



**HUAWEI**

**Internal Information System Operation  
Policy**

**Huawei Technologies Spain, S.L.**



## Index

|  |    |
|--|----|
| 1. Introduction .....  | 3  |
| 1.1. Object and purpose .....  | 3  |
| 1.2. Scope of application .....  | 4  |
| 2. Definitions .....   | 4  |
| 3. Principles of the Internal Information System .....                   | 5  |
| 4. Governance Structure of the Internal Information System .....         | 6  |
| 5. Procedure of the Internal Information System .....                    | 7  |
| 5.1. Access .....  | 7  |
| 5.2. SII Officer .....   | 8  |
| 5.3. Reception of the Communication.....                                 | 8  |
| 5.4. Admission or Non-Admission of the Communication for Processing..... | 9  |
| 5.5. Processing of the Case .....  | 10 |
| 5.6. Resolution .....  | 11 |
| 6. Management and Archiving of Information .....                         | 12 |
| 7. Conflicts of Interest .....   | 12 |
| 8. Confidentiality .....   | 13 |
| 9. Data Protection .....   | 13 |
| 10. Protection of Informants .....                                       | 14 |
| 11. Information on the System and External Channels.....                 | 14 |



<Translation, the Spanish version shall prevail>

## 1. Introduction

Huawei Technologies España, S.L. (the "**Company**" or "**Huawei**") expresses its commitment to maintaining an environment of integrity, transparency, and ethics, where a culture of compliance and responsible behavior is promoted.

In compliance with Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, as well as in line with Huawei's corporate principles and compliance standards, the Company establishes this Internal Whistleblowing System Policy (the "**Policy**").

This Policy aims to regulate the operation of the Internal Whistleblowing System (IWS) and ensure that all individuals within its scope of application -including employees, executives, collaborators, contractors, suppliers, business partners, and other third parties associated with Huawei- can report, in good faith, any possible violations or irregularities according to the established procedures, and do so without fear of retaliation, harm, or any form of adverse treatment.

### 1.1. Object and purpose

The Internal Information System is a confidential, accessible, and secure means that allows for the responsible and good-faith communication of any suspicion or knowledge of legal or internal regulatory violations by Huawei, whether by organization professionals or third parties associated with it.

The IIS is an integral part of Huawei's compliance program and aims to:

- Facilitate the detection and communication of possible irregularities or risks of non-compliance.
- Establish the procedure for managing, analyzing, and investigating received communications, defining the roles and responsibilities of the involved individuals.
- Ensure compliance with Law 2/2023, dated February 20, which regulates the protection of persons who report regulatory violations and combats corruption.

The IIS serves as a preferred channel for reporting facts or behaviors that may constitute a violation, by action or omission, of current laws or Huawei's internal regulations. Its use contributes to preserving the integrity, ethics, and compliance culture of the organization.

The Company guarantees that all communications will be treated with the utmost confidentiality, diligence, objectivity, and respect for the rights of the affected individuals, ensuring:

- Protection of the identity of the informant,
- Absolute prohibition of retaliation, and
- Handling of information in accordance with applicable regulations, including personal data protection laws.



<Translation, the Spanish version shall prevail>

## 1.2. Scope of application

This document applies to all Huawei professionals, regardless of their position, function, or geographical location. All of them are obligated to report any violation or well-founded suspicion of non-compliance with external or internal organizational regulations that they become aware of in the course of their activities.

Similarly, suppliers, contractors, subcontractors, collaborators, and other individuals who maintain a professional or commercial relationship with Huawei and act under its supervision or direction may use the SII to report any irregularity related to the Society's activities.

Individuals involved in the management or investigation of communications must actively cooperate, providing the information and evidence necessary for their proper analysis.

## 2. Definitions

**External Channels:** public channels enabled by Public Administrations or independent bodies for the direct communication of violations within the scope of application of the Whistleblower Protection Law (such as the external channel of the Independent Whistleblower Protection Authority – A.A.I., or applicable regional or sectoral channels).

**Investigation Commission:** internal collegiate body responsible for the instruction and investigation of communications admitted for processing, acting with independence, objectivity, impartiality, and confidentiality, in accordance with the provisions of this document.

**Communication:** information transmitted through the SII regarding facts or behaviors that may constitute a violation of the law or internal regulations. It can be made anonymously or identified.

**Conflict of Interest:** a situation in which personal, professional, or any other interests of a person involved in the management, analysis, investigation, or resolution of a communication may influence, compromise, or call into question their independence, objectivity, or impartiality.

**Affected Person:** the natural person identified in a communication as a presumed responsible party for a violation.

**Whistleblower:** the natural person who communicates or reveals information about possible violations through the SII. Whistleblowers may include, among others: employees, partners, members of the board of directors, executives, interns, volunteers, candidates in selection processes, self-employed individuals or professionals providing services to Huawei, as well as employees and representatives of suppliers, contractors, and other third parties professionally linked to the Company.

**Violation:** any action or omission that may constitute:

- a serious or very serious criminal or administrative offense,
- a breach of European Union law included within the scope of Directive (EU) 2019/1937,
- a violation of current legal regulations, policies, or internal procedures of the Company,



<Translation, the Spanish version shall prevail>

- or unethical behavior or actions contrary to corporate values.

Acts of retaliation against whistleblowers or actions that pressure or induce a professional to commit a violation will also be considered reportable.

**Whistleblower Protection Law:** Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and combat corruption.

**LOPDGDD:** Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights, which adapts the GDPR to the Spanish legal system and establishes complementary provisions applicable to the processing of personal data in Spain.

**Board of Directors:** the board of directors of Huawei with which the whistleblower or affected person has a professional or contractual relationship.

**Register of Communications:** a secure system or file where received communications, actions taken, investigations conducted, and final results are documented, ensuring traceability and retention according to legal deadlines.

**Internal Information System Manager:** the person, body, or commission designated by Huawei responsible for directing and supervising the operation of the SII and ensuring its proper management.

**GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and the free movement of such data.

**Internal Information System or SII:** a set of rules, procedures, bodies, and tools designed to facilitate the communication, reception, management, investigation, and resolution of information or communications about possible violations, in accordance with the Whistleblower Protection Law and applicable regulations.

### 3. Principles of the Internal Information System

The IIS is governed by the following fundamental principles:

- **Accessibility:** The IIS and its procedures will be public, accessible, and easily usable by all persons authorized to communicate information.
- **Flexibility in communication:** Communications may be made in writing, verbally, or through both means, with the guarantees provided for in this document.
- **Anonymity:** Anonymous submission of communications will be allowed if the Informant so decides.
- **Confidentiality and integrity of information:** The confidentiality of the Informant's identity, the Affected Person, and any third party mentioned in the communication, as well as all

information and actions taken during the management and processing of the case, will be guaranteed. Access to information will be limited exclusively to the IIS Responsible, the Investigation Commission, and, where applicable, to persons strictly authorized due to their function.

- **Good faith, truthfulness, and proportionality:** Communications must be made in good faith, providing true and sufficient information, and should be limited to facts directly related to the activity of Huawei and/or the Affected Person. The fraudulent or malicious use of the IIS may result in internal sanctions or legal liabilities as appropriate.
- **Prohibition of retaliation:** The Company guarantees that no adverse measures, direct or indirect, will be taken against persons who report irregularities in good faith and in accordance with the requirements of the Whistleblower Protection Law.
- **Protection of personal processing of personal data** will be carried out in accordance with the provisions of the GDPR, the LOPDGDD, and the Whistleblower Protection Law, applying the principles of lawfulness, loyalty, confidentiality, minimization, and limitation of access.
- **Respect for the rights of affected persons:** In all investigations, the rights to privacy, defense, hearing, and presumption of innocence of persons affected by the communication will be respected.
- **Legality and compliance with regulations:** The operation and use of the IIS will comply with the applicable regulations, particularly the Whistleblower Protection Law, as well as any other relevant provisions in the various legal areas affected.

#### 4. Governance Structure of the Internal Information System

In order to ensure compliance with the Whistleblower Protection Act, the independence in the management of the SII, and the proper processing of communications, the following governance structure is established:

The Compliance Officer will act as the Responsible for the SII, being in charge of the initial reception and management of communications, their admission or rejection for processing, and the supervision of the case until its resolution, ensuring at all times independence, confidentiality, and the absence of retaliation.

The Investigation Commission will be the body responsible for the instruction of admitted communications. It will generally be composed of the following members:

- Compliance Manager, as a permanent member, except in cases of conflict of interest;
- One or several members designated ad hoc by the SII Officer, depending on the nature of the investigated facts and provided there is no conflict of interest; and
- Any other members deemed necessary based on the nature of the investigated facts, provided there is no conflict of interest.



<Translation, the Spanish version shall prevail>

The Investigation Committee will operate under the supervision of the SII Officer and will not replace the functions legally assigned to this officer, acting as a support and collaboration body.

The legal department of the Company may intervene as an internal advisor when necessary for the proper legal qualification of the facts, to ensure respect for the principle of contradiction and the right to defense, or for the review of the final report. Its intervention will be strictly limited to the scope of legal advice, without direct access to the Informant's data unless it is indispensable.

Additionally, the human resources department of the Company may only intervene when the facts under analysis affect the employment relationship of the Informant or the Affected Person, or when disciplinary measures may result. In such cases, the said department must sign a declaration of absence of Conflict of Interest, and its access to information will be limited to what is strictly necessary for the performance of its function.

## **5. Procedure of the Internal Information System**

### **5.1. Access**

Persons who have information or reasonable indications of a possible Non-Compliance must report it through the Internal Information System (IIS). The use of this system is confidential and will not result in any type of retaliation, provided that the communication is made in good faith and in accordance with the requirements set forth in Article 35 of the Whistleblower Protection Act.

Communications may be submitted in writing, via the email address: [alertahuaweisp@huawei.com](mailto:alertahuaweisp@huawei.com), verbally, or by both means, at the informant's discretion, through the channels enabled for this purpose.

All verbal communications, including in-person meetings, must be documented through recording and subsequent full transcription. The Whistleblower will be informed in advance of the recording, and once transcribed, they may review it, request corrections, and validate it by signing.

Regardless of the medium used, the Whistleblower will be provided with clear and accessible information about:

- the External Channels enabled by competent authorities, specifically the following, among others:
  - the Independent Whistleblower Protection Authority (AAI);
  - the competent authorities of the autonomous community, such as the Madrid Transparency Portal;
  - the institutions or bodies of the European Union;

Either directly or after having previously communicated the matter through the corresponding Internal Information System of Huawei.

- the processing of personal data applied to the information provided during the handling and resolution of the Communication.



<Translation, the Spanish version shall prevail>

When the Communication is submitted in writing, the form available as **Annex I** of this document must be completed. In any case, the Communication must include, at a minimum, the following elements:

- **Identification of the Informant**, unless they choose to remain anonymous.
- **Data of the Affected Person**: first name and last name, and any other relevant information that facilitates their identification.
- **Detailed description of the facts**, circumstances, and reasons that, in the informant's opinion, constitute a Breach.
- **Available documentation or evidence**, as well as identification of possible witnesses or persons knowledgeable about the facts.
- **Conflicts of Interest**, if applicable, related to the Communication and that could affect the Informant, the SII Responsible, members of the Investigation Commission, or the Administrative Body.
- **Secure contact information** (address, email, or alternative means) for receiving notifications related to the case, which can be modified later through the SII.

## 5.2. SII Officer

The SII Officer will be the Compliance Officer, who will direct and supervise the operation of the SII, including the reception, analysis, admission or rejection for processing, and the processing of cases derived from received communications.

The SII Officer will act at all times with full independence, impartiality, objectivity, and neutrality, performing their duties with integrity and in accordance with the provisions of this document and the Whistleblower Protection Act, as well as other applicable regulations.

## 5.3. Reception of the Communication

The SII Officer will manage and process the files derived from communications received through the SII.

Upon receiving the communication, the SII Officer will proceed to:

1. Register the Communication in the Communication Register, indicating the date of receipt; and
2. Assign a unique file number or identification code for traceability.

The SII Officer will send the Informant a receipt acknowledgment of the Communication within a maximum period of seven (7) calendar days from its receipt, unless such acknowledgment could compromise the confidentiality or proper handling of the provided information. The lack of a



<Translation, the Spanish version shall prevail>

receipt acknowledgment within the legal timeframe will not, under any circumstances, imply the acceptance of the Communication.

#### **5.4. Admission or Non-Admission of the Communication for Processing**

Once the communication is registered, the SII Officer will evaluate whether it should be admitted for processing, based on the criteria detailed below:

- Only communications that clearly and sufficiently describe facts that could constitute a Non-Compliance will be admitted for processing.
- Among others, the following cases will not be admitted for processing:
  1. **Non-Constitutive Facts of Non-Compliance:** when, clearly, the facts presented do not fall within the scope of application of the SII.
  2. **Communications made under threat or coercion.**
  3. **Communications made in bad faith**, understood as such, among others:
    - (i) Those that are not based on reasonable indications of possible Non-Compliance;
    - (ii) Communications supported by evidence or information obtained illegally;
    - (iii) Communications in which the Informant is aware of the falsity of the facts or acts with manifest disregard for the truth.

The use of the SII in bad faith may result in the application of the appropriate disciplinary or legal measures, and the Informant may be held responsible for any liabilities that arise.

Before deciding on admission or non-admission, the SII Responsible may request additional information or supplementary documentation from the Informant to properly evaluate the reported facts. The final decision on admission or non-admission will be communicated to the Informant by the SII Responsible.

In the case of non-admission, the Communication will include the reasons justifying it and inform the Informant of their right to rephrase the Communication or pursue other legal avenues they deem appropriate.

In the case of admission for processing, the SII Responsible will transfer the file to the Investigation Commission, which will be responsible for conducting the investigation and analysis of the facts as provided in this document.

Additionally, if the reported facts could constitute a crime, the file will be immediately forwarded to the Public Prosecutor's Office. If they affect the financial interests of the European Union, it will be transferred to the European Public Prosecutor's Office.



## 5.5. Processing of the Case

Once the Communication is admitted for processing, the SII Responsible will transfer the case to the Investigation Commission, which will be responsible for carrying out the necessary actions for the processing and instruction of the case.

### 5.5.1. Preliminary Procedures

The Investigation Commission will carry out, prior to the instruction phase, the following actions:

- **Identification of participants:** it will prepare a list of the individuals who will participate in the analysis and investigation process, including members of the organization and, if necessary, external advisors whose involvement is required for the proper management of the case.
- **Confidentiality agreements:** all individuals participating in the investigation must sign, prior to their participation, a confidentiality agreement and a conflict-of-interest statement. **Annex II** includes the corresponding agreement model.

If during the instruction phase it becomes necessary to involve new individuals not initially included, the Investigation Commission must obtain this agreement before allowing access to any information in the case.

- **Protection of personal data:** it will be ensured that the handling of personal information managed during these procedures complies with the current regulations on the protection of personal data and the internal procedures established for this purpose.

### 5.5.2. Investigation Phase

The Investigation Commission will be responsible for coordinating and directing the investigation phase, carrying out all necessary actions and verifications to verify the accuracy, consistency, and truthfulness of the received information, as well as to clarify the facts subject to the Communication.

During this phase, appropriate actions will be taken with full respect for the rights of the affected persons and other participants. For these purposes:

1. **Information to the Affected Person:** generally, the Affected Person will be informed of the existence of the Communication and the start of the investigation process. This communication may be postponed if there is a real risk of compromising the effectiveness of the investigation or the obtaining of evidence.
2. **Hearing of the Affected Person:** once informed, the hearing procedure will begin, which will include, at least, an interview with the Investigation Commission, where the Affected Person will be informed of the facts under analysis and will be allowed to present their version, accompanied by any evidence they consider appropriate.



<Translation, the Spanish version shall prevail>

All of this without prejudice to the right of the Affected Person to submit written statements.

3. **Investigation Actions:** the Investigation Commission may carry out any necessary procedures, including:
  - Request for testimony from affected, involved, or witness persons;
  - Interviews and hearing procedures with the parties involved;
  - Request for documentation, evidence, or relevant supplementary information.
4. **Advisory and Collaboration:** The Investigation Commission may seek the collaboration of other internal areas or external advisors, when necessary, always ensuring the confidentiality of the Informant, third parties involved, and the communication itself.

The involvement of the legal and human resources departments will comply with what is set out in section 3.1 of this document.

5. **Documentation of Actions:** for each action taken, especially interviews, meetings, and statements, a report must be prepared and signed by the persons involved to verify its content.

All documentation will be incorporated into the file with the same security and confidentiality guarantees as the rest of the information.

6. **Investigation Report:** upon completion of the investigation, the Investigation Commission will issue an investigation report that will include, at a minimum:
  - Description of the reported facts, referring to the file number and date of receipt;
  - Actions and procedures carried out, along with their results;
  - Conclusions reached, including the identification of any control deficiencies that may have facilitated the situation;
  - Proposal for resolution of the file and, if applicable, corrective, disciplinary, or preventive measures to be adopted.

## 5.6. Resolution

Upon completion of the investigation phase and receipt of the investigation report issued by the Investigation Commission, the SII Officer will issue the corresponding resolution, evaluating the conclusions of the case.



<Translation, the Spanish version shall prevail>

The resolution will be communicated to the Informant and the Affected Person with due diligence and ensuring the confidentiality of their identity, except in cases where there is a legal obligation to disclose it.

The instruction and resolution process must be completed within a maximum period of three (3) months from the receipt of the Communication. This period may be extended by an additional maximum of three (3) months if the complexity of the case requires it, as established in the Whistleblower Protection Law.

The absence of an express resolution within the legal timeframe will not, under any circumstances, imply the acceptance of the communication or the validation of the reported facts.

## **6. Management and Archiving of Information**

The SII Officer will ensure the proper management, custody, and traceability of information related to communications received through the SII. All documentation generated during the processing of Communications—including their registration, actions taken, evidence collected, investigation reports, and resolution—will be kept securely and confidentially.

Only persons strictly authorized to manage the case file will have access to this information, maintaining the confidentiality required by the Whistleblower Protection Law. Information may only be disclosed when necessary for the processing, investigation, or resolution of the Communication, or when required by a competent authority within the framework of a legal procedure.

Personal data processed under the SII will be retained for the time necessary to decide on the admission of the case and, in any case, for a maximum of three (3) months from the receipt of the Communication. After this period, they must be deleted, unless it is necessary to block them to verify the system's operation or to continue the investigation based on another regulation that allows it.

## **7. Conflicts of Interest**

During the management and processing of communications received through the Internal Information System, it must be ensured at all times that the independence, impartiality, and absence of conflicts of interest of the individuals involved in the procedure are maintained.

A Conflict of Interest will be deemed to exist when there are personal, professional, or any other circumstances that may compromise or influence the objectivity, neutrality, or independence of any of the individuals involved in the reception, analysis, investigation, or resolution of the Communication, including the SII Responsible, members of the Investigation Commission, or any other person participating in the case.

In such cases, the following rules will apply:

- Any Person Affected by a possible Conflict of Interest must immediately report it, refraining from intervening in the case from the moment they become aware of it.



<Translation, the Spanish version shall prevail>

- If the conflict affects the SII Responsible, they must inform the Administrative Body or the appropriate body so that another person can be designated to assume their functions regarding the affected case.
- If the conflict affects any member of the Investigation Commission or any other person participating in the process, that person must be removed from actions related to the case, and a substitute must be appointed to ensure the independence and proper processing of the case.
- The person appointed as a substitute must have the necessary independence, suitability, and training to assume the role with full impartiality.

The existence of a Conflict of Interest, as well as its management, substitution, and measures taken to ensure the independence of the procedure, must be documented internally in the case file, preserving the confidentiality of the information.

Failure to comply with the obligation to report a Conflict of Interest or to abstain from intervening may be considered an internal violation and may result in appropriate measures, depending on the severity of the violation.

## **8. Confidentiality**

The identity of the Informant, the Affected Person, and any third party mentioned in the Communication will be treated with strict confidentiality and cannot be disclosed without the consent of the Affected Person, except when it constitutes a legal obligation or is necessary within the framework of an investigation, administrative, disciplinary, or judicial procedure.

The SII must be designed to ensure restricted access exclusively to the SII Responsible, members of the Investigation Commission, and, if applicable, persons expressly authorized according to this document, as well as confidentiality at all stages of the procedure.

## **9. Data Protection**

Personal data processed under the SII will be managed in accordance with the GDPR, the LOPDGDD, and the Whistleblower Protection Act. The legal basis for processing will be the fulfillment of a legal obligation.

Only the SII Responsible, members of the Investigation Commission, and, if applicable, those individuals whose intervention is strictly necessary and who have been expressly authorized, as well as, when appropriate, competent authorities, may access the data. Access to personal data will be limited to the minimum necessary to fulfill the assigned functions, applying the principles of minimization, access limitation, confidentiality, and necessity.

Data will be retained according to the legally established periods and blocked when they are no longer necessary, without prejudice to their retention when required to verify the operation of the SII, for the processing of administrative, judicial, disciplinary procedures, or for the exercise, defense, or fulfillment of claims.



<Translation, the Spanish version shall prevail>

Whistleblowers and affected individuals may exercise the data protection rights that apply to them, ensuring in any case the protection of the whistleblower's identity.

## **10. Protection of Informants**

All persons who communicate information in the circumstances provided for in the Informant Protection Act shall be entitled to the protection provided therein, provided they act in good faith, have reasonable grounds to believe the information communicated is true, and comply with the legal requirements.

Any form of retaliation, direct or indirect, against the informant or against any person who has collaborated in the investigation, due to the communication made or their participation in the procedure, is strictly prohibited.

## **11. Information on the System and External Channels**

Huawei will provide clear and easily accessible information on how the SII and External Channels operate to competent authorities, including the Independent Whistleblower Protection Authority (A.A.I.).



<Translation, the Spanish version shall prevail>

### COMMUNICATION FORM

Anonymous communication

Identifying Data of the Informant:

Department:

Position (*employee/executive/member of the board of directors*):

Contact Information:

Identifying Data of the Affected Person:

Department:

Position (*employee/executive/member of the board of directors*):

Narrative of the facts allegedly constituting non-compliance, indicating the place and date on which they occurred:

Documents and evidence:

Other possible witnesses:

Statement of a possible Conflict of Interest situation: