

ETHICS CHANNEL MANUAL

SWORD SOFTWARE DEVELOPMENT S.L

1. INTRODUCTION

Our legal system is increasingly promoting citizen participation in the proper functioning of public and private institutions. This gives citizens the possibility of reporting infringements detected within an organization so that appropriate action can be taken and they can be remedied.

Sword Software Development S.L guarantees its commitment to the principles of legality, transparency, corporate and professional ethics, thereby rejecting any type of irregular conduct within our organization. We therefore provide an anonymous channel for reporting incidents or unlawful conduct that occurs or may occur within the organization, thereby strengthening our compliance culture.

For the foregoing reasons, this Manual on the operation of the Sword Software Development S.L Ethics Channel has been created so that it is known by its employees, by anyone who has an employment or professional relationship with Sword Software Development S.L and, ultimately, by any interested person connected with us.

2. PURPOSE AND SCOPE

This Manual regulates the procedure necessary for the proper implementation and operation of the Sword Software Development S.L Ethics Channel.

The Ethics Channel is a reporting channel through which irregularities committed within the organization and of which the reporting person has knowledge or reasonable suspicion may be reported, including anonymously.

2.1. Who can use our Ethics Channel?

This channel may be used by anyone who has a professional and/or employment relationship with Sword Software Development S.L, such as employees, shareholders, partners, collaborators, etc. Suppliers, customers and, ultimately, anyone who is aware of conduct within the organization that may be harmful to citizens or society as a whole may also report information.

2.2 What matters can be reported through the channel?

By way of guidance, and without limitation or exclusion, unlawful or potentially unlawful conduct that may be reported through the channel includes: harassment, fraud and corruption (bribery, document forgery, etc.), theft, data protection or information security issues, unethical practices or malpractice (misleading advertising), etc.

In addition, questions or enquiries may be raised regarding matters related to our compliance culture, and advice or guidance may also be requested concerning practices or processes related to the organization.

3. PRINCIPLES

The operation of the Ethics Channel is governed by the principles of good faith, confidentiality and protection against retaliation, and independence and impartiality.

3.1. Principle of Good Faith

Anyone using the Ethics Channel to report an irregularity must comply with the principle of good faith, which requires that every communication or report made through the Ethics Channel be based on facts or indications from which it may reasonably be concluded that an act capable of being reported has occurred. Reporting a fact knowing it to be false or with the intention of harming a third party is strictly prohibited. Anyone who submits a report that is untruthful or motivated by revenge or an intention to harm the reported person may be subject to sanctions.

3.2. Principle of Confidentiality and Protection against Retaliation

Sword Software Development S.L will guarantee the highest level of confidentiality for communications received through the Ethics Channel, as well as for the identity of the interested person and the reported person, preventing such information from being disclosed. Only the persons responsible for properly managing the procedure will have access to it and will maintain the required confidentiality. This confidentiality obligation will not apply when the organization is required to disclose and/or make available information and/or documentation relating to its actions, including the identity of the parties involved, at the request of the competent judicial or administrative authority.

Likewise, Sword Software Development S.L guarantees protection against possible retaliation within the organization for anyone who reports an irregularity and for anyone who may participate in the investigation of the facts.

3.3. Principle of Independence and Impartiality

Sword Software Development S.L has outsourced the Ethics Channel management service in order to comply with the necessary principles of objectivity, independence and impartiality when investigating reports or providing guidance on the procedure, thereby avoiding any potential conflicts of interest.

4. OPERATION OF THE ETHICS CHANNEL

4.1. Internal Reporting System: Ethics Channel

The channel provided by Sword Software Development S.L for communications relating to our organization is the Ethics Channel, which can be accessed through the following link: sword-software-development.canales-eticos.com.

In addition, Sword Software Development S.L guarantees the availability of the Ethics Channel through means such as its website, should we have one, where it will always be located in a visible section independent from the other sections so that it is easily accessible to users.

The use of the organization's Ethics Channel does not prevent the reporting person from using external channels established by the competent authorities, the State Security Forces and Corps, as well as judges and courts.

4.2. How to submit a communication through the Ethics Channel platform

When accessing our Ethics Channel, the reporting person will be informed of the possibility of downloading the Tor Browser, as it is a browser that fully protects the reporting person's identity because the device's IP address is not recorded. The download can be made directly through the information window at the top of the Ethics Channel home page, thereby ensuring the highest level of confidentiality in communications.

To submit a communication, the reporting person should access the New Communication tab and complete the following sections:

1. Description. The subject of the communication and as detailed a description as possible should be provided, and files may be uploaded as documentary evidence.
2. Identification. This is not mandatory. In this section, the reporting person is informed that they may choose not to disclose their identity. If they wish to identify themselves, they should provide their first and last name together with their email address.
3. Terms and rules of use. The reporting person must read and accept the rules governing the Ethics Channel as confirmation that they have been informed.

Once the communication has been submitted, the platform will provide a code for monitoring the procedure.

In order for the user to monitor the procedure and check its status, they must select the "Follow-up" option on the same Ethics Channel home page and enter the numerical code provided when the communication was submitted.

All communications between the reporting person and the Investigator will take place through the platform established for this purpose, including a chat between the reporting person and the Investigator. However, where the user has identified themselves by providing their email address, communications between the reporting person and the Investigator will take place by email.

The report must be submitted individually. If several people are aware of the same facts, each of them must report them individually through the channel.

4.3. Reporting of False or Bad-Faith Complaints

The Sword Software Development S.L Ethics Channel must be used responsibly and appropriately. Reporting false facts with a malicious and morally dishonest attitude constitutes a breach of the good faith that must govern employment and professional relationships with Sword Software Development S.L and may result in disciplinary measures in accordance with the applicable collective bargaining agreement.

If, following the appropriate analysis, it can be concluded that the reported facts are manifestly false and that the report was submitted with a malicious attitude and in bad faith:

(i) the report will be closed, documenting the reasons that led to the closure of the case, thereby ending the investigation;

(ii) the proposed sanction will be reported in writing to the Management Body or, where applicable, the Board of Directors, which will decide on the disciplinary action to be applied to the bad-faith reporting person and/or on the possibility of pursuing civil or criminal liability.

5. MANAGEMENT OF COMMUNICATIONS

The processing or management of the procedure, from the moment a communication or report is submitted, is carried out by an independent third party (Investigator) outside Sword Software Development S.L in order to ensure the impartiality and objectivity required by this type of procedure and to avoid conflicts of interest.

The procedure covers the period from the submission of the report through the channel to its resolution and has therefore been divided into the following phases:

5.1. Receipt phase: receipt, examination and categorization of the communication

Once the Investigator receives the submitted communication, they will send the reporting person an acknowledgement of receipt within seven (7) calendar days, informing them of one of the following outcomes:

- **Admission for processing**. The facts reported or denounced may be considered unlawful acts or irregular conduct that undermine the principles and values of the organisation, and it will therefore be necessary to continue with their investigation.
- **Inadmissibility**. The report will be deemed inadmissible and the proceedings will be closed in the following cases:

  (i) The facts described cannot be considered unlawful or irregular; (ii) The facts described are not supported by sufficiently compelling evidence.

  There may be cases in which the reporting person is advised on other ways to proceed and informed of the procedure that would be most appropriate for resolving the matter reported. In some cases, if the communication may be relevant to another department for the purpose of improving the service, it will be referred to the corresponding department or area of the organization.

In all cases, the decision adopted and the reason for accepting or rejecting the report for processing will be communicated in writing.

5.2. Investigation phase

5.2.1. Opening of the case file and investigation of the reported facts

Once the communication has been evaluated, assessed and accepted, the Investigator will prepare an opening case file for the report under investigation.

The purpose of the opening case file is to ensure maximum traceability of the investigation process in the event that the report is requested by any competent judicial authority.

The Investigator will act with the appropriate confidentiality safeguards and in accordance with the other applicable principles, and will be responsible for investigating the report and collecting evidence.

During the investigation, the different areas of the organization may be involved to effectively obtain evidence and analyses that allow the reported facts to be verified.

The organization's Management Body may be requested by the Investigator at any time to complement, in a coordinated manner, the investigative actions carried out by the latter, always with the highest level of confidentiality and discretion.

If considered necessary, the Investigator will take steps to examine the facts in greater depth and obtain additional information in order to make an appropriate decision objectively, based on the evidence collected. Investigative actions may include: requesting new evidence and/or documentation from the reporting person to improve the investigation process; arranging interviews with the persons involved; reviewing all information relating to the professional relationship of the persons involved with the organization, always respecting data protection and privacy laws; forensic analysis by an independent external expert; and any other action considered necessary to continue the investigation process, in compliance with applicable data protection regulations.

At all times, the investigation will consist of an objective analysis of the available documentation, obtaining evidence, collecting proof and analyzing it.

The investigation period will not exceed three (3) months from receipt of the communication or, if no acknowledgement of receipt was sent to the reporting person, three (3) months from the expiry of the seven (7)-day period following submission of the communication, except in

cases of particular complexity requiring an extension, in which case it may be extended by a maximum of a further three (3) months.

5.2.2. Conclusion of the investigation and conclusions report

Once the allegations and evidence collected by the Investigator have been analyzed, the investigation phase is closed and a conclusions report is prepared reflecting the outcome of that phase. This conclusions report will clearly set out the assessment of the facts and a proposed course of action with possible measures to be applied. Any limitation encountered during the investigation must be reflected in the report.

5.3. Decision phase

Following the investigation phase, during the decision phase, the organization's Management Body or Board of Directors will analyze the report prepared by the investigative team, including its proposed measures, in order to issue the appropriate decision determining the measures to be applied.

The reporting person and the reported person must be informed in writing of the decision adopted and the reasons for it, which may result in one of the following options:

- **Dismissal of the report**. Case in which the investigation of the reported facts shows that there has been no breach.
- **Upholding of the report**. Case in which the reported facts are proven to be true, and it is necessary to detail the actions supporting that conclusion and the measures that will be adopted.

In cases of extreme seriousness, the organization will be required to report such facts to the State Security Forces and Corps and/or judges and courts.

6. REGISTER BOOK

Sword Software Development S.L maintains a register book of the information received and the internal investigations arising from it, ensuring in all cases the applicable confidentiality requirements.

This register will not be public and may only be accessed, in whole or in part, at the reasoned request of the competent judicial authority, by court order, within judicial proceedings and under the supervision of that authority.

Personal data relating to the information received and the internal investigations referred to in the preceding section will only be retained for the period necessary and proportionate to comply with the law. In no event may the data be retained for more than ten years.

7. PERSONAL DATA PROTECTION

Sword Software Development S.L guarantees the confidentiality of the personal data of any reporting person who has identified themselves, and such data will not be disclosed to the persons referred to in the reported facts or to third parties. Appropriate technical and organizational measures will be implemented to preserve identity and ensure the confidentiality of personal data.

Data subjects may exercise their data protection rights as set out in Articles 15 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Lastly, access to the personal data contained in the Ethics Channel will be strictly limited to persons who need such access within the scope of their powers and functions in order to manage the procedure.

In Barcelona, on 13 October, 2026

53008247D DAVID MARTINEZ HERNANDEZ (R: B66263641)

Firmado digitalmente por 53008247D DAVID MARTINEZ HERNANDEZ (R: B66263641)
Fecha: 2026.10.13 17:09:13 +02'00'

Signed: _____

Sword Software Development S.L