Whistleblowing Policy

Company:	Nordnet AB (publ), Nordnet Bank AB
Approved by:	Board of Directors
Date of approval:	2025-11-24 (replaces 2024-11-25)
Document owner:	Chief Compliance Officer
Revised:	Annually or more often if required
Confidentiality class:	Open

Table of contents

1 Introduction

1.1 Background

This policy applies to Nordnet AB (publ) and Nordnet Bank AB, hereafter referred to as “Nordnet” or “the Company”.

1.2 Purpose and objective

The purpose of this policy is to describe the routines and procedures that Nordnet has established to capture potential or actual violations against Nordnet’s internal regulations, code of conduct, as well as against national law – where these offenses entail or could entail considerable damage for Nordnet.

1.3 Regulatory basis

This policy is established in accordance with:

- EBA Guidelines on internal governance under Directive 2013/26/EU (EBA/GL/2021/05)
- Swedish Banking and Financing Business Act (lag (2004:297) om bank- och finansieringsrörelse, 6 kap. 2 b §)
- Swedish Act on the Protection of Persons Reporting Irregularities (lag (2021:890) om skydd för personer som rapporterar om missförhållanden)

2 Reporting principles

2.1 The notifier

A basic principle of whistleblowing is that each employee, consultant, trainee, job applicant, board member and shareholder actively working within the Company, as well as other persons who are in corresponding work situations within Nordnet (“Notifier”), should have the full opportunity to call attention to a potential or actual violation, and that the Notifier’s privacy and confidentiality can be guaranteed throughout the process – unless they decide otherwise.

A Notifier who has reported suspected violations directly to the Swedish FSA (Finansinspektionen) or to EBA shall not be held responsible for having breached any obligation of professional secrecy, if the Notifier had reason to believe that a violation had occurred. The same applies if a Notifier has made a report via Nordnet’s internal reporting system for whistleblowing reports.

2.2 Reporting

Notifiers within Nordnet have the option to anonymously report potential or actual violations in written form via a specific communication tool. Additionally, Notifiers can report orally to the Chief Compliance Officer. The Notifier may also choose not to remain anonymous. Information relating to the case should not be disclosed to third parties unless required by law or administrative decision.

3 Roles and responsibilities

Receiver: At Nordnet, Chief Compliance Officer, and by him/her designated alternate receivers within the Compliance function, are receivers of whistleblowing reports. The receiver is responsible for making an initial assessment of the report, take lead in the investigation, and inform the CEO and the board of directors when required.

Notifier: The notifier is the person who submits a whistleblowing report.

4 Process and procedures

4.1 General process description

1. The Notifier submits the report either by using the web-based tool, or by an oral report to the Chief Compliance Officer.

2. The Receiver receives a notification of a new case (if the report is submitted through the web-based tool).

3. The Notifier receives a confirmation that the report has been received (no later than 7 days from submission of the report).

4. The Receiver investigates whether the report is based on facts. The Receiver can ask the Notifier for additional information via the web-based tool or orally in the case of an oral report.

5. If the report is deemed to be based on facts the case will be investigated further and any relevant people needed in order to conduct the investigation properly can be approached.

6. The result of the investigation is shared with relevant people such as department heads etc. The CEO shall always be informed as well unless the report only relates to an isolated, minor event or one specific individual.

7. Appropriate measures are taken.

8. The result of the investigation is shared with the Notifier (no later than 3 months from confirmation of the received report).

5 Protection of the notifier

Throughout the whole process the notifier shall be protected. However, it should also be taken into account that the person/s implicated in a report must be allowed to voice their concerns in a

respectful and objective manner. In addition to the Notifier themselves, natural and/or legal persons connected to or aiding the Notifier – in a work-related context – shall be afforded protection from reprisals due to the Notifier's report.

A Notifier who has reported suspected violations shall not be held responsible for having breached any obligation of professional secrecy when reporting directly to the Chief Compliance Officer or via the web-based communication tool described above, if the Notifier had reason to believe that a violation had occurred.

6 Documentation

Reports submitted by a notifier are stored in the whistleblowing tool itself. Further investigative and operative measures (e.g. protocols from meetings etc.) relating to the case shall be properly documented and stored locally by the compliance function, with restricted access.

7 Retention of records

Records and data relating to the case shall only be kept for as long as is necessary with regards to the purpose of processing the whistleblowing report, but in any case, no longer than two years from the notification date. If a Notifier's report leads to investigation, the records shall be deleted when the investigation is complete or, in case the investigation leads to action against the person/s in question, when the records are no longer needed for the purposes of the investigation.

8 Communication and trainings

All employees throughout Nordnet group should be familiar with the policy and it should be easily accessible on the intranet. The whistleblowing process should be a part of the onboarding training sessions provided by Compliance as well as provided when deemed necessary.