

Neurosoft

**WHISTLEBLOWER POLICY
NEUROSOFT SA**

November 03, 2023
Version 01

Approved by BoD



NEUROsoft



Table of Neurosoft Whistleblower policy Amendments

Version No - Date of Approval	BoD Decision	Description
01 - 03/11/2022	11/12/2023 (item 1)	Initial version



Contents

Table of Neurosoft Whistleblower policy Amendments	1
1 Introduction	3
2 Definitions and abbreviations	4
3 No Retaliation	5
4 Reporting Incidents	6
5 Investigation and Oversight	7
6 Acting in good faith	8
7 Confidentiality and Anonymity	8
8 Retention of Records & Policy Review	8



1 Introduction

The Company expects each director, manager, employee, client and supplier to comply with all applicable laws and Euronext Growth Market requirements. The Company is committed to promoting honesty and integrity and maintaining the highest ethical standards in all its activities. Consistent with these values the Company does not tolerate any illegal or unethical behavior, including fraud, criminal acts, regulatory violations, manipulation of accounting and auditing records, or any breach of the Code or any other policies, procedures, or practices established by the Company.

The Audit Committee must ensure the Company has the appropriate procedures for i) the receipt, retention, and treatment of Incidents (as defined below), and ii) the confidential, anonymous reporting of concerns regarding questionable accounting or auditing matters. This policy serves to fulfill these Audit Committee responsibilities.

This policy applies to each Incident reported, and the procedures, protections and other provisions of this Policy are for the benefit of every director, manager, employee and contractor of the Company.

2 Definitions and abbreviations

This Section of the Whistleblower policy also include the following definitions and abbreviations.

Company	Means Neurosoft S.A.
Group	Means a parent undertaking and all its subsidiary undertakings according to the definition of the International Accounting Standard 28
Administrator	Means the person designated by the board to oversee the day -to-day administration of this Policy, including receiving, tracking, and reporting to the board on Incidents reported.
Audit Committee	Means the Audit Committee appointed by the Company's board of directors
Board of Directors, or BoD	The Company's Board of Directors
Code	Means the Code of Conduct adopted by the Board
Reporter	Means a Company's employee or supplier reporting Incidents under this policy
Incident	<p>Means one or more violations or suspected violations of the Code, applicable laws, or the Company's accounting, financial reporting, internal accounting controls, or auditing policies and procedures, or related matters, including, but not limited to, the following non-exhaustive list of examples:</p> <ul style="list-style-type: none"> - suspected violations of applicable law, whether civil or criminal, including breaches of occupational health and safety legislation; - suspected violations of corporate policies or guidelines of the Company or the Code; - questionable accounting, internal accounting controls, auditing practices or accounting or auditing irregularities; - experiencing or observing discrimination, harassment, sexual misconduct, workplace violence, substance abuse, violation of human rights, or similar behaviors; - any falsification of contracts, books, records, reports or accounts,



	<ul style="list-style-type: none"> - direct or indirect participation in any bribes, kickbacks, improper profit-sharing arrangements, illegal or improper inducements or payments to any public official or other acts of corruption or bribery; - fraud against or involving the Company, its subsidiaries or any party having a business relationship with the Company; - risks to the Company's assets, property, or resources; - risks to the environment; - any matter that involves a significant threat to the health and safety of the Company's personnel, other representatives or business partners and/or the general public, including unsafe working conditions; - concerns about the company's business practices; - a matter likely to receive negative publicity or - any retaliation against any Reporter for intending to make or making a good faith to report under this Policy.
Investigator	Means the person or people designated by the BoD with responsibility for investigating and bringing closure to reported incidents
Policy	Means this Whistleblower Policy
Reporter	Means an Employee Reporter or a director, manager or other person reporting incidents in accordance with this Policy, including but not limited to suppliers, business partners, consultants and clients.

3 No Retaliation

People who raise Incidents must not face retaliation, discrimination or harassment from the Company employees, managers or directors for speaking up. The Company will protect any person who raises an Incident honestly, and the Company's employees who retaliate, discriminate or harass people who raise Incidents will face disciplinary measures and may have their employment terminated. Honest reporting does not mean that you have to be right when you raise an Incident you just have to believe that the information you are providing is accurate to the best of your knowledge.

All forms of unlawful retaliation are prohibited, including any form of adverse action, discipline, threats, intimidation or other



form of retaliation for reporting under or complying with this policy. The Company considers retaliation as a violation of this policy, which will result in disciplinary action, up to and including termination of employment or any other working relationship with the Company.

If a person has been subject to any conduct that he/ she believes that constitute retaliation for having made a report in compliance with this policy or for having participated in any investigation relating to an Incident, they must immediately report the alleged retaliation to the Head of Human Resources, Chief Executive Officer or Chief Financial Officer ideally within ten (10) days of the offending conduct. If for any reason, such person does not feel comfortable discussing the alleged retaliation with these people, he/she can report the alleged retaliation through the Whistleblowing line by phone +2106855061 (int 211) or via email whistleblow@neurosoft.gr. These individuals will ensure that an investigation is conducted in a timely fashion.

Any complaint should be as detailed as possible, including the names of all individuals involved and any witnesses. The Company will directly and thoroughly investigate the facts and circumstances of all perceived retaliation and will take prompt corrective action, if appropriate.

Moreover, any manager or director who observes retaliatory conduct must report the conduct to the Head of Human Resources, Chief Executive Officer or Chief Financial Officer so that an investigation can be made and corrective action taken, if appropriate.

Bringing any alleged retaliation to the Company's attention promptly enables it to honor our values, and to promptly and appropriately investigate the reported retaliation in accordance with the procedures outlined in the Policy.

Any employee, regardless of position or title, who has been determined to have engaged in retaliation in violation of this policy, will be subject to appropriate disciplinary action, up to and including termination of employment or any other working relationship with the Company.

4 Reporting Incidents

Incidents must be reported promptly by Reporters to someone who can address them properly.

If an Employee Reporter believes that in the circumstances it would not be appropriate to report an Incident to their supervisor, the Employee Reporter may report the Incident to any officer or other member of the Company's management team to whom the person believes it would be appropriate to report the Incident.

Where a manager or other senior member of management receives an Incident report, it must be promptly forwarded to the Administrator.

Suspected fraud or violations of applicable laws should be promptly reported directly to the Administrator.

Reporters may report their concerns under the Policy through the available channels. They should choose the channel that

is most appropriate given the nature of their concern :

- To the Administrator,
- To the Chairman of the Audit Committee.

Access to Incident reports is strictly controlled to prevent interference with, and ensure the independence, effectiveness and integrity of any ensuing Incident investigation. Upon receiving an Incident report, the Administrator will forward it to the Chairman of the Audit Committee and the Chief Legal Officer (provided that such individuals are not related to or the subject of the Incident). Incident reports received through third-party provider of confidential, anonymous reporting services are automatically forwarded to the Administrator, Chairman of the Audit Committee and/or Chief Legal Officer.

5 Investigation and Oversight

The Administrator has been designated by the BoD and will serve as the Investigator for Incidents of a general nature that are not more appropriately investigated by another person. Where an Incident pertains to a matter more appropriately investigated by another person, the Administrator will consult with the Chairman of the Audit Committee and Chief Legal Officer to assign an appropriate internal or external Investigator to investigate the Incident. No person will be appointed to investigate an Incident where that person is or could reasonably be perceived to be in a conflict of interest, or otherwise not impartial or unbiased in conducting the investigation.

The Investigator will investigate Incidents in an independent, expeditious, and confidential manner, taking care to protect the identity of the people involved and to ensure that the investigation is not impaired in any manner.

The Investigator will contact the Reporter to acknowledge receipt of the Incident report within 15 business days.

All Incidents will be promptly investigated, and appropriate corrective action will be taken if warranted by the investigation.

All people (including the Reporter) must fully cooperate in the Investigator's investigation.

The Investigator may involve other people in the investigation as deemed appropriate (including members of the Company's management). The Investigator may agree to authorize an independent investigation and/or to engage external consultants to assist in the investigation. The Investigator has direct access to the Chairman of the Audit Committee.

The Audit Committee shall oversee the activities of the Administrator and Investigator and the investigation and resolution of Incidents. All material Incidents, including all Incidents relating to accounting, internal accounting controls or auditing matters, will be promptly reported by the Administrator to the Chairman of the Audit Committee for investigation in cooperation with and under the supervision of the Audit Committee. The Administrator will report to the Audit Committee on all other material Incidents once per quarter. The Administrator may periodically report to the Audit Committee a summary of any other non-material Incidents.



6 Acting in good faith

A Reporter must act in good faith and have reasonable grounds for believing that the information disclosed is true.

Incidents found to have been made in bad faith, maliciously or which were known to be false when made, will be viewed as a serious offence that could give rise to disciplinary action, up to and including termination of employment with the Company.

7 Confidentiality and Anonymity

All Incident reports will be treated as confidential, and each report and the identity of the Reporter will be kept confidential to the extent permissible by law and feasible to permit proper investigation and resolution. Reports will only be accessible to people that the Investigator determines have a “need to know” and where such access will not otherwise compromise or interfere with the independence, effectiveness and integrity of the investigation. Ordinarily, a need to know arises from an obligation to investigate or to take remedial action based on the information contained in the Incident report. For clarity, sharing Incident Information in a manner required by this Policy will not be considered a breach of confidentiality.

Reports of Incidents must be supported by sufficient information and evidence to enable a proper investigation, particularly in the case of anonymous Incident reports, since the Investigator may not be able to seek further details from the Report. Incident reports should include:

- The date(s) of Incident(s);
- The identity of individuals and witnesses involved;
- A description of the specific actions or omissions that constitute the Incident;
- How the Reporter became aware of the Incident;
- Any steps taken by the Reporter to date with respect to the Incident; and
- Any materials or documents relevant to support or evidence the Incident.

While this Policy facilitates anonymous reporting and protects Reporter anonymity, such measures may hinder the effective investigation of an Incident. Also, as a practical matter, it is possible that the identity of an anonymous Reporter may become known during the Incident investigation or resolution or may be subject to legal disclosure requirements. Therefore, the Company encourages Reporters to only report anonymously where necessary, given the inherent difficulty in properly investigating, following up on, and resolving anonymously reported Incidents. If a Reporter remains anonymous and does not provide sufficient detail regarding the Incident, the Investigator may not be able to initiate or complete a comprehensive Incident investigation.

8 Retention of Records & Policy Review

Records pertaining to an Incident are the property of the Company and shall be retained:



- In compliance with the applicable laws and the Company's retention policies,
- Subject to safeguards that ensure their confidentiality and when applicable, the anonymity of the Reporter,
- In such manner as to maximize the usefulness to the Company's overall compliance program.

This Policy shall be reviewed annually along with updates to the Code.