**Group policy**
**Guidelines**

# “Fighting against fraud”

| | |
|---|---|
| **Scope** | This policy applies to all EDF group entities, excluding regulated infrastructure entities. |
| **Upline reference(s)** | Group Ethics and Compliance Policy |
| **Downline reference** | Associated supporting guide |
| **Owner** | Executive Secretary |
| **Author** | Group Ethics and Compliance Department |
| **Version** | 1.2 |
| **Signature date** | 18 April 2017 |
| **Application date** | 1 June 2017 |

# I. General Objectives

"Fraud consists of deliberately deceiving others to obtain an illegitimate gain, or to circumvent legal obligations or organisational rules. Fraudulent behaviour implies a factual and intentional element, and the concealing of the unauthorised action"[1].

Fraud may arise from either internal or external sources and may manifest itself in different forms: misappropriation of funds (fake invoices, manipulation of cheques or other forms of payment, etc.) theft or destruction of property belonging to the company (supplies, equipment, data, etc.), or false declarations (fake expense receipts, undeclared absences from work, falsified reporting statistics, etc.).

The fight against fraud is imperative: fraud is expensive, can seriously harm our reputation, and it threatens the shared trust that is the company's cement.

Even though it is impossible for a prevention system to eliminate all risks of fraud, it is still essential, in order to promote a culture of integrity at all levels of the organisation, to put in place rigorous practises, and to constantly improve the efficiency of the existing internal inspection procedures. Assessing the probability of the occurrence of fraud - and its impact - must be part of the periodic process of risk assessment.

These guidelines, destined for managers, describe the requirements applicable to prevent, detect and respond to a suspicion of fraud. They will be supplemented by a supporting guide entitled "Fighting against fraud," which is designed to explain to the managerial line and the Fraud Officer (REC) the main checks to be carried out to help control the risks of fraud.

18 April 2017

Pierre Todorov
Executive Secretary of the EDF Group

[1] Definition of the "Institut Français de l'Audit et du Contrôle Internes" (French Institute of Internal auditing and control, a.k.a. IFACI)

# II. Requirements/methods

The EDF Group has adopted the principle of zero tolerance with respect to fraud in all its forms, applicable to all employees in the Group, whether they are senior managers, managers or other employees. Everyone should be made aware of this policy.

The Group Ethics and Compliance Policy (Section 7 - Fighting against fraud) recommends that the senior manager put in place a system appropriate to the level of risk exposure of fraud within their entity.

The fight against fraud is an integrated strategy based on a range of measures or actions with an aim towards:

- reducing the risk of fraud (see item II.1),
- detecting fraud (see item II.2),
- and responding to a fraud alert (see item II.3).

This strategy is part of logic of continuous improvement based on the operational experiences of the Group's entities.

## II.1) Reducing the risk of fraud

In accordance with EDF Group's internal inspection guide, preventing fraud is based on two requirements.

**Requirement #1 - A fraud risk assessment is developed annually[2] , and an action plan is drafted for the most serious risks. A Fraud Officer (the entity's Ethics and Compliance manager– hereinafter "REC") responsible for managing this action plan, is appointed by the senior manager of the entity.**

The fraud risk assessment and the plan of action are drafted by the REC, then validated by the entity's executive committee. These documents identify and prioritize the risks of fraud relating to the industrial, commercial, and support function processes (e.g. Purchasing, sales, treasury, personnel, fixed assets-stocks, accounting, etc.) of the entity.

The entity must be able to demonstrate that it has a plan to combat fraud commensurate to the risk identified in the risk assessment.

The fraud prevention plan defines the training/awareness raising, inspection, testing and reporting actions. The coordinators of these actions are identified and the results are tracked.

**Requirement #2 - Responsible for defining and implementing the action, the Fraud officer (REC) ensures employee awareness is raised, and that managers are trained in the risk of fraud related to their activity**.

Communications must regularly be made on the risk of fraud, in a format appropriate to the activities undertaken. It must be sent to all employees in the entity and be rooted in the Group's commitments in the areas of integrity and the protection of its reputation.

The employees should be made aware of the risk of fraud via concrete examples (purchasing, expense accounts, holidays, delegations, etc.). The awareness-raising action should set out the applicable rules, inform employees of their rights and duties, the means of alerting the appropriate persons, and any possible penalties.

[2] This feeds into the mapping of the Group's risks.

For managers: an emphasis is made on their responsibilities in terms of implementing preventive measures, detection, processing of Fraud alerts, reporting the cases processed, and the related best practices identified.

Training sessions should be organised on a regular basis. Training should be tracked (purpose, dates and participants). Instruction on fraud may involve information on the disciplinary or criminal penalties applicable, and, if necessary, include the use of actual internal cases (while preserving the anonymity of persons and checking with the Legal Department whether it is possible to communicate details about ongoing criminal enquiries).

The organisation of the Group is based on the division of responsibilities and on the checks associated with them. The system of separation of tasks and functions contributes to the quality and the safety of the fraud prevention system. The same goes for good practises in terms of access to the information system.

Each senior manager must put in place a clear, relevant, regularly updated system of delegation of powers (refer to the Legal Department's policy "Delegation of Powers").

## II.2) Detecting fraud

In accordance with EDF Group's internal inspection guide, detecting fraud is based on one requirement.

**Requirement #3 - Each entity implements an inspection plan and conducts random tests of industrial, commercial, and support function processes, according to the risks identified.**

An inspection/detection plan is carried out on the industrial and commercial processes as well as on the support function processes, on the basis of the entity's fraud risk analysis. This plan defines the standard checks to be carried out by managers and their frequency, the in-depth checks to be carried out in the event of detection of discrepancies, and whether they are in the entity or in the functional departments.

Referring to the supporting guide "Fighting against fraud" enables the entity to more easily detect areas of fraud related to the six major processes (Procurement; Sales; Cash management; HR.; Fixed assets / Stocks; Accounting). The procedures to be applied, the preventive measures, the elements of alert, and the checks to be implemented are detailed in each of the guide's theme sheets.

The entity documents and consolidates all the checks carried out, any flaws identified, and the corrective actions implemented.

Fraud is not only identifiable in the framework of the usual operational inspections. It is also necessary to use other systems in order to identify fraud, in particular being vigilant with respect to the existence of weak signals or alarm signals (see associated supporting guide - section 1.3) and the use of the Group's alert system (via the procedure managed by the Group Ethics and Compliance Department).

Lastly, the Internal Audit Department can identify, from the missions carried out, dysfunctions which increase the risk of fraud, or even actual clear cases, and formulate appropriate recommendations.

## II.3) Processing Fraud alerts

Appropriate processing of fraud alerts, is based on six requirements:

**Requirement #4 - Adapt the processing of fraud alerts according to the actual risks incurred.**

Three levels of alert exist based on the risks involved and the level of responsibility of the person(s) for handling them.

➔ **Level 1** is processed by the manager.

This level corresponds to fraud with no serious consequences, often carried out due to some variance with the usual internal procedures, and whose identification and assessment does not require complex research.

➔ **Level 2** is processed by the senior manager of the entity or the company manager. This level corresponds to fraud:

- whose impact does not cause any serious harm to the company's interests (even if the fraud can be referred for criminal prosecution); or
- whose impact is beyond the manager's area of responsibility, or in cases in which it is impossible to make an assessment without in-depth research or investigations in the computing system; and
- which does not carry the risk of immediate media coverage.

To treat the fraud alert, the senior manager of the entity or the company manager may rely on the expertise of the Group DHR and the Executive Secretary, in particular that of the Group Ethics and Compliance, Security and Economic Intelligence, Internal Audit and Group Legal Departments.

➔ **Level 3** is processed by a senior-level, ad-hoc working group.

These include cases where the fraud has been committed by a manager of the Group, or entails a significant and immediate media impact, or whose disclosure may cause serious harm to the Group's interests, or includes factual information susceptible to being exploited by third parties.

In this case, an ad hoc body is convened that combines the Group's Executive Secretary, the member of the Executive committee concerned, the Group Director of Human Resources, the Financial Director and a representative of the Group Ethics and Compliance, Communication and Legal departments.

At the fraud has been handled, the alert shall be closed by means of a summary report (description of the fraud, corrections made and any measures taken during the processing of the alert).

**Requirement #5 - Give priority to the managerial line.**

The direct manager must be informed of any alerts under his responsibility, and he/she, in turn, informs his or her own manager. If informing the direct manager appears inappropriate, the alert should be relayed to another member of the management at a higher level. If this is impossible, it is necessary to contact the entity's Ethics and Compliance Manager, by consulting the EDF website.

The entity's senior manager or the company manager is the only person who can authorise in-depth investigations, in particular in the computing system, under the oversight of the legal, IT and human resources functions.

**Requirement #6 - Respect the legal framework and observe the rules and values of the Group, taking care to:**

- implement the investigations and preservation measures overseen by the Legal Department:
- apply the rules of the Group IT Charter;
- respect the rights of the persons involved at each stage of the fraud investigation;
- be respectful of the rights of the person who first reported the fraud. He should not be punished or be subject to discriminatory measures if his alert was made in good faith.

**Requirement #7 - Protect the information exchanged.**

The identity of the persons involved must remain confidential.

Internal communications must be secured and limited to the persons involved in the processing, and there must be no internal or external communications made without the formal authorisation of the manager responsible for handling the alert.

Any data should be transmitted in confidential, encrypted mode, in accordance with Group rules.

The availability, integrity, confidentiality and traceability of all data must be preserved.

N.B. all written documents with a direct or indirect reference to the alert can be used as evidence by judicial authorities.

**Requirement #8 – Provide documents and inform the Group's Ethics and Compliance Department and, if necessary, the accounting department in clear cases of fraud.**

The Fraud Officer (REC) must describe the corrective measures put in place or have them described, as well as the relevant disciplinary action taken, whether this be internal (disciplinary committee) and/or external (criminal prosecution).

The Group Ethics and Compliance Department must be informed for purposes of consolidating Group reporting.

The Group Accounting Department must be informed of any allegations of fraud which may have an accounting or financial impact.

**Requirement #9 – Take appropriate sanctions in the event of fraud.**

The employee at question should be subject to disciplinary measures set out in article 6 of the Electricity and Gas Industries ("Industries Electriques et Gazières") statute or laid down in the Labour Code or in local legislation.

The employee may also face civil and/or criminal penalties.

# III. Organisation, management and monitoring of the guidelines

## III.1) Responsibility within the entities

The Fraud Officer (REC) oversees the implementation of these guidelines. He/she does not replace the managers who retain ownership of the risks of fraud in their area of responsibility. He/she shall coordinate the actions detailed in the entity's plan of action "Fighting against Fraud" and ensure that the fraud risk assessment, the training and awareness-raising actions and fraud tests are carried out. He/she centralises reporting on all cases of fraud processed by the entity.

The undertaking of an in-depth investigation of a case of fraud by a resource external to the Group must systematically be submitted to the Internal Audit Department.

## III.2) The improvement loop (operational experience)

The Fraud Officer (REC) shall periodically present a report to the management committee on the cases of fraud detected and treated, and explain any best practices identified based on the results of the actions taken.

He/she must provide to the Group Ethics and Compliance Department an annual report of the actions taken and the associated reporting carried out ("table of significant breaches").

## III.3) Management of the guidelines

The Ethics and Compliance Department is responsible for the management and monitoring of the implementation of these guidelines. It can conduct any verification action by contacting the member of the Executive committee concerned.

An Internal Audit may be carried out to assess the implementation of these guidelines and propose any necessary changes.

# IV. Detailed list of reference documents

| Documentary history | Statute |
|---|---|
| Fighting against fraud within EDF group: decision of 14 September 2010 | Superseded by these guidelines |
| Practical guide "Fighting against fraud within EDF group" | Superseded by these guidelines |
| How to process Fraud alerts: baseline for managers of EDF group - December 2014 | Superseded by these guidelines |
| Group Ethics and Compliance Policy 17 May 2016 | Upline reference(s) |
| Supporting guide "Fighting against fraud" | Downline reference(s) |

# V. Appendix

In the appendix to these guidelines, the Group Ethics and Compliance Department offers a support guide "Fighting against fraud" designed to explain to the entity's managerial line or Fraud Officer (REC) the key inspections to be carried out to contribute to the control of the risk of fraud associated with the major support function processes.