

Procedural instructions regarding secunet Group's whistleblowing system

| | |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version no. | 1.0 (24 May 2023) |
| Valid with effect from | June 2023 |
| Approval by the Management Board | 24 May 2023, 538. VS |
| Description of document | <ul style="list-style-type: none"> ■ These procedural instructions describe generally applicable principles for processing reports of potential grievances within secunet Group (including the human rights and environmental due diligence obligations pursuant to the German Law on Supply Chain Due Diligence LkSG). ■ This document is applicable to all secunet Group companies. |
| Scope | secunet Group |
| Policy classification | open |
| Responsibilities | Stephanie Ventz (Compliance Officer) |

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 1 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

Contents

| | |
|--------------------------------------------------------------------|----------|
| Documentation of changes | 3 |
| 1 Objectives and area of application | 4 |
| 2 Information on submitting reports and complaints | 5 |
| 2.1 Who can report a breach or complaint? | 5 |
| 2.2 Option of anonymous reporting | 5 |
| 2.3 Reporting for valid reasons | 5 |
| 2.4 What can be reported? | 5 |
| 2.5 Who is responsible for the whistleblowing system? | 6 |
| 2.6 Protection of whistleblowers | 6 |
| 3 Reporting channels | 7 |
| 3.1 In-person reports | 7 |
| 3.2 BKMS Whistleblowing System | 7 |
| 3.3 E-mail | 7 |
| 3.4 Phone | 7 |
| 3.5 Post | 7 |
| 3.6 External reporting channels | 7 |
| 4 Investigations | 8 |
| 4.1 How is the whistleblower involved in the fact-finding process? | 9 |
| 4.2 How long does the fact-finding process take? | 9 |
| 4.3 Data protection | 10 |

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 2 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

Documentation of changes

| <i>Version no.</i> <i>Date</i> | <i>Changes</i> |
|-----------------------------------|------------------------------------------------------------------|
| Version 1.0 24 May 2023 | <ul style="list-style-type: none">• First creation |

Preliminary remarks

For the sake of better legibility, masculine pronouns shall be used throughout the following when referring to persons. All statements apply equally to all genders.

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 3 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

1 Objectives and area of application

Integrity is our industry’s highest asset. Our corporate success is rooted in integrity and ethically correct behaviour. To ensure that we can live up to this claim, it is important that we learn of potential misconduct and rectify it. secunet Group’s whistleblowing system is used for receiving and processing information and complaints about potential breaches of rules or grievances within secunet Group and in the associated supply chains.

These procedural instructions describe generally applicable principles for processing reports of potential grievances within secunet Group (including the human rights and environmental due diligence obligations pursuant to the German Law on Supply Chain Due Diligence LkSG). In principle, the processes described in these procedural instructions shall apply if the reporting channels described in the “[Reporting channels](#)” section are used.

These procedural instructions reflect the applicable legal requirements for whistleblowing systems and whistleblower protection, such as the EU Whistleblower Directive 2019/1937, the Whistleblower Protection Act (HinSchG), the Supply Chain Due Diligence Act (LkSG) and the Data Protection Act (GDPR).

This document applies equally to all secunet Group companies.

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group’s whistleblowing system | | Page 4 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

2 Information on submitting reports and complaints

2.1 Who can report a breach or complaint?

All secunet employees, customers, suppliers and other third parties (e.g. directly affected persons, persons with knowledge of a (possible) breach by a direct/indirect supplier) have the possibility of contacting secunet via various channels to report breaches or submit a complaint.

2.2 Option of anonymous reporting

With the BKMS Whistleblowing System and the postal service, secunet Group provides reporting channels that enable anonymous submission of a report or complaint. Whistleblowers are nevertheless encouraged to identify themselves so that they can be contacted in case of important queries. All reports are treated seriously, regardless of anonymity.

2.3 Reporting for valid reasons

All reports must be based on valid reasons (secunet must have verifiable and credible information about a breach) that lead the whistleblower to believe that the reported facts are true (reporting in good faith). No financial benefits are offered or granted to whistleblowers.

Subject to the applicable legal system, reasonable steps may be taken against whistleblowers if it is established that they have knowingly reported false information.

2.4 What can be reported?

Generally speaking, breaches and/or grievances can be reported via the whistleblowing system if...

- the breach was committed by a secunet employee (includes breaches of statutory and internal regulations, e.g. employment contract, code of conduct, policies, etc.),
- the breach was committed by third parties (customers, indirect and direct suppliers or business partners of secunet) (includes all breaches of our Supplier Code of Conduct for Suppliers and Business Partners, including a breach of human rights and environmental due diligence obligations and the resulting risks).

Regarding these topics in particular:

- Corruption / conflict of interest
- Breaches of competition or antitrust law
- Breaches of the Data Protection Act
- Breaches of confidentiality regulations
- Breaches relating to human rights and the environment
- Other breaches of the law

Tip-offs, complaints or suspected breaches (actual or potential) can also be reported and are taken seriously.

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 5 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

2.5 Who is responsible for the whistleblowing system?

The central unit responsible for secunet Group’s whistleblowing system is the Corporate Compliance department. The persons entrusted with managing the whistleblowing system guarantee impartiality, are independent and are obliged to maintain confidentiality.

As a rule, the Compliance Office is responsible for accepting all reports and complaints. This department documents the receipt and content of the report or complaint and handles the report.

Information on rule breaches and complaints are treated in strict confidence and are only communicated to the necessary group of people on a need-to-know basis.

Whistleblowers have the option of making a report to the compliance officer of their respective company. The Corporate Compliance department is notified of each report and is authorised to access the report for the purposes of carrying out the necessary investigation and documentation. The respective company remains primarily responsible for responding to the reported information or complaint.

2.6 Protection of whistleblowers

The identity of the whistleblower is protected with the utmost care. secunet Group safeguards the interests of the whistleblower by providing a secure whistleblowing system and ensuring that all information received is treated confidentially.

The investigations are carried out fairly and with respect for all parties concerned following an objective and transparent procedure without any bias. The “presumption of innocence” applies to all internal investigations.

secunet Group prohibits and does not tolerate any form of retaliation (e.g., adverse action, disciplinary action, threats, intimidation) for reporting a breach in good faith or otherwise cooperating with an investigation into a breach.

Knowingly reporting false information constitutes an offence. Measures taken as a result of such a report are not retaliatory measures.

In its investigations, Corporate Compliance endeavours to protect the legitimate interests of other persons affected by a disclosure. Raising suspicions about another person can have serious consequences.

It is important that the whistleblowing system is used responsibly. secunet Group will not support any actions that could cause employees to become victims of unfounded or false accusations.

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group’s whistleblowing system | | Page 6 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

3 Reporting channels

Every breach and every complaint should be reported via one of the following reporting channels in order to ensure that the Corporate Compliance department is made aware of it and that whistleblowers are adequately protected.

3.1 In-person reports

Information and complaints can also be reported to the relevant line manager. However, there is no obligation to notify one's line manager.

Alternatively, information and complaints can also be reported to the Compliance Office in person.

3.2 BKMS Whistleblowing System

Information and complaints can be reported via the electronic whistleblowing system (BKMS). This system is confidential and secure. There is also the option of making an anonymous report. A report can be made in German or English.

secunet Group's BKMS Whistleblowing System can be accessed via the following link: <https://www.bkms-system.com/secunet>

3.3 E-mail

Information and complaints can also be reported to the Corporate Compliance department by e-mail at compliance@secunet.com.

3.4 Phone

You can also make a report by calling the following telephone number: +49 201 54541224

3.5 Post

The postal service can also be used for reporting information or complaints. Please use the following postal address:

Postal address:
secunet Security Networks AG
 Chief Compliance Officer
 Personal/confidential
 Kurfürstenstrasse 58
 45138 Essen, Germany

3.6 External reporting channels

We encourage all whistleblowers to report breaches via the secunet whistleblowing system. There are also optional external reporting channels that are operated by the relevant authorities.

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 7 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

4 Investigations

We address all reports of breaches or complaints by conducting internal investigations using transparent and clearly defined processes. In this way, we ensure that our internal standards are rigorously applied and that our board members and managers live up to their legal and corporate responsibilities. Our investigations are always carried out in compliance with all applicable laws and regulations.

The report is handled in German or English. This also applies to communication with the reporting person. The entire investigation process from receipt of a report right through to the outcome of the investigation is described below:



Once the report or complaint has been received, it is documented internally by the Compliance Office. The whistleblower will receive a confirmation of receipt within seven days of receipt of the report. The next step is for the Compliance Officer to assess the plausibility and validity of the report and investigate whether there are sufficient grounds to believe that a breach of regulations has occurred or is occurring, or whether any relevant risks pursuant to the LkSG may exist. They also check whether sufficient information is available to investigate the matter further and, if necessary and possible, contact the whistleblower to request further information.

If the information does not indicate a breach of rules or a violation of human rights and environmental due diligence obligations, or if there is not enough information available, the case is closed and the whistleblower is informed if their contact details are known.

The Corporate Compliance department conducts further investigations internally, if necessary with the involvement of additional stakeholders, to clarify the facts. In this case,

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group’s whistleblowing system | | Page 8 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

the potentially affected party will be informed immediately and given the opportunity to comment as early as possible.

Depending on the criticality of the matter, preventive and corrective measures may be established in order to appropriately address the breach identified. These may include labour law measures or procedural amendments, for example, and can even extend to the dismissal of employees and the termination of business relationships.

If a risk or a breach relating to human rights and environmental due diligence obligations has been identified in a complaint within our enterprise, pursuant to LkSG, appropriate remedial and preventive measures are initiated and monitored in accordance with the applicable legal provisions in order to immediately eliminate the risk and prevent it from recurring. This applies to a breach of duty abroad as well as domestically.

The Corporate Compliance department will notify the whistleblower in writing of the progress of the procedure and of any preventive or remedial measures taken no later than three months after the report has been submitted. If the allegations are unfounded, the person affected will be vindicated upon request. The results of each investigation should be used to avert potential misconduct and prevent it from occurring in the future (lessons learned).

As a rule, information about investigation results is only made available to the parties who actively need it for subsequent proceedings or to fulfil legal obligations. At the end of the investigation, a final report is drawn up and the Management Board and, if necessary, the Supervisory Board are informed of the facts or incident.

If necessary based on the results obtained, other competent bodies, decision-makers and, if applicable, the authorities will be called in and the relevant data will be disclosed to them.

The report or complaint will be investigated in accordance with GDPR.

4.1 How is the whistleblower involved in the fact-finding process?

Every report and every complaint is taken seriously by secunet Group. As such, the whistleblower is always notified of how the matter is being dealt with and the outcome of the individual steps. We endeavour to be as transparent as possible towards the whistleblower during the fact-finding process.

4.2 How long does the fact-finding process take?

The scope and complexity of the report or complaint determine the duration of the procedure. Reports and complaints are given high processing priority. The company carries out the investigation of the reported facts quickly and without culpable delays. Depending on the scope and complexity, a thorough investigation can take a few days or even several months.

| | | |
|-------------------------------------------------------------------------|-----------------------|--------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 9 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |

4.3 Data protection

Information on data protection can be found in the corresponding data protection statement for the secunet Group whistleblowing system.

| | | |
|-------------------------------------------------------------------------|-----------------------|---------------|
| Procedural instructions regarding secunet Group's whistleblowing system | | Page 10 of 10 |
| Valid with effect from: | June 2023 | |
| Version no.: | 1.0 dated 24 May 2023 | |