INCIDENT REPORTING-POLICY

ZIELE DES INCIDENT REPORTING SYSTEMS

Die Seibersdorf Labor GmbH, eine 100%-Tochtergesellschaft der AIT Austrian Institute of Technology GmbH, verpflichtet sich in ihrem Tun und Handeln zu höchster Ethik und Integrität. Dies ist sowohl für den unternehmerischen Erfolg als auch für die Wahrung der nationalen und internationalen Reputation entscheidend. Daher ist das gemäß der EU-Richtlinie 2019/1937 im AIT Konzern eingeführte Incident Reporting-System ein wichtiges Werkzeug im Umgang mit korruptem, illegalem oder anderem unerwünschten Verhalten.

Wenn Sie einen begründeten Verdacht haben oder Zeuge von besorgniserregenden Angelegenheiten werden, möchten wir Sie ermutigen, eine entsprechende Meldung oder Frage in das Incident Reporting-System einzugeben. Wir nehmen sämtliche Eingaben ernst und leiten bei Bedarf entsprechende Schritte ein, um ähnliche Vorfälle in Zukunft zu vermeiden.

Grundsätzliches zum Incident Reporting-System
Das Incident Reporting-System ist eine externe webbasierte und verschlüsselte Webanwendung, d.h. dass sämtliche Informationen nicht auf Servern der Seibersdorf Labor GmbH oder des AIT Konzerns gespeichert sind, sondern auf Hochsicherheitsservern in Deutschland. Dieses System ist so eingerichtet, dass die Herkunft eingegebener Informationen weder vom Betreiber (BKMS®) der Webanwendung oder der Seibersdorf Labor GmbH noch im AIT-Konzern nachvollzogen werden kann.

Dieses Incident Reporting-System steht allen Mitarbeitenden, ehemaligen Mitarbeitenden, Praktikant:innen, PhD's, freien Dienstnehmer:innen, aber auch Mitarbeitenden von Geschäftspartner:innen oder Kooperationspartner:innen zur Verfügung.
Die gesamte Bearbeitung und Dokumentation erfolgt zu Ihrem Schutz ausschließlich mit dem Incident Reporting-System.

Alle Eingaben werden vertraulich behandelt und nur von ausgewählten Personen bearbeitet, die speziell geschult sind und zusätzlichen Geheimhaltungspflichten unterliegen.

Dieses Incident Reporting-System ist nicht für die Eingabe von Verbesserungsvorschlägen oder Fehlermeldungen wie auch nicht zur bewussten Verbreitung von Fehlinformationen vorgesehen und darf dafür nicht missbraucht werden.

Eingabe einer Meldung bzw. Frage

Sie werden bei der Meldung eines Hinweises oder einer Frage durch entsprechende Erläuterungen im Incident Reporting-System unterstützt.
Sie können Hinweise oder Fragen unter Angabe Ihres Namens oder anonym in das Incident Reporting-System eingeben.

Hinweise bzw. Fragen sind dann zulässig, wenn sie einen Bezug zu den Schwerpunktthemen im Incident Reporting-System haben und in gutem Glauben getätigt wurden. Damit ist gemeint, dass Sie einen hinreichenden Grund zur Annahme haben, dass der gemeldete Hinweis bzw. die Frage auf fundierten Tatsachen basiert.

Bearbeitung Ihrer Meldung bzw. Frage

Nach Eingang Ihrer Meldung wird geprüft, ob der Hinweis zulässig ist bzw. einen Bezug zu den möglichen Schwerpunktthemen hat.

Wenn Sie Ihre Meldung anonym eingegeben haben, erfolgt, falls noch Rückschlüsse auf Ihre Person möglich sind, eine weitere Anonymisierung bzw. Pseudonymisierung. Gleiches wird, entsprechend dem Need-to-know-Prinzip, auch durchgeführt, wenn in der Meldung nicht betroffene Personen genannt oder nicht relevante Informationen enthalten sind.

Innerhalb von sieben Kalendertagen erhalten Sie eine Bestätigung über den Eingang der Meldung, insofern Sie eine gesicherte Mailbox eingerichtet haben.

Spätestens nach drei Monaten erhalten Sie eine Rückmeldung über den Stand der Ermittlungen, gegebenenfalls über die ergriffenen Maßnahmen. Sollte zu diesem Zeitpunkt die Bearbeitung noch nicht abgeschlossen sein, erfolgt eine weitere Rückmeldung nach Abschluss der Ermittlungen bzw. nach Umsetzung etwaiger Maßnahmen.

Überprüfung

Die Stabsstelle „Internal & Technical Auditing“ überprüft regelmäßig die rechtmäßige Bearbeitung der Meldungen.

Ihr Schutz

Sie werden gemäß der EU-Richtlinie, Kapitel VI geschützt, wenn:

a) es sich um eine zulässige Meldung handelt;
b) diese Meldung gem. Artikel 7 der EU-Richtlinie intern über das AIT-Incident Reporting-System oder extern gem. Artikel 10, erstattet wurde;
c) es sich um einen Fall handelt, der im Art. 2 der EU-Richtlinie genannt ist.

Dieser Schutz gilt auch für u.a. Dritte, die mit Ihnen in Verbindung stehen und in einem beruflichen Kontext Repressalien erleiden könnten, wie z.B. Kolleg:innen oder Verwandte.

Sie sind auch bei Meldungen oder Fragen zu den zusätzlichen Schwerpunktthemen sowie bei nationalen Sachverhalten zu einem in c) genannten Fall im Incident Reporting-System, welche über die EU-Richtline hinausgehen, geschützt.