporting System.

All submissions will be treated confidentially, and only processed by selected persons who have received special training and are subject to additional secrecy obligations.

The Incident Reporting System is not intended for submitting suggestions for improvement or error reports, nor for the deliberate dissemination of misinformation, and may not be misused for this purpose.

Submitting a report or query

The Incident Reporting System will guide you through the reporting process.

You may enter information or a query into the Incident Reporting System either under your own name or anonymously.

Reporting information or submitting a query is permitted when these are relevant to the categories covered by the Incident Reporting System and are submitted in good faith. That means you must have sufficient reason to believe that the reported information or query is based on solid facts.

Processing your report or query

After your report has been received it will first be assessed to determine whether the information is admissible or is relevant to the specified categories.

If you have submitted your report anonymously but the information provided enables you to be identified, the information will be further anonymised, or pseudonymised. Correspondingly, according to the need-to-know principle, the same steps will be taken where the report specifies persons or information not relevant to the issue.

You will receive confirmation of receipt of the report within seven calendar days after submission if you have set up a secure mailbox.

You will receive an update on the progress of the investigation or of the measures which have been taken within three months at the latest. If, after three months, the report is still being processed, you will be informed once again when the investigations have been concluded and appropriate measures have been taken.

Monitoring

The Internal & Technical Auditing unit regularly checks that reports are being processed correctly.

Your protection

You will be granted protection under Chapter VI of the EU Directive if:

a) the report submitted is permissible;
b) the report has been submitted internally via the AIT Incident Reporting System in accordance with Article 7 of the EU Directive or externally in accordance with Article 10
c) the report concerns a case specified in Article 2 of the EU Directive.

This protection also applies to third persons that are connected with you and may suffer retaliation in a work-related context, e.g. colleagues or relatives.

You will also be granted protection when submitting reports or queries on the specified additional categories or national matters concerning a case specified in c) which are outside the scope of the EU Directive.