SNF
WATER SCIENCE

WHISTLEBLOWING PROCEDURE

PURPOSE OF THE WHISTLEBLOWING PROCEDURE

This policy defines the conditions of use of the professional alert system within SNF Group. It aims to provide the persons listed in the Scope below with a channel to report any facts of non-compliance with the Group's Code of Conduct and any other applicable policies they become aware of.

This alert system complements but does not replace the internal reporting methods within the SNF Group (such as the hierarchical channel, employee representative bodies, and the Human Resources Department). Every employee or collaborator remains free to use the communication channel they deem most appropriate.

SCOPE

This alert system is available to:

- All Group employees, including current or former
- External and occasional collaborators (subcontractors, intermediaries, suppliers, clients)
- Members of the management and executive bodies of the Group entities
- Shareholders in a Group affiliate, whatever their holding status is

The alert system is authorized to receive reports for facts and situations falling into one of the following categories:

- Actions or situations contrary to the SNF Group's Code of Conduct,
- Violation or attempted concealment of a violation:
  - of the laws of the countries in which the SNF Group operates
  - of the SNF Group's internal regulations
  - of an internationally ratified or approved commitment by the countries in which the Group operates, especially France and the United States
- A serious threat or harm to the public interest

Facts, information, or documents, regardless of their form or medium, covered by national defense secrecy, medical confidentiality, judicial deliberation secrecy, investigation or judicial instruction secrecy, or the attorney-client privilege between an SNF Group lawyer or legal advisor and their client are excluded from the scope of the alert system defined by this Charter. Contacts related to any other subjects cannot be considered within the scope of this alert system, but collaborators can be directed to other competent contacts within the company.

REPORTING PROCEDURE

Who Can Submit a Report?

Anyone wishing to submit a report under this charter must meet the following cumulative conditions:

- Be a physical person and disclose their identity
- Have personally become aware of the reported facts
- Receive no financial compensation for the report
- Act in good faith, meaning having reasonable grounds to believe that the reported facts are accurate based on the information at their disposal and that they are likely to be subject to an alert

Anyone meeting the above conditions cannot be subjected to any disciplinary action or retaliatory measures, even if the facts later prove inaccurate or do not result in any action. Conversely, the abusive use of the alert system, made in bad faith or with the aim of slandering, exposes the author to disciplinary sanctions and may incur civil and criminal liability. An anonymous report does not fall under the right to raise concerns about this procedure.

To Whom Does One Address the Report?

People wishing to submit a report can do so via the following email address dedicated to the alert system: **ethics@snf.com**

The recipient of this report is the SNF Group Chief Compliance Officer. Two delegated compliance officers in China and the United States support the Group's Chief Compliance Officer. They may be contacted if necessary.

Reporting Modalities

To enable effective handling, the report must include a detailed description of the reported facts and be accompanied by any documents on which the report is based. Whenever possible, it should be written in French or English. However, any report will be processed regardless of the language used.

Response Time

The Chief Compliance Officer must acknowledge receipt of the report made by this charter within seven days.

Subsequently, a first response must be provided within three months from the acknowledgment of receipt of the report to inform the author of the actions already taken or planned to assess the integrity of their alert (e.g., initiating an internal investigation) and address the reported situation. Depending on the circumstances, third parties may be involved in handling the report.

CONFIDENTIALITY

The confidentiality of the identity of the authors of the report, the individuals mentioned in the report, and any third parties mentioned in the report is guaranteed within the framework of the professional alert system by the chief compliance officer as well as any third parties involved in the handling of the report. Information that may identify the author of the report cannot be disclosed (including to the person(s) implicated in the report) except to the judicial authority and with the consent of the author of the report.

PROTECTION OF THE DATA OF THE INDIVIDUALS CONCERNED

The personal data collected within the framework of the alert system are subject to automated processing implemented by the Group in compliance with applicable regulations on personal data.

Categories of Collected Data

The professional alert system only records the following personal data:

- Identity, contact details, and position of the whistleblower
- Identity, position, and contact details of the individuals subject to a report
- Identity, position, and contact details of individuals involved in the collection or processing of the report
- Reported facts
- Information collected during the verification of the reported facts
- Report of the verification operations
- Follow-up actions taken based on the report

Rights of the Individuals Concerned

Any person identified in the alert system can access their data and request the Chief Compliance Officer to rectify or delete them if they are inaccurate or incomplete. The right to rectification applies to factual data, the material accuracy of which can be verified by the chief compliance officer with supporting evidence.

CONCLUSION OF THE PROCESS

Data related to a report the Chief Compliance Officer considers as falling outside the system's scope are immediately destroyed. When a report does not result in disciplinary or judicial proceedings, the data is destroyed or archived by the chief compliance officer within two months from the closure of the verification operations. When disciplinary proceedings or legal action are initiated against the person implicated or the author of an abusive report, the data related to the report is retained until the conclusion of the proceedings and the exhaustion of all legal remedies.

All Rights Reserved SNF - Published 03/2024

SNF WATER SCIENCE