COMPLIANCE ALERT SYSTEM
MasterGrid Group

I. Introduction – Management Commitment

MasterGrid Group management affirms its commitment to promoting a culture of ethics, transparency, and accountability in business practices. This Compliance Alert procedure is a key tool to prevent, detect, and address any breaches of legal and ethical rules applicable to our activities.

The process is designed to allow employees to report any potentially harmful situation or incident to MasterGrid, including safety issues, unethical behavior, fraud, or any activity that could harm the Group.

1.1 Legal Framework

The system complies with:

- Law No. 2016-1691 of December 9, 2016, on transparency, the fight against corruption, and the modernization of economic life, commonly known as the "SAPIN 2 Law."
  Article 8, paragraph III, of this law provides: "appropriate procedures for collecting reports from their staff members or from external and occasional collaborators shall be established by legal entities under public or private law with at least fifty employees […]."

- EU Directive 2019/1937 on whistleblower protection, transposed by Law No. 2022-401 (Waserman Law)

- Labor Code provisions on employee rights and obligations

1.2 Objectives

The implementation of the Compliance Alert system allows the MasterGrid Group to meet various objectives:

- Enable reporting of serious issues or threats to the public interest or MasterGrid operations
- Protect employees and assets by ensuring a safe work environment
- Strengthen legal compliance and anti-corruption efforts
- Foster a culture of openness and transparency

Management considers that each report constitutes an opportunity for improvement and is committed to treating these alerts seriously, impartially and confidentially.

1.3 Scope

Who can report?

This system applies to:

- All MasterGrid employees (permanent, temporary, interns, apprentices)
- Business partners, suppliers, subcontractors, administrative partners
- Any person aware of relevant acts or behavior

What can be reported ?

The system covers:

- Violations of laws, regulations, or international treaties
- Corruption, fraud, or influence peddling
- Environmental, health, or public safety threats
- Discrimination, harassment, or behavior contrary to MasterGrid values
- Any other breach affecting the public interest or company operations

II. Whistleblower Status

2.1 Recognition Criteria

Any person who meets the following conditions is recognized as a whistleblower:

- Have personal knowledge of the facts through professional activity
- Act in good faith, without financial gain or intent to harm
- Follow the procedure steps (internal reporting first, then external if needed)

2. 2 Protection

In accordance with the law, Management guarantees the following protections:

- Strict confidentiality
- No retaliation (no sanctions, discrimination, or dismissal)
- Civil and criminal immunity
- Support from internal referent or legal assistance

Any violation of these protections subjects those responsible to disciplinary and legal sanctions.

III. Exercising the Right to Alert

3.1 Internal Reporting

Internal reporting consists of an alert addressed directly to MasterGrid. It can be carried out using internal Group tools/channels but also using an external channel for people who do not have access to internal tools/channels. Internal reporting is encouraged as a first step, except in cases of serious and imminent danger justifying direct external reporting (see 3.2).

The dedicated reporting channels are as follows:

- A form accessible 24/7
    - via the Group's intranet under the "Legal Section"
    - via the MasterGrid website under the "Commitment" section.
- A dedicated email address: alerte.compliance@mastergrid.com

At their option, the Employee can also ask their line manager, the HR department or the Legal Department in order to jointly complete the dedicated form.
When using the dedicated form, the following information will be required from the submitter:

- First and last name
- Submitter's contact information (email address and telephone number)
- Date of incident
- Detailed description of the report
- Persons involved, if known
- Relevant evidence or documents, if available (not mandatory)

3.2 External reporting

If internal reporting is ineffective or in case of serious danger, contact a competent authority: (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046357368)

IV. Alert Handling

Once a report is received, MasterGrid undertakes to conduct an impartial and rigorous internal investigation to verify the facts and act accordingly.

4.1 Reception and Registration

Any report will be received by a college of Directors (named “Alert Group”) made up of people exercising the following functions:

- The President and General Managers of the MasterGrid Group.
- The Director of Human Resources
- The Legal Director (also fulfilling the function of “Alert Referent”)
- The Administrative and Financial Director

This Group guarantees neutrality, confidentiality and the absence of conflicts of interest. If necessary, internal and/or external experts can be called upon (IT, legal advice, independent auditors, etc.).
An acknowledgment of receipt of the report will be sent to the Whistleblower within a maximum of 7 working days, confirming that the report has been taken care of.

4.2. Preliminary Evaluation

A preliminary assessment meeting of the report will be organized within 10 days at the initiative of the Alert Referent. On this occasion, the Whistleblower may be contacted again by the Alert Referent in order to provide as much information as possible for the holding of this meeting.

The preliminary assessment will determine:

- The admissibility of the report (facts consistent with the scope of the alert).
- The seriousness and urgency of the facts.
- Possible risks for MasterGrid and/or third parties.

Based on these elements, the Alert Group will decide on the nature of the report:

- Non-serious / No action: the report will be closed and the closure information will be communicated to the issuer.
- Serious / Follow-up: a working pair will be appointed within the Alert Group in order to carry out an internal investigation (with or without the involvement of a third-party firm previously referenced in the supplier database). The sender will be informed of the admissibility of the report and will benefit from the status of whistleblower.

4.3 Investigation

In the event that the report is analyzed as serious by the Alert Group, a mission letter will be sent to a working pair, within the Alert Group, who will carry out an internal investigation. The mission letter must specify the investigation period, the locations and the people and/or business units which will be the subject of this internal investigation.

The internal investigation will be carried out within a reasonable time, proportional to the complexity of the facts without exceeding a period of 3 months from receipt of the report.

The pair of investigators will collect all the evidence necessary but strictly limited to the progress of the investigation, will interview the witnesses and the people involved while respecting the presumption of innocence and the principle of adversarial proceedings.

At the end of the investigation, a confidential report will be drawn up with the conclusions and recommendations following the standard plan below:

Standard outline of the internal investigation report:

- Mission letter: specifying the period, locations and people/business units subject to the investigation.

- Composition of the mission

a) Holders of the mission – names of natural persons who contribute to the execution of the mission

b) Assistance: names and mission of any assistants

c) Practical progress of the investigation: travel, hearings carried out, dates of investigations, working methods followed, precautionary measures possibly put in place

- Detailed presentation of the investigation results: list of all acts and operations noted.

- Conclusions of the investigation: facts whose proof was reported thanks to the investigative actions.

- Appendices including in particular documentary evidence and reports or minutes of interviews enabling the conclusions of the mission to be drawn.

4.4 Results and Action Plan

At the end of the drafting of the investigation report, a feedback meeting with the Alert Group will be organized by the Alert Referent and the pair of investigators. Based on the conclusions of the investigation, Groupe Alert will define and implement an action plan to correct the breaches and prevent their recurrence.

1. Immediate corrective actions

- Disciplinary sanctions: If misconduct is proven, proportionate sanctions are applied in accordance with the internal regulations and legislation.
- Preventive measures: Suspension of risky activities, strengthening of internal controls, review of procedures.

2. Medium / long-term actions

- Training and awareness: Organization of specific sessions to remind you of MasterGrid's ethical rules and commitments.
- Process improvement: Review of internal policies or procedures that allowed the reported events to occur.
- Strengthening governance: Implementation of additional control systems or creation of new monitoring tools.

3. Monitoring and evaluation

- Management ensures the proper execution of the action plan.
- Monitoring indicators (KPIs) will be defined to evaluate the impact of the measures taken.
- A periodic audit can be carried out to ensure the sustainability of corrective actions.

At the end of the restitution meeting, a response will be sent to the Whistleblower, informing him of the measures envisaged or taken, in compliance with confidentiality rules and legal obligations, and of the closure of the report. He will be informed in writing, within a reasonable period of time which may not, in any case, exceed a period of 3 months from acknowledgment of receipt of the report.

V. Communication and training

Management is committed to ensuring clear and accessible communication on the establishment and operation of the internal alert system.

5.1 Information access

The internal alert procedure will be made available to all employees and stakeholders by the following means:

- MasterGrid Intranet.

- Display on information panels.

- Welcome booklet for new employees.

- Specific communication by email or during team meetings.

The procedure is available in Englis and French.

5.2 Awareness and training

To ensure the effectiveness of the system, a communication program will be put in place for all MasterGrid Group employees.

1. Employee awareness :

Objective: Raise awareness among all employees of the importance of the system, the types of facts that can be reported and the protections granted.

Content :

- Presentation of the system and reporting channels.
- Rights and obligations of whistleblowers.
- Confidentiality and protections offered.
- Consequences of reports on the operation of MasterGrid.

Terms: General communication of the system.

2. Alert Group training :

Objective: Guarantee that the Alert group responsible for processing alerts has the necessary skills to conduct impartial investigations and protect whistleblowers.

Content :

- Investigation methodology.
- Legal and ethical framework.
- Management of confidentiality and conflicts of interest.

Modalities: Specific information session

5.3 Continuous improvement

1. Return of Employees

Anonymous surveys may be carried out to assess employees' understanding and adherence to the system.

The feedback will be used to adapt training and communication materials.

2. Audit of the system

Management will carry out an annual audit to verify the effectiveness and accessibility of the internal alert system.

The results of this audit will be presented to the Management Committee and will be the subject of information to the Social and Economic Committee (ESC)

5.4 Management Commitment

MasterGrid Management reaffirms that communication and training are essential pillars to guarantee the effectiveness of the internal alert system. It is committed to providing the necessary resources to raise awareness and train each employee, while promoting a work environment where transparency and integrity are valued.