Guidelines of the request collection and reporting system

These guidelines are established in accordance with the laws and texts dealing respectively with:

- *The labor code,*
- *Health and environmental alerts,*
- *The General Data Protection Regulation (GDPR),*
- *The code of civil service and ethics of civil servants,*
- *Ethics of the research profession and scientific integrity,*
- *Transparency and the fight against corruption,*
- *Whistleblowers protection and procedures for collecting and processing their reports.*

The corresponding references are available at the end of the document.

1. Introduction – what is this system, and why is it important?

Our institution strives to combine transparency with a high level of professional ethics. Our reference framework in these matters is Cirad's Code of Ethics, which stipulates respect for human values, laws and regulations and, more specifically, for the terms and conditions of research partnership and scientific integrity.
The service that we are setting up puts us on a virtuous path towards these objectives and ensures whistleblowers protection. It is based on a dedicated secure platform guaranteeing the confidentiality of exchanges and the protection of its users and enabling the collection and transmission of:

- Information or support requests in terms of ethics (in the general sense or in the sense of the ethics of civil servants) and scientific integrity, so that they can be handled adequately.
- Alert reports of risks that may impact the actions carried out by the institution (see the "**When to send an alert?**" section).

By allowing us to detect possible dysfunctions as soon as possible and to act on them, this tool is important for both ensuring the dissemination of a culture of ethics and scientific integrity within the institution and maintaining the trust placed in us. The platform is thus accessible to all those involved in Cirad's activities, whether they are employees or not (students, partners, collaborators, administrators, clients, suppliers, co-contractors, subcontractors, consultants, etc.).

2. When to send an alert?

The request collection and reporting service may be used to alert of serious risks affecting individuals, the institution, society, the conduct of research or the environment. Alerts must be made through the platform in order to allow for proper referral and processing of the case, as well as to ensure the protection of the persons making them (who may be whistleblowers in cases corresponding to this definition).
Issues that may be reported include potential breaches of ethics or scientific integrity, misdemeanors, irregularities and violations of laws in a work-related context. However, items covered by secrecy (in the sense of national defense, medical secrecy, the secrecy of judicial deliberations, the secrecy of the investigation or judicial inquiry, or attorney-client privilege) cannot be reported.

Reasons for reporting may be, for instance:

- ***Corruption and financial irregularities****; for example, bribery, unfair competition, money laundering, fraud, conflict of interest*
- ***Health and safety violations;*** *for example, workplace and personal health and safety, product safety, discrimination and harassment*
- ***Violations of Human rights and fundamental freedoms***
- ***Environmental violations;*** *for example, illegal dumping of hazardous waste*
- ***Violations of privacy;*** *for example, misuse of personal data*
- ***Public service ethics*** (only for claims concerning the rights and duties of civil servants)
- ***Breaches of Cirad's Code of Ethics***
- ***Research misconducts*** *(frauds such as fabrication, falsification, plagiarism; any other form of misconduct).*

A whistleblower does not need to have compelling evidence in order to express a suspicion. However, deliberate reporting of false or defamatory information is not acceptable and any abuse of the whistleblowing service is a serious offence that may lead to disciplinary action.
Depending on the case, the report may be made anonymously at first. However, the appropriate treatment of certain alerts may make it necessary to lift anonymity: in such a case, the message author's identity will only be known to the investigation team.

3. How to send a request or a report?

You may:

- **Option 1:** send a message through the platform: https://report.whistleb.com/en/cirad.
- **Option 2:** directly get in touch with a point of contact (référent) within the organisation, who will then log in your request or report on the platform.

In both cases, all messages received will be treated as strictly confidential.
The whistleblowing platform is administered by WhistleB, an external service provider based in Europe. All messages are encrypted. To ensure the anonymity of the person sending a message, WhistleB does not record IP addresses or metadata.
The message sender may decide to remain anonymous when getting in touch with the investigation team. Once the message is deemed admissible and if lifting anonymity is ever required in the course of case processing (e.g. processing of scientific integrity issues), this will be done with the authorisation of the person and confidentiality will be preserved. However, this prior authorization will not be required for facts that must be brought to the attention of the judicial authority, and the sender of the message will be informed insofar as this does not compromise the proceedings.

4. The investigation process

THE INVESTIGATION TEAM
Access to messages received through the platform is restricted to appointed individuals with the authority to handle requests and alerts within the institution: these include, in particular, the

focal points (référents) for ethics and scientific integrity, occupational health and safety, harassment, the delegation for legal affairs and compliance, the work psychologist, etc. Their actions are recorded in the platform's event log and processing is confidential. When deemed necessary for the investigation, experts may be invited to access case data on the platform. These persons are also bound to confidentiality.

RECEIVING A MESSAGE

Upon receiving a message, the instruction team examines its admissibility within 7 days.

The investigation team may reject a message if:

- The reported facts do not correspond to a request for information or support nor to a report according to the procedures in place;
- The message has not been made in good faith or is malicious;
- There is insufficient information to allow for further investigation;
- The subject matter of the message has already been addressed.

If a message concerns matters not covered by the categories of requests or reports in these guidelines, the investigation team may, where appropriate and with the consent of the sender, refer the message to the competent persons or services.
If the message is admissible, the appropriate investigation procedure for the type of request or report is implemented, under the coordination of the appropriate person(s) within the institution (for example the scientific integrity officer, in the case of a message related to this field). Regardless of the conclusion of the admissibility examination phase, the author of the message will be informed.
In the case of an alert, the respondent(s) will be informed within a month. When precautionary measures are deemed necessary in order to secure elements that may be used as evidence during the investigation of the case, the respondent(s) is/are informed after these measures have been implemented.

INVESTIGATION

All messages are handled with care and according to strict rules:

- Confidentiality: prior to any participation in the processing of a message or in an investigation, experts from within or outside the institution are required to sign a confidentiality agreement. This agreement prohibits the dissemination of any information (identification of the protagonists of the case or of the persons involved in its processing, elements of the investigation, etc.) outside the scope of the investigation team.
- Respect for anonymity: no one, either within the investigation team or among the people involved in processing, is authorized to attempt to identify the person who makes an anonymous report.
- Impartiality, neutrality: each person in charge of case processing or invited to contribute to it is required to fill in a declaration of interests and to update it on a regular basis. The examination of this declaration under the responsibility of the referent(s) concerned enables the identification of potential conflict of interest and ensures that the investigation will never be entrusted to a person likely to be directly or indirectly involved in the case, or to show a bias.

Each admissible request or report will be treated according to its nature by the focal point (référent) within the establishment (see above "**The investigation team**"), according to the appropriate procedure.

In cases where there is no specific procedure, an alert that is deemed admissible will be processed as follows:

- An *ad hoc* focal point is designated within the investigation team to coordinate the investigation of the case.
- He/she forms and coordinates a processing committee (PC).
- The PC is in charge of investigating the alert, which involves: i) qualifying the reported facts and ii) determining their reality and level of seriousness; iii) implementing any action necessary for the investigation of the case (identifying and interviewing the parties concerned, collecting and examining relevant information, possibly implementing additional precautionary measures, inviting external experts, etc.); iv) writing a report presenting the information collected and their analysis; and issuing recommendations for the head(s) of the concerned institution(s).

Regardless of the procedure, once the alert has been processed the investigation team will attempt to respond to the author of the message within 3 months of the date of the acknowledgement of receipt. However, in complex cases (e.g.: investigation involving several institutions or countries), longer response times are to be expected.
The operational decision regarding the follow-up to the processing of the case (leading to different types of measures: scientific, disciplinary, organizational, support, legal, etc.) on the basis of the produced report is the responsibility of the head of the concerned institution. From the time the report is submitted, this decision is made within a maximum of 2 months in the case of a person subject to labor law (as is the case for Cirad employees), or 3 years in the case of a civil servant.

5. Protection and privacy

WHISTLEBLOWER PROTECTION
A person who blows the whistle as a mean to express genuine suspicion or misgivings will not be at risk of losing their job or suffering any form of sanctions or personal disadvantages as a result. The whistleblower may be mistaken, as long as he or she is acting in good faith.
Subject to respect for the right to protection of personal data, whistleblowers who have identified themselves and the persons targeted by the alerts are kept informed of the outcome of the investigation.
In the case of reports of suspected offences, the whistleblower will be informed if his or her identity is transmitted to the judicial authorities.

PROCESSING OF PERSONAL DATA
Cirad, as data controller, collects information to promote ethical and transparent partnership research. As part of the management of the whistleblowing platform, this data is processed on the basis of Cirad's legal obligations or its legitimate interest.
The collected and processed information is related to:

- Identification data (surname, first name) of the persons concerned by the alert or the request, or by its processing (with the exception of the whistleblower, if they have elected to remain anonymous);
- The facts reported and the elements collected in the context of their verification;
- The stages in the investigation of the case and their documentation.

This information is intended only for competent and authorized people within Cirad, who treat it as confidential. If necessary it may be transmitted to the competent authorities.

The personal data associated with messages deemed inadmissible will be anonymized or deleted without delay.
Regarding admissible messages, the data will be kept for the time necessary to process the alerts received and to monitor their consistency over time according to the procedures provided for in the type of alert. In all cases, data that are not necessary for the investigation (in particular, the mention of unrelated third parties) will be destroyed when the case is closed by the focal point in charge, i.e. on the date when an official decision on the action to be taken has been made by the head of the institution following transmission of the report.
In the absence of disciplinary proceedings or legal action, the case is closed by the referent in charge. After 30 days, the case file is archived in an anonymous and non-modifiable form on the platform (intermediate archiving).
However, in the context of Cirad's legal or regulatory obligations, data may be kept for a longer period:

- When disciplinary proceedings are initiated (against the person concerned or the author of an abusive alert), the data relating to the alert and its processing are kept for a period not exceeding the limitation period for legal action challenging the disciplinary measure that may have been decided.
- In the event of legal proceedings being taken (against or on the initiative of the person concerned or the author of an alert), the data relating to the alert and its processing are kept until the proceedings have been completed and all means of appeal have been exhausted.

Once these additional time limits have elapsed, the case file will be closed and archived in accordance with the procedures set out above.
In cases of scientific misconduct, the period between the closure of the file and its archiving in anonymized form is extended to 3 years. This duration corresponds to the period beyond which no previous disciplinary sanction may be invoked in support of a new sanction concerning persons subject to labor law, such as Cirad employees.

WhistleB (Whistleblowing Centre Ab, World Trade Centre, Klarabergsviadukten 70, SE-107 24 Stockholm, Sweden) acts as data processor in the context of the processing carried out by CIRAD through the whistleblowing platform. These processing operations include the management of encrypted reporting messages, which WhistleB and its subcontractors cannot decrypt or read: thus, neither WhistleB nor its subcontractors have access to the unencrypted content.
The personal data collected and processed on the platform are protected by appropriate technical and organisational measures to ensure a level of security commensurate to the risk.

In accordance with Regulation (EU) 2016/679 (GDPR) and local data protection law, in particular French 78-17 "Informatique et Libertés" Law dated 1978 January 6th in its modified version, you are entitled the rights of

access, modification, erasure and portability (when applicable) of your personal data, and of limitation and opposition of its processing, with the right to withdraw your consent at any time. You can claim those rights by writing to our Data protection Officer (dpo@cirad.fr). You also have a right to submit a complaint directly to the appropriate data protection Supervisory Authority.

References

- **Health and environmental alerts:** law n° 2013-316 of 16 April 2013 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027324252/ and decree n° 2014-1628 of 26 December 2014 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029965466/.
- **The General Data Protection Regulation (GDPR):** regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679.
- **The ethics of civil servants:** law n° 2016-483 of 20 April 2016 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032433852 and decree n° 2017-519 of 10 April 2017 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034411018.
- **Ethics of the research profession and scientific integrity:** Réseau National des Référents à l'Intégrité Scientifique: "Guide pour le recueil et le traitement des signalements relatifs à l'intégrité scientifique", November 2018 : https://www.hceres.fr/sites/default/files/media/downloads/2018_Guide-traitement-signalements-IS_RESINT.pdf . Conseil Français de l'Intégrité scientifique : "Vade-mecum pour le traitement des manquements à l'intégrité scientifique, à l'usage des chefs d'établissements", June 2019 : https://www.hceres.fr/sites/default/files/media/downloads/2018_Guide-traitement-signalements-IS_RESINT.pdf . Decree n° 2021-1572 of 3 December 2021 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000044411360.
- **Transparency and the fight against corruption:** law n° 2016-1691 of 9 December 2016 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033558528 and
- **Whistleblowers protection:** directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L1937 . Law n° 2022-401 of 21 March 2022 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000045388745.
- **Procedures for collecting and processing whistleblower reports:** decree No. 2022-1284 of 3 October 2022: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046357368.
- **Labor Code - Disciplinary Procedure - Articles L1332-4 and L1332-5:** https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072050/LEGISCTA000006177888/#LEGISCTA000006177888
- **General Civil Service Code - Disciplinary Procedure - Article L532-2:** https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044425430
- **Cirad's Code of Ethics:** https://www.cirad.fr/en/Media/espace-docutheque/docutheque/fichiers/cirad-code-of-ethics-december-2017