



# Whistleblower Policy

Classification: Public  
Version: 1.4

2021-12-17

# Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>2</b>	<b>INFORMATION ON REPORTING CHANNELS .....</b>	<b>3</b>
<b>3</b>	<b>WHO CAN REPORT? .....</b>	<b>4</b>
<b>4</b>	<b>WHAT CAN YOU REPORT ON? .....</b>	<b>4</b>
<b>5</b>	<b>WHAT CANNOT BE REPORTED? .....</b>	<b>6</b>
<b>6</b>	<b>HOW DO YOU REPORT? .....</b>	<b>7</b>
<b>7</b>	<b>ANONYMITY .....</b>	<b>7</b>
<b>8</b>	<b>WHO PROCESSES THE REPORTS AND FOR HOW LONG? .....</b>	<b>8</b>
<b>9</b>	<b>PROTECTION FROM RETALIATION AND OTHER RIGHTS .....</b>	<b>9</b>
<b>10</b>	<b>INFORMATION ABOUT THE REPORT TO THE PERSON IN QUESTION .....</b>	<b>10</b>
<b>11</b>	<b>DATA PROCESSING .....</b>	<b>10</b>
<b>12</b>	<b>TRAINING .....</b>	<b>10</b>

# 1 Introduction

- 1.1 NNIT A/S including affiliates (“NNIT”) is a trustworthy company with an open and honest company culture in which every employee is free to express themselves.
- 1.2 NNIT expects all employees, management, the board of directors and any other person or entity doing business with NNIT to comply with applicable laws, regulations and internal procedures.
- 1.3 NNIT is committed to detect and prevent illegal activities, financial fraud, business ethics misconduct, security breaches or similar. Therefore, all employees, management and the board of directors of NNIT as well as all other persons doing business with and/or advising NNIT such as suppliers, customers, business partners, lawyers or auditors and other relevant persons are encouraged to report concerns regarding acts or omissions that could harm NNIT.
- 1.4 NNIT has standard internal communication channels in place, where concerns can be reported directly to managers, HR/Legal and even senior management, but at the same time NNIT understands and recognizes that in some situations persons may be reluctant to report concerns due to a sense of loyalty towards NNIT or colleagues or in the worst case in fear of retaliation.
- 1.5 NNIT has therefore established a whistleblower-function with internal reporting and procedures, enabling *inter alia* employees, the management, the board of directors of NNIT, business partners and advisors to NNIT and persons specified below to report concerns of illegal or fraudulent behavior, business ethics misconduct and security breaches in a secure and confidential way. The purpose of the whistleblower-function is also to fulfill the Whistleblower Directive as implemented in relevant countries for NNIT. The person reporting the concerns shall in the following be referred to as the “Whistleblower”.

# 2 Information on reporting channels

- 2.1 The purpose of this Whistleblower Policy is
  - a) to inform of NNIT’s internal reporting channel (whistleblower function) and procedure for handling of whistleblower cases, and
  - b) to inform the employees of NNIT A/S of the external reporting channel established at Datatilsynet in Denmark at [whistleblower.dk](http://whistleblower.dk). This reporting channel is established to fulfill the Whistleblower Directive. More information on the reporting channel can be found at [whistleblower.dk](http://whistleblower.dk).
- 2.2 The Whistleblower can choose to report in either of the reporting channels. However, NNIT shall – in accordance with the Whistleblower Directive – **encourage reporting through internal reporting channels** before reporting through external reporting channels, where the breach can be addressed

---

effectively internally and where the reporting person considers that there is no risk of retaliation (see also section 9 below).

- 2.3 This Whistleblower Policy will in the following only concern NNIT's internal reporting channel.

## 3 Who can report?

- 3.1 All employees, including the management, may report – as is required by the Whistleblower Directive - concerns detected as part of his/her engagement with NNIT to NNIT's internal reporting channel.
- 3.2 Further, NNIT has decided to expand the persons who can report to NNIT's internal reporting channel beyond the requirement in the Whistleblower Directive. The following persons with a *work-related connection to NNIT* can therefore also report concerns through NNIT's internal reporting channel.
- 3.3 Former employees, persons who have been in a recruitment process with NNIT, paid or unpaid trainees, the board of directors of NNIT, shareholders as well as all other persons doing business with and/or advising NNIT, such as lawyers, auditors, suppliers, customers and business partners and their employees may report. *However, these persons should due to data protection rules not include sensitive personal data in reports.* The following data are categorized as sensitive data in data protection legislation: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

## 4 What can you report on?

- 4.1 The whistleblower-function may only be used to report on the following matters, which has taken place or will take place within NNIT:
- 1) Breaches of EU law falling within the scope of the Whistleblower Directive, cf. section 4.2 below.
  - 2) Severe breaches of other parts of EU law or national law or other severe matters, cf. section 4.3-4.10 below.
- 4.2 Only breaches of the EU acts listed in the Whistleblower Directive can be reported. The Whistleblower Directive lists these acts in Annex, part 1. The list, and implementation of the rules, entails that all (and not only severe) breaches can be reported within specifically the following areas:
- 1) public procurement;
  - 2) financial services, products and markets, and prevention of money laundering and terrorist financing;

- 3) product safety and compliance;
- 4) transport safety;
- 5) protection of the environment;
- 6) radiation protection and nuclear safety;
- 7) food and feed safety, animal health and welfare;
- 8) public health;
- 9) consumer protection;
- 10) protection of privacy and personal data, and security of network and information systems; and.
- 11) EU competition law and state aid law.

4.3 Besides breaches mentioned in clause 4.2 above, *severe breaches of other parts of EU law or national law or other severe matters* can be reported.

4.4 A breach of law or a matter will as a starting point be severe if it is in the interest of the public.

4.5 NNIT's compliance function will for each report assess if the report concerns a severe breach or another severe matter as mentioned in section 4.3.

4.6 The following violations of the criminal code will be assessed as examples of severe law violations:

- Bribery,
- falsification of documents,
- hacking,
- wire tapping,
- recording of other people's conversations,
- theft,
- embezzlement,
- fraud,
- data fraud, and
- criminal breach of trust and extortion.

4.7 Gross or repeated violations of special legislation will be assessed as severe breaches, for instance legislation which shall ensure public health and safety or protection of nature and environment.

4.8 Harassment will also be assessed as severe breaches in the following cases:

- Sexual harassment, cf. the Danish Equal Treatment Act section 1, subsection 4, cf. subsection 6.

- Gross harassment, e.g. due to race, gender, color, language, assets, national or social origin, political or religious affiliation.
- 4.9 As examples of conditions which in general are considered serious matters can be mentioned:
- Disregard for vocational standards which e.g. could cause a risk for people's health and safety.
  - Serious errors and serious disorders related to IT operations or IT system operations.
  - Severe *business ethics* misconduct
  - Special circumstances where minor collaboration difficulties entail great risks and thus constitute a serious matter.
- 4.10 This lists above serves as examples only.
- 4.11 If you are in doubt about whether your concern should be reported or not, we encourage you to report the finding through the whistleblower-function.
- 4.12 Your report should include a description of your concern and, if possible, the name and title of the person suspected of irregular behavior.
- 4.13 It is important that the whistleblower-function is not used to report false and/or unfounded accusations. All reports must be made in good faith and must be well-founded. If a report is filed in bad faith or is based on personal reasons, such as revenge or as an act of spite etc., NNIT reserves the right to take appropriate measures, including legal action, against the Whistleblower if he/she can be identified.

## 5 What cannot be reported?

- 5.1 You cannot report on the following:
- a) Information on your own employment, unless such a report relates to a serious offense or an otherwise serious issue such as sexual harassment.
  - b) Information on minor irregularities such as breaches of internal guidelines of a less serious nature about for instance sick absence, smoking, alcohol, attire, private use of office supplies, incompetence and infringement of accessory provisions, such as lack of compliance with documentation obligations.
- 5.2 Such reports will in accordance with the data protection regulation be deleted from the whistleblower system. Instead, such concerns should be reported through standard internal communication channels, i.e. to direct managers, HR/Legal or senior management.
- 5.3 Furthermore, the Danish law on protection of whistleblowers lists that reports cannot contain certain classified information, information covered by lawyers' and healthcare personnel's confidentiality obligations and other information covered by confidentiality obligations as further specified in the legislation.

## 6 How do you report?

- 6.1 You file a whistleblower-report through the whistleblower system: [nnit.whistleblownetwork.net](http://nnit.whistleblownetwork.net). You will receive a confirmation of receipt of the report within 7 days, unless your report is anonymous.
- 6.2 The whistleblower system is hosted by an external independent third party. The independent party only operates the system and does not have access to the reports in any way. All data reported through the whistleblower system is encrypted and stored safely.
- 6.3 We strongly urge you to report through the whistleblower system and **NOT** to send reports via e-mail to the person(s) in NNIT's compliance function as the information in the report will not be securely transferred and encrypted and you will not be able to report anonymously.
- 6.4 When reporting through the whistleblower system, you may choose to remain available for further inquiries, even if the report is made anonymously. We recommend that you make yourself available as we may need additional information to conduct an investigation.
- 6.5 You remain available by opening a secure post box in the whistleblower system. When creating a post box, you will be provided with a case number and be asked to choose a password. With the case number and password you can log into the post box in order to see if you have received any questions or answers related to the report.
- 6.6 If you realize that you have provided incomplete or incorrect information, and have not created a post box, you may file a new report through the whistleblower system in which you refer to the earlier report and describe what should be corrected.
- 6.7 All reporting should be in English or Danish.

## 7 Anonymity

- 7.1 The Whistleblower may choose to report on an anonymous basis.
- 7.2 Before filing a report, you should carefully consider whether to be anonymous or not. We encourage you to identify yourself, as additional information may be required to carry out an investigation. The system is designed and set up to secure the Whistleblower from any retaliation and the Whistleblower's identity will only be disclosed to the person(s) investigating the report. Please note that if the report leads to legal proceedings against the person in question you may be called as a witness in a trial, in which anonymity is forfeited.
- 7.3 To ensure full anonymity it is however necessary to file the report from a private computer that is **NOT** on NNIT's corporate network. The whistleblower system does not log IP addresses or Machine IDs and does not use cookies. Only the report itself is registered.

- 
- 7.4 You should be aware that uploaded documents may contain metadata that can compromise the anonymity. Therefore, you should ensure that any compromising metadata is removed from a document before uploading it. Metadata is for example author details in a word document. Such data may be evident in the properties of the word document.
- 7.5 NNIT encourages the Whistleblower to disclose his/her identity, as this may prove vital for the further investigation of the matter. The Whistleblower's identity will only be disclosed to the person(s) investigating the report.

## 8 Who processes the reports and for how long?

- 8.1 Reports are handled in a secure and confidential way by NNIT's compliance function. Upon receipt of a report, NNIT's compliance function performs a preliminary screening and consults the CEO and/or CFO of NNIT A/S in order to decide whether to investigate the matter further.
- 8.2 If a report concerns the executive management, including the CEO and/or CFO, the NNIT's compliance function will instead consult the chairman of the Audit Committee – as an independent third party – in order to decide whether to investigate further.
- 8.3 If the preliminary screening concludes that the report
- is *well-founded* and falls *within* the scope of the whistleblower-function, a further investigation will be initiated
  - is *unfounded* and no further information is made available, no further investigation will be initiated
  - does not fulfill the legal requirements to qualify for reporting through the whistleblower-function, the compliance function will decide whether to forward the report to the relevant person within NNIT or let the Whistleblower know whom to contact instead. The report will subsequently be deleted from the Whistleblower system.
- 8.4 If it is decided to investigate the concerns set out in the report further, the compliance function designates an appropriate investigator and informs the Chairman of the Audit Committee that an investigation has been initiated. The investigator may be an internal or external resource depending on the matter.
- 8.5 Depending on the area of concern, the investigation will under normal circumstances be carried out by the following functions:
- *Financial fraud* will be investigated by NNIT Finance under the responsibility of the CFO
  - *Severe Business Ethic misconduct* will be investigated by NNIT Legal under the responsibility of the CEO or CFO depending on the area of misconduct
  - *Severe Security breaches* will be investigated by NNIT Q&S under the responsibility of the SVP of People, Communication & Quality



- *Data Protection breaches* will be investigated by NNIT Legal or Q&S

Investigations regarding illegal activities will be carried out by the relevant function within the area of illegality.

- 8.6 If the report is not anonymous, NNIT will send feed-back to the Whistleblower as fast as possible and within three months from the confirmation of receipt of the report.
- 8.7 The Compliance Function will quarterly provide the Audit Committee with a list of all reports made, information on the result of the preliminary screening and status on reports being investigated.
- 8.8 Once an investigation is completed and relevant actions have been taken the report is deleted in the whistleblower system, unless NNIT assesses that it is necessary and proportionate to store the report in the whistleblower system for the purpose of fulfillment of legislative obligations. The report is kept in the suspected person(s) personal file for as long as needed but only with necessary personal information.
- 8.9 The case may be of a nature which calls for handing over the report and further investigation to the police. If a report leads to court proceedings, the report will not be deleted from the whistleblower system until a possible appeal period has expired.

## 9 Protection from retaliation and other rights

- 9.1 All reports filed in good faith are protected against any retaliation.
- 9.2 Reports filed in bad faith may be met with legal actions as described above under section 4.134.12
- 9.3 Whistleblowers covered by the whistleblower directive and EU member state laws implementing this directive are provided an explicit legislative protection against retaliation and hinderance of reporting or attempt of hinderance. At the moment such protection applies for:
- a) employees in NNIT A/S using the internal reporting channel
  - b) Whistleblowers, cf. section 3, using the external reporting channel regarding NNIT A/S, and
  - c) Whistleblowers, cf. section 3, disclosing information regarding NNIT A/S in accordance with the mentioned legislation.
- 9.4 The legislative protection implies:
- a) The Protection is only provided for whistleblowers who have had reasonable grounds to believe that the information on breaches reported or disclosed was true at the time of reporting/disclosure and that such information is within the scope of this Whistleblower Policy, cf. section 3 and 4.

- b) A Whistleblower who fulfills the conditions in section 9.3 and section 9.4, litra a, shall not be considered to have breached any legislative confidentiality obligation and will not have incurred any liability of any kind, if the Whistleblower had reasonable ground to assume that the report or disclosure was necessary to disclose an issue covered by section 4.
- c) That the whistleblower – and relevant persons, companies and authorities connected to the Whistleblower – are protected by legislation by retaliation as further specified in the national legislation.
- d) In legal proceedings, a Whistleblower shall have the right to rely on a reporting or public disclosure to seek dismissal of the case, provided the Whistleblower had reasonable grounds to believe that the reporting or public disclosure was necessary for revealing a breach covered by section 4.

## 10 Information about the report to the person in question

- 10.1 NNIT is required to inform the person suspected of illegal/irregular activities. NNIT will for each report conduct an assessment of when the person in question should be notified. This assessment will be carried out to ensure that the notification does not obstruct any ongoing investigation of the matter.
- 10.2 No information on who has filed the report will be disclosed, and anonymity will thus be secured.

## 11 Data processing

- 11.1 Any personal data will be processed in accordance with this whistleblower policy and NNIT's privacy policy. The data subject's rights in relation to processing of personal data are described in NNIT's Data Privacy Policy.

## 12 Training

- 12.1 All NNIT employees will undergo regular training in NNIT's Whistleblower Program and all NNIT employees will on an annual basis be obligated to read and understand the NNIT Whistleblower Policy and document it.