TABLE OF CONTENTS

TABLE OF CONTENTS....3
TITLE 1 - PURPOSE AND SCOPE....5
ARTICLE 1: PURPOSE....5
ARTICLE 2: SCOPE OF APPLICATION....5
ARTICLE 3: COMPLIANCE WITH THE RULES OF PROCEDURE....5
TITLE 2 - GENERAL DISCIPLINE....6
ARTICLE 4: GENERAL AND PERMANENT RULES....6
ARTICLE 5: RULES ENACTED BY SERVICE NOTES....6
ARTICLE 6: ACCESS TO THE ESTABLISHMENT....6
ARTICLE 7: WORKING HOURS....7
ARTICLE 8: TARDINESS AND ABSENCES....8
ARTICLE 9: PROTECTION OF PROPERTY AND MONITORING....8
ARTICLE 10: USE OF COMPUTER RESOURCES AND TELEPHONE TECHNOLOGIES....10
ARTICLE 11: FILMING - RECORDINGS....10
ARTICLE 12: PROTECTION OF THE SITE AND THE ENVIRONMENT....11
ARTICLE 13: GENERAL WORKING CONDITIONS AND DAILY LIFE IN THE ESTABLISHMENT....11
ARTICLE 14: RELATIONS WITH THIRD PARTIES....12
ARTICLE 15: PROVISIONS PERTAINING TO SEXUAL AND MORAL HARASSMENT, TO SEXIST ACTS AND THE PRINCIPLE OF NON-DISCRIMINATION....12
ARTICLE 16: OTHER REGULATIONS....14
TITLE 3 - HEALTH AND SAFETY....15
CHAPTER I: GENERAL PROVISIONS....15
ARTICLE 17: PRINCIPLE....15
ARTICLE 18: SANCTIONS....16
ARTICLE 19: EMERGENCY PROVISIONS....16

TABLE OF CONTENTS

CHAPTER II: GENERAL RISK PREVENTION MEASURES 17

ARTICLE 20: INFORMATION AND STAFF TRAINING IN DEALING WITH RISKS 17

ARTICLE 21: MEDICAL SURVEILLANCE 17

ARTICLE 22: RISK PREVENTION INSTRUTIONS 18

ARTICLE 23: SAFETY DRILLS 18

ARTICLE 24: MARKINGS AND SIGNS 18

ARTICLE 25: MOVEMENT AND CIRCULATION WITHIN THE ESTABLISHMENT 18

ARTICLE 26: RESTAURANT SERVICES 20

ARTICLE 27: SMOKING 20

ARTICLE 28: ALCOHOL AND NARCOTICS ABUSE 21

CHAPTER III: RIGHTS AND OBLIGATIONS FOR THE PREVENTION AND DECLARATION OF WORK ACCIDENTS 23

ARTICLE 29: PREVENTION OF ACCIDENTS AT WORK 24

ARTICLE 30: SERIOUS AND IMMINENT DANGER, RIGHT OF WITHDRAWAL 24

ARTICLE 31: WORK ACCIDENT DECLARATION 24

TITLE 4 - DISCIPLINARY PROCEDURES 25

ARTICLE 32: GENERAL PROVISIONS 25

ARTICLE 33: APPLICABLE SANCTIONS 25

ARTICLE 34: APPLICABLE PROCEDURES 25

TITLE 5 - DEPOSIT - PUBLICITY AND ENTRY INTO FORCE 27

ARTICLE 35: FORMALITIES OF ENTRY INTO FORCE 27

INDEX OF ACRONYMS 28

APPENDICES 29

CHARTER OF THE USE OF COMPUTER RESOURCES AND INTERNET SERVICES AT THE CEA (NIG 608) 29

LIST OF POSITIONS REQUIRING A HIGH DEGREE OF VIGILANCE 36

ANTI-CORRUPTION: CONDUCT CODE 40

GUIDELINES FOR COLLECTING AND REVIEWING MISCONDUCT REPORTS AS SET DOWN IN THE FRAME OF THE “SAPIN”LAW II 55

TITLE 1

PURPOSE AND SCOPE

ARTICLE 1: PURPOSE

In accordance with articles L. 1321-1 and in conformance with the Labour Code, the purpose of these Rules of Procedure is to set down the following directives at the CEA Cadarache Centre, hereinafter referred to as "the Establishment":

• Health and safety rules,

• The conditions in which employees may be called upon to participate, at their employer's request, in restoring work conditions that protect the health and safety of employees, should they appear to be jeopardized;

• General and permanent rules pertaining to the discipline as well as to the nature and extent of the applicable sanctions

The present Rules of Procedure are also intended to state:

• The provisions governing all employees' rights of defence,

• The provisions governing moral and sexual harassment and gender-based-discrimination.

ARTICLE 2: SCOPE OF APPLICATION

2.1 The Geographical Scope of Application

The present provisions of these Rules of Procedure shall apply throughout the CEA Cadarache Establishment, including its facilities located outside its enclosure. These include the CEA Guest House ("le Château"), the Institute of Nuclear Sciences and Techniques (the INSTN), the City of Energies ("La Cité des Energies"), as well as all construction and civil engineering sites.

These Rules of Procedure do not apply to the INBS-PN area, which is under the jurisdiction of the CEA Establishment, DAM/DIF.

2.2. Scope of application concerning people:

2.2.1. The provisions of this regulation apply to all persons entering the Establishment, whether they are linked to the CEA by a work contract or not.

2.2.2. However, the provisions governing the nature and extent of sanctions and disciplinary procedures may apply only to employees who are legally bound to the CEA by a work contract conferring disciplinary power.

ARTICLE 3: COMPLIANCE WITH THE RULES OF PROCEDURE

3.1. Any infringement of the provisions of the present Rules of Procedure may be sanctioned in accordance with legal or conventional procedures.

3.2. Notwithstanding the measures that may be taken by employers by virtue of their disciplinary powers, access to the Establishment may also be prohibited in the event of a serious breach of conduct to the Rules of Procedure, particularly with respect to safety.

TITLE 2 GENERAL DISCIPLINE

3.3. The provisions of the Rules of Procedure are applicable within the general framework of a hierarchical subordination relationship. In addition, FLS security officers have the authority to record and report any breach of the Rules of Procedure in their areas of responsibility.

ARTICLE 4: GENERAL AND PERMANENT RULES

Every person entering the Establishment is under obligation to comply with its internal rules and regulations, as well as with all instructions pertaining to health, safety and discipline that have been set down in accordance with the directives and prescriptions brought clearly to his or her attention.

ARTICLE 5: RULES ENACTED BY SERVICE NOTES

Special provisions pertaining to general and permanent disciplinary and/or health and safety regulations may be issued by the Head of the Establishment.

ARTICLE 6: ACCESS TO THE ESTABLISHMENT

6.1. General Provisions

6.1.1. Access to the Establishment is possible on workdays, from Monday to Friday inclusive from 6:30 AM to 7:30 PM.

6.1.2. Access to the Establishment is subject to the entry and exit control measures issued by the CEA and implemented by the Head of the Establishment.

6.1.3. Any person who is granted access to the Establishment shall receive an access badge that must be worn visibly and on a permanent basis.

6.1.4. Monitoring access and departure from the Establishment:

The access badge must be presented to the FLS security officers when entering the Centre or at any time upon request.

The FLS Security Service is thereby able to identify the holder of the personal access badge. The monitoring consists of an electronic reading of the badge.

Similarly, a possible search of the vehicle may be carried out by FLS security officers in accordance with existing procedures.

The Head of the Establishment may prohibit access of certain vehicles to the Centre for security reasons or for reasons pertaining to public order.

6.1.5. Particular attention and care must be taken to keeping the badge in a safe place. In the event of loss or theft of the access badge, a declaration must be made immediately on the first workday following the discovery of its theft or loss, at the reception building of the Establishment (i.e. “The Main Gate”). In the event of forgetting or losing the access badge, the person concerned may present an identity document at the reception building of the Establishment and a temporary access badge will be issued to them for the day.

6.1.6. The right of access to personal computerized data, in particular data pertaining to checks on the entry and exit of employees, is exercised by contacting the reception team or via the link available on the Intranet site of the Establishment under the heading, “Security Officer”.

6.2. Monitoring entrances and exits in Reinforced Protection Zones (ZPR) and buildings with controlled access:

6.2.1. CEA employees and persons who are required to enter facilities in Reinforced Protection Zones (ZRP) on a routine basis are provided with a secure badge, subject to approval of the facility manager in charge.

6.2.2 The Facility Managers of Reinforced Protection Zones (ZPR) and buildings with controlled access are responsible for authorising access to their zone, to their building or to their building area.

Based on the data obtained from the secure badges allowing access to the Establishment, the facility manager validates the badge for access to the zone and to the authorised building(s) under his responsibility.

6.3. Access procedure outside normal working hours of the Establishment:

Access outside the normal working hours of the Establishment must be authorised by the Head of the Establishment or his delegate in accordance with the current procedures in force.

6.4. Upon termination of the employee’s activities or at the end of his/her contract, the access badge must be returned without delay to the Establishment reception building, (The Main Gate) either by the holder or by the company that submitted the application for the access badge.

ARTICLE 7: WORKING HOURS

7.1. The collective timetable of the CEA/Cadarache Establishment is set as follows: 7:55 AM to 4:35 PM with a noon time break, subject to specific contractual provisions, interventions within the framework of standby duty, shift work or shift work in successive teams.

7.2. The daily working time for CEA employees is the total time spent inside the Establishment, with the exception of the 42 minutes deducted for breaks of which 35 minutes are allotted for lunch.

7.3. Employees may be required to work outside the collective timetable for programme or security reasons, on a temporary or permanent basis. This is the case in particular for employees of continuous and semi-continuous services, in staggered hours, for those who work on security duty stations (PMS) on the site of the Establishment, or who are kept on standby duty at home with interventions. These situations are the responsibility of the supervising managers within the framework of the rules set down by the Head of the Establishment.

TITLE 2 GENERAL DISCIPLINE

7.4. Any employee assigned to work in successive shifts must respect the specified time schedule for the shift to which he/she is assigned. The employees concerned shall be notified in writing and within a reasonable period of notice of the names of each team and the time schedule set for each team.

ARTICLE 8: TARDINESS AND ABSENCES

8.1. The employee's line manager must be informed of any delay in reporting to work by any means available.

8.2. Employees may not be absent from work without the authorisation of their line manager unless they are subject to the rules applicable to trade union representatives or in the exercise of their mandate as representatives of employees and in compliance with the provisions of article L. 4131-1 of the Labour Code governing the right to withdraw in the event of serious and imminent danger.

8.3. Any leave of absence is subject to prior authorisation, following a request made by the CEA employee sent to his line manager within a reasonable period of time. The departure cannot be effective until the request has been validated by the person's line manager.

The line manager shall validate the request within a reasonable period of time. In the event of an unexpected absence, the employee must inform his line manager as soon as possible of his unavailability.

8.4. In the event of absence due to illness, the employee must notify or have his line manager informed as soon as possible and send proof of absence within 48 hours to the Human Resources Department (SRHS).

ARTICLE 9: PROTECTION OF PROPERTY AND MONITORING

9.1. The staff is responsible for the equipment and clothing provided by the CEA. Any disappearance or deterioration must be reported without delay to the line manager.

9.2. Unless prior written authorisation has been obtained from the Direction of the Establishment and in accordance with current procedures, the following behaviour is prohibited:

- the introduction, carrying and possession of weapons or ammunition and explosive materials of any kind, and the use of weapons or ammunition of any kind
- the introduction of controlled biological or chemical agents (drugs, psycho, tropic substances and chemical precursors of category 1)
- the use of radio transmitters which may cause interference with:
  - the Establishment's communication systems,
  - the control-command equipment,
  - the portable equipment for operational dosimetry
- the introduction of animals on the Centre or on any of its official premises.

Removing or displacing materials belonging to the CEA or those belonging to a company working on the premises of the Establishment must be carried out in accordance with the current procedures in force.

9.3. Direction may carry out random searches at any time, particularly in the event of the disappearance of objects or equipment belonging to the CEA. Persons entering the facility may be asked by FLS security guards to allow a complete search of their vehicle and check the items transported.

Such persons have the right to refuse these searches. In such a case, FLS security guards are legally authorised to detain them pending the arrival of the judicial police services who will conduct these searches. During the control or pending the arrival of the judicial police services, a third person employed by the CEA Cadarache Establishment may assist these persons.

In addition to this, video-surveillance systems may be set up at the Establishment after prior notification of the staff and in accordance with the legal provisions in force.

9.4. Every employee must ensure that his or her workstation is secure before leaving, including:
• the safekeeping of nuclear materials, precious metals and other valuables,
• the secure storage of classified documents or documents bearing a level of protection (restricted, confidential, etc.).

9.5. Lost and found items are to be left at the offices of the FLS.

9.6. The use of service vehicles is strictly professional and it is formally forbidden to use service vehicles for private purposes, unless specifically authorised by one's line manager (during an on-call duty, for example).
Any employee borrowing a service vehicle must be in possession of a valid driver's license corresponding to the specific type of vehicle used.
It must also be recalled that drivers must at all times comply with the Regulations of the National French Road and Motorways Code (Code de la Route).

When using service vehicles, employees guilty of traffic violations detected by an automatic control device will be reported and the disclosure obligation provided for in the provisions of Regulations of the National French Road and Motorways Code (Code de la Route) will be applied. In this respect, the Direction of the Establishment will enter the form including the employee's identity via the website www.antai.fr and will send a copy of his or her driver's license. The fine will then be sent to the employee whose responsibility will be to pay, in a personal capacity, the fines for which he or she is personally liable with respect to the administration.

TITLE 2 GENERAL DISCIPLINE

ARTICLE 10: USE OF COMPUTER RESOURCES AND TELEPHONE TECHNOLOGIES

10.1. All users must comply with the Charter for the Use of Information Technology and Internet Services at the CEA, which can be found in the appendices of the present Rules of Procedure.

10.2. Non-professional telephone and/or fax communications are permitted on an occasional basis and within reasonable limits compatible with the operation of the service.

10.3. The CEA may carry out verification concerning the nature and duration of internet connections. The data can be monitored over a 12-month period.

10.4. Furthermore, all users must:
• never disclose their passwords,
• prevent access to their computer session when they leave their workstation.

10.5. The CEA is required to process personal data on its staff and on any person entering the Establishment (see also Article 6.1.6).

An information notice, describing how the CEA collects, uses and manages personal data, the rights of individuals and the way in which the CEA complies with its legal obligations, is accessible by posting at the entrance of the Establishment.

An information notice, entitled «Information on personal», is accessible from the DJC intranet page on protection of personal data.

The CEA has appointed a Data Protection Officer («DPO») who is authorised to deal with all the issues related to data protection of a personal nature. The («DPO») can be contacted at the following address: dpd@cea.fr.

ARTICLE 11: FILMING RECORDINGS

11.1. Land or air photographs of the Establishment are subject to a request for authorisation to take pictures in accordance with the procedures in force. Photographic or cinematographic photographs of the site, laboratories or installations, site materials and sound recordings must be authorised in accordance with the company's procedures.

11.2. An employee photographed or filmed for publication outside the CEA or on the intranet must submit his/her written permission.

In the case of an internal publication at the CEA, no prior authorisation from the person concerned is required; his or her consent is presumed to have been obtained if he or she made no objections at the time such photographs were taken.

11.3 It is strictly forbidden to use for personal purposes any photographic device or camera equipment and any recording or reproducing apparatus of sounds and images within the premises of the Establishment.

TITLE 2 GENERAL DISCIPLINE

ARTICLE 12: PROTECTION OF THE SITE AND THE ENVIRONMENT

12.1. The deposit of materials, products, supplies or materials is prohibited outside of shops, sheds or areas designed for this purpose.

12.2. The disposal of materials, waste and effluents is regulated by specific instructions issued by the Direction of the Establishment.

12.3. Hunting and any gathering or harvesting of plants is prohibited unless authorised by the Direction of the Establishment.

12.4. Feeding or distributing food to the wildlife on the Centre is strictly prohibited.

ARTICLE 13: GENERAL WORK CONDITIONS AND LIFE INSIDE THE ESTABLISHMENT

13.1. In all circumstances, decent dress and correct behaviour are required.

13.2. It is forbidden to carry out personal work on the premises of the Establishment.

13.3. The distribution of leaflets and posters is to be carried out in accordance with the proper legal and conventional regulations. Any out-of-panel display may be removed by the Direction.

13.4. It is also forbidden:
• to carry out collections for legal entities without the express authorisation of the Direction. This provision does not apply to the collection of union dues;
• to hold, even after working hours, assemblies or meetings not authorised by the Direction, with the exception of the trade union meetings as provided for in article 9.2 of the CEA Labour Convention.

13.5. Trade union sections or trade union establishments may assemble their members within the premises of the Establishment as defined in the Convention provisions of the CEA.

TITLE 2 GENERAL DISCIPLINE

ARTICLE 14: RELATIONS WITH THIRD PARTIES

14.1. CEA employees have a duty to respect the principles of loyalty, integrity and neutrality in their professional relations with third parties (suppliers, service providers, customers, partners and contacts) in the course of their professional activities.

14.2. It is expressly forbidden for CEA employees to solicit or accept from a third party, at any time, directly or indirectly, any offers, promises, donations, gifts or benefits of any kind. This includes performing or refraining from performing any act related to their activity or function, or facilitated by their activity or function in violation of their legal, contractual or professional obligations, with or without any direct or indirect consideration.

14.3 All CEA employees are legally bound to observe a type of behaviour that respects the provisions of the Anti-Corruption Code of Conduct annexed to these Rules of Procedure, especially in the form of gifts or benefits. The procedure described in annex to these Rules of Procedure (Collection and processing procedure alerts under the so-called Sapin II Law) is a possibility offered to employees, which does not exclude other reporting channels (hierarchy, CEA mediator, employee representatives).

ARTICLE 15: PROVISIONS PERTAINING TO SEXUAL AND MORAL HARASSMENT, TO SEXIST ACTS AND THE PRINCIPLE OF NON-DISCRIMINATION

15.1. In accordance with article L. 1152-1 of the Labour Code:

“No employee shall be subjected to repeated acts of moral harassment that have as their object or effect a deterioration of their working conditions that is likely to degrade their rights and dignity, to impair their physical or mental health or to compromise their professional future”.

“No employee, trainee, apprentice or any other person shall be punished, dismissed or subjected to any direct or indirect discriminatory measure, particularly with regard to remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or contract renewal for having suffered or refused to suffer repeated acts of moral harassment or for having witnessed such acts or having related them”.

Any employee who has engaged in acts of moral harassment shall be subject to disciplinary action (article L. 1152-5).

15.2. In accordance with article L.1153-1 of the Labour Code:

“No employee shall be subject to:
• sexual harassment, consisting of repeated sexual remarks or behaviour that infringes on one’s dignity due to their degrading or humiliating nature or resulting in the creation of an intimidating, hostile or offensive situation against him/her;

• actions equated with sexual harassment, consisting of any form of serious, even unrepeated, pressure exerted for the real or apparent purpose of obtaining an act of a sexual nature, whether it is sought for the benefit of the perpetrator or for the benefit of a third party".

"No employee, no trainee, no apprentice, no candidate for recruitment, training or an internship in a company or any other person shall be penalized, dismissed or discriminated against, directly or indirectly, in terms of remuneration, training, reclassification, assignment, qualification, classification, promotion, transfer or contract renewal for having suffered or refused to suffer sexual harassment as defined in Article L. 1153-1, including, the case mentioned in 1 of the same article, remarks or conduct that have not been repeated" (article L. 1153-2 of the Labour Code).

"No employee, no person in training or working in the frame of an internship may be punished, dismissed or discriminated against for having reported or testified about sexual harassment" (Article L.1153-3 of the Work Code). Any employee who has engaged in acts of sexual harassment (Article L. 1153-6 of the Labour Code) is liable to disciplinary action"

15.3. In accordance with article L.1142-2-1 of the Labour Code:

"No employee shall be subjected to acts of a sexist nature, defined as any act pertaining to the gender of a person, having the object or effect of undermining his or her dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment»

15.4 In accordance with article L.1132-1 of the Labour Code:

"No person may be excluded from a recruitment or access to an internship or a period of training in a company, no employee may be sanctioned, dismissed or discriminated against, directly or indirectly, as defined in Article 1 of Law N° 2008-496 of May 27th 2008. This law sets down various provisions for adapting to Community law for the purpose of combating discrimination, particularly in the field of the meaning contained in Article L.3221-3 referring to profit-sharing measures or distribution of shares, training, reclassification, assignment, qualification, classification, professional promotion, transfer or contract on the grounds of a person's origin, gender, morals, sexual orientation, gender identity, age, marital status or family status, pregnancy, genetic characteristics, the particular vulnerability resulting from one's economic situation, apparent or known to the person concerned, the person's belonging or not belonging, true or supposed, to an ethnic group, a group or a group of people, a nation or an alleged race, one's political opinions, trade union activities or mutualists, religious beliefs, physical appearance, family name, place of residence or bank address, or because of his or her state of health, loss of autonomy or disability, his or her ability to express themselves in a language other than French."

TITLE 2 GENERAL DISCIPLINE

ARTICLE 16: OTHER REQUIREMENTS

16.1. All the professional mail of CEA / Cadarache is handled by its mail service. The stamp of “personal” or “trade union” mail shall protect individual business mail. The sending or forwarding of an employee’s personal mail is prohibited including any direct legal address registration at the CEA / Cadarache of written advertisements or telephone announcements.

16.2 The organisation of sales or of any other type of commercial operation in the Establishment is prohibited, except with special authorisation and prior consent granted by the Head of the Establishment.

TITLE 3 HEALTH AND SAFETY

CHAPTER I: GENERAL PROVISIONS

ARTICLE 17: PRINCIPLE

17.1. Prevention of the risks of occupational accidents and diseases concerns everyone. It requires each person accessing the Establishment to comply strictly with applicable health and safety requirements.

The Head of the Establishment reserves the right to prohibit access to the Establishment to any person whose behaviour or presence would be likely to undermine safety.

Furthermore, any person exhibiting behaviour or health conditions that could constitute a state of danger to himself, others or to the facility shall be taken to the premises of the Occupational Health Service facility by means of the FLS security guards in accordance with the procedures in force. The employee's line manager must be informed of the assumption of responsibility for the person concerned.

17.2. Prevention of risks of occupational accidents and diseases is the subject to:
• Statutory requirements relating to safety at the workplace (Labour Code and Work Convention, in particular the Single Document and the Prevention Plans),
• The following provisions of the Rules of Procedure,
• General Rules for Radiation Protection,
• Instructions relating to certain activities, a building, a room, a facility, a material which is the subject of either a notice or a notification to the persons concerned or made available to them at the workplace.
• Safety instructions for the execution of the work.

17.3. Only equipment that meets regulatory requirements is authorised in the facility.

17.4. All equipment used, particularly on construction sites, must comply with the safety standards in force and be up to date with regard to the periodic inspection schedules. Workplaces, especially work sites, must be left clean and in good order at the end of the day.

At the end of the work, the premises must be restored in good condition, taking care not to leave any material or debris.

17.5 Pursuant to Article L. 4122-1 of the Labour Code:

In accordance with the instructions given to him by the employer in the conditions provided for in Article 4 of the Rules of Procedure, it is the responsibility of each worker, according to his training and to the best of his possibilities, to take care of his health and his safety and that of the other persons affected by his actions or his omissions at work.

TITLE 3 HEALTH AND SAFETY

CHAPTER I: GENERAL PROVISIONS

The employer's instructions must specify, particularly when the nature of the risks justify it, the conditions of use of work equipment, the means of protection, of dangerous substances and preparations. They are adapted to the nature of the tasks to be performed.

The provisions of the first paragraph shall not affect the principle of the employer's responsibility.

ARTICLE 18: SANCTIONS

Failure to comply with health and safety requirements and instructions may result in disciplinary sanctions for CEA employees in accordance with Chapter 9 of the Labour Convention or may result in contractual measures for outside companies in accordance with Article 17 of the General Conditions of Purchase of the CEA and/or the withdrawal of the access badge.

ARTICLE 19: EMERGENCY PROVISIONS

19.1 Conduct in the event of an accident or an incident:

Anyone witnessing an accident or incident must immediately alert:
• The Central Security Station (PCS) by telephone at N°18 (land line) or 04 42 25 22 18 (mobile) or by call button. The witness must provide as much information as possible about the location, nature and magnitude of the accident.
• The Local First Aid Team (ELPS), if one exists in the facility, or the safety manager concerned.

Only the trained FLS personnel is authorised, with the help of its specialized vehicles, to transport injured (even slightly injured), sick or contaminated employees.

19.2. In the event of a general alert of the Establishment announced by the sirens outside or by loudspeakers inside the facilities:
• All people present in the buildings must remain there,
• People moving about the Establishment in a vehicle or on foot must immediately go to the building nearest them,
• All people must comply with the instructions broadcast in the buildings by the Centre's General Broadcasting Network,
• The use of vehicles is prohibited unless specific instructions are given otherwise and the use of telephones must be limited to safety reasons.

19.3. Some facilities are subject to specific safety rules (e.g. fire, radiation protection, handling, electrical or chemical hazards), leading to specific actions posted in the facility. In the event of an alarm in a facility, the people present in the building must comply with the safety conduct rules and follow the instructions given by the Facility Manager.

CHAPTER II: GENERAL RISK PREVENTION MEASURES

ARTICLE 20: INFORMATION AND STAFF TRAINING IN DEALING WITH RISKS

20.1. Information: Nominative Professional Data Sheet (FPN)

The FPN is the communication support between the actors of facility safety and the Occupational Health Service (SST). This document codifies the conventional and radiological risks for every employee in order to define his or her medical surveillance. It is based on the Professional Risk Assessment (EvRP) which constitutes the Single Document of the Institution and which is available on its intranet site.

The facility manager and the employee sign the FPN.

20.2. Training:

In accordance with the Labour Code, every employee must complete a general training course on quality, safety and the environment, supplemented if necessary by training at the workplace.

ARTICLE 21: MEDICAL MONITORING

21.1. All employees must report for medical check-ups and additional examinations as required by the legislation and the CEA regulations.

21.2. The notice of physical aptitude for employment shall be renewed in accordance with the provisions of the Labour Code. It may be suspended or restricted at any time by decision of the occupational physician.

Every employee must comply with the notices of physical aptitude or inaptitude for the work place issued by the occupational physician, with respect to the personal professional record relating to the employee's activities and work conditions.

21.3. The personal professional record is used, in particular, to determine the nature and frequency of medical examinations that the employee must undergo, depending on the radiological classification specified at his/her workplace (category A, B or Not exposed).

21.4. Regular medical check-ups are mandatory for the following situations:
• resuming work after an occupational illness,
• resuming work after maternity leave.
• resuming work after an absence of at least 30 days due to a work-related accident, illness or non-occupational accident.
Medical check-ups are also planned in the following cases:
• resuming work after an absence of more than 3 weeks.
• a request for early return to work before the date initially designated by the employee's attending physician.

TITLE 3 HEALTH AND SAFETY

CHAPTER II: GENERAL RISK PREVENTION MEASURES

A pre-recovery visit can be organised at the employee's request by his/her doctor or by the Medical Advisory Board.

21.5. In addition to the regular medical check-ups, all CEA employees may obtain an appointment with an occupational physician on an issue relating to his or her health or workplace.

21.6 In the event of a behavioural disorder of a person, the line manager or the facility manager may request a consultation with the occupational physician or have the matter referred to the FLS as an emergency with the order to contact the SST (i.e. The CEA / Cadarache Medical Services). The line manager or the facility manager must then fill in a form describing the behavioural disorder and forward it to the FLS.

ARTICLE 22: RISK PREVENTION INSTRUCTIONS

The prevention of accidents at work and occupational diseases demands strict observance by the staff of the instructions dealing with the legal and regulatory dictates concerning this prevention and employee safety.

ARTICLE 23: SAFETY DRILLS

The procedure to be followed in the event of an accident or incident is defined by the procedures validated by the Head of the Establishment or his representative. It must be learned by everyone, in particular by means of security drills organised by the facility manager or the Head of the Establishment on a regular basis.

ARTICLE 24: MARKINGS AND SIGNS

Any person moving about in the Establishment must respect the markings in place in the facilities, the health and safety signs as well as those posted on the evacuation routes and at emergency exits.

ARTICLE 25: MOVEMENT AND CIRCULATION WITHIN THE ESTABLISHMENT

25.1. Pedestrian movements

Pedestrian traffic is prohibited outside the lanes provided for this purpose, especially in the forest or in proximity of the fences that constitute the Centre's enclosure.

25.2. Traffic Regulations

25.2.1. Driving within the premises of the Establishment is limited to professional and routine movements. It is forbidden outside the usual routes of the road network and the boundaries of facilities, especially in the forest or near the fences.

CHAPTER II: GENERAL RISK PREVENTION MEASURES

25.2.2. FLS vehicles (ambulances, automobiles and other intervention vehicles) have priority when using their lights, sound and other regulatory devices. For other vehicles, the use of an audible alarm warning is prohibited, except in case of immediate danger.

25.2.3. During arrival and departure periods of the personnel, buses are given priority when leaving the car park. In addition, it is strictly forbidden for any vehicle to use the bus lanes.

25.2.4. Any traffic accident occurring on the Establishment's road network must be reported immediately to the FLS security services. However, the reports drawn up by its security officers only have internal value within the CEA and are not enforceable against third parties.

25.2.5. The General Provisions of the French National Road and Motorway Code for traffic and parking are applicable in the Establishment. Unless otherwise indicated by signs, the authorised speed limit of vehicles throughout the entire site is:
• 70 km / h for light and two-wheel vehicles.
• 50 km / h for buses, heavy vehicles and machines.

The use of mobile phones while driving is formally forbidden.

The Head of the Establishment may carry out road side checks by FLS security officers. They may include compliance with speed limits, the use of mobile phones while driving and failure to wear seat belts.

25.2.6 Offenders may be subject to administrative measures depending on the seriousness of the offence:
• A statement of infringement sent to the person concerned and to his hierarchy,
• Withdrawal of the secured access badge and substitution by a daily access pass for a fixed period, as well as the withdrawal of the authorisation to drive vehicles inside the Establishment.

Any unsafe behaviour identified by FLS security officers will be subject to the same measures.

25.3. Parking rules:

25.3.1. Vehicles may only be parked in designated car parks. It is specifically forbidden to park:

CHAPTER II: GENERAL RISK PREVENTION MEASURES

• in front of fire hydrants, fire doors, gates and emergency exits, as well as on the pavement and along marked red and white edges,
• on a pedestrian crossing and on the marked sites reserved for persons with reduced mobility or safety devices.

25.3.2. Parking on the car parks at the Main Entrance Gate of the Establishment is strictly limited to the time necessary to complete access formalities.

25.3.3. If an employee is required to leave his/her vehicle on the premises, (for only professional reasons i.e. missions...) and must recover it after closing hours on the Centre, parking is authorised in the specific areas designated for this purpose, i.e. after the Main Entrance Gate (PEP) on the central parking area, between the entry and exit routes. The FLS Brigade Chief on duty must be informed by the owner of the vehicle beforehand.

25.3.4. Violations of the parking rules may be subject to administrative restrictions on vehicle access, taken by the Head of the Establishment and implemented by the FLS security services.

25.3.5. These measures shall not preclude the application of the disciplinary procedures in force.

ARTICLE 26: RESTAURANT SERVICES

26.1. It is forbidden to have meals in the Establishment outside the premises provided for this purpose, unless authorised by a hierarchical manager.

26.2 Access to collective dining rooms shall be permitted within the time limits set by the Head of the Establishment.

26.3. Access to the restaurants of the Establishment in working or protective clothing is prohibited, except for personnel in uniform.

26.4. Employees bringing their own meals to the collective dining areas must remain the exception and they must comply with food hygiene standards.

ARTICLE 27: SMOKING

27.1. Pursuant to the Public Health Code, smoking is prohibited in all enclosed and covered areas of the Centre, including the collective transport means chartered by the CEA and in all CEA service vehicles.

27.2. Use of the electronic cigarette also applies to the above provisions. It is formally prohibited in all enclosed and covered areas of the Centre.

CHAPTER II: GENERAL RISK PREVENTION MEASURES

27.3. It is strictly forbidden to smoke in the forest as well as in the outdoor areas which are subject to a risk of fire or explosion.

ARTICLE 28: ALCOHOL AND NARCOTICS ABUSE

28.1. General measures

It is forbidden for any person to:

• enter or remain in the Establishment while under the influence of alcohol or drugs or any of the substances or plants classified as narcotic drugs;
• allow entry into the facility, without notifying the facility manager concerned or the line manager, of persons who are obviously intoxicated or under the influence of any substances or plants classified as narcotic drugs;
• carry in or consume alcoholic beverages on the premises of the Establishment with the exception of those listed in article R.4228-20 of the French Labour Code (wine, beer, cider and perry). Such beverages may be consumed with meals at the Establishment restaurant or during celebrations («pots») or festive events authorised in advance by the facility manager or a line manager having at least the rank of Service Head. Furthermore, these alcoholic beverages must be consumed in moderation in order to avoid jeopardizing workplace safety and road safety on the site;
• bring in or hold, distribute or consume, except for the conduct of research programs, narcotic substances within the Establishment.
It must be recalled that the consumption and possession of narcotic drugs constitute offences punishable by criminal sanctions under Articles L. 3421-1 of the French Public Health Code and 222-37 of the Criminal Code.

Any person exhibiting behaviour or a state of health that might constitute a source of danger to himself/herself or to others or to the facility may be subject to suspension of his/her activities by the hierarchy or, if necessary, by the FLS. Such persons will be taken to the Occupational Health Service (SST) by the following means of the FLS in accordance with current procedures.

In this situation, a detailed report will be drawn up, making it possible to objectify the difficulties encountered (see Article 21.6). The occupational physician shall organise, as soon as possible, the care of the person once accompanied on his premises and must inform the Direction of the said person's departure from the Establishment.

TITLE 3 HEALTH AND SAFETY

CHAPTER II: GENERAL RISK PREVENTION MEASURES

28.2. Special measures applicable to highly vigilant posts:

Activities involving a high degree of permanent vigilance and for which disorderly behaviour, (particularly alcohol or drug consumption), might prove likely to expose other people and property to danger, are listed in the Appendix (NHPD Note DIR 2016-243).

The employees concerned are informed in writing that they are assigned to positions involving such activities and associated preventive measures.

In addition to the prohibitions in section 28.1, in order to ensure their own safety and that of their colleagues, as well as to avoid any damage to property, consumption of alcohol and narcotic substances is prohibited for workers employed in positions with a high degree of vigilance.

28.3. Breath alcohol screening by a “Breathalyser” and drug screening by a saliva test:

The implementation of an effective prevention policy justifies that workers in highly vigilant positions are not, during the performance of their duties, intoxicated or under the influence of narcotics.

For workers in highly vigilant positions, the Direction of the Establishment may decide to carry out screening for consumption of alcohol or narcotics, using random checks.

Breath alcohol screening by Breathalyzer or drug screening by a salivary test may be carried out by an FLS manager, or by a manager in the employee’s hierarchy, having at least the rank of Service Head.

The person responsible for screening must have received appropriate information on the conditions and manner of administering the Breathalyser or saliva test and interpretation of the results. As such, he must scrupulously comply with the instructions for use written by the supplier, ensure that the screening test is in perfect condition (validity and conservation) and avoid any circumstance likely to distort the results.

CHAPTER II: GENERAL RISK PREVENTION MEASURES

Before being screened by a Breathalyser or saliva test, the person concerned must first be informed that it can only be carried out with his consent. The person responsible for the Breathalyser test or the screening of narcotic drugs by a saliva test should however specify that in case of refusal, the person subjected to a Breathalyser test or saliva test is subject to disciplinary action that may even include dismissal.

The worker concerned may request the presence of a third party during the screening.The person responsible for screening is legally bound by professional secrecy regarding the results.

In the event of a positive result, the employee has the right to request a second medical expertise which is to be conducted under the responsibility of the CEA and which must be carried out as soon as possible.

TITLE 3 HEALTH AND SAFETY

CHAPTER III: RIGHTS AND OBLIGATIONS FOR THE PREVENTION AND DECLARATION OF WORK ACCIDENTS

ARTICLE 29: PREVENTION OF ACCIDENTS AT WORK

Employees are required to comply with the instructions for the prevention of accidents at work and occupational diseases. The instructions relating to specific hazards are pointed out and explained to the personnel in advance by the facility manager or his delegate.

Any intervention by an outside company in a facility requires prior written authorisation by the facility manager

ARTICLE 30: SERIOUS AND IMMINENT DANGER, THE RIGHT OF WITHDRAWAL

30.1 Any worker who has reasonable grounds to believe that a situation presents a serious and imminent danger to life or health, or who notices any malfunction in the protection systems, must alert his facility manager or his delegate immediately and may withdraw from such a situation.

30.2 A worker who has exercised his right to withdraw from a situation where this danger or this malfunction persists cannot be asked to resume his/her post.

30.3. If a representative of the CEA Cadarache staff notices that there is a serious and imminent case of danger, directly or through the intermediary of a worker, he/she must immediately notify the Head of the Establishment or the facility safety engineer (FSE); he or she must also record this incident in writing on the special register held at the ISE. The Head of the Establishment or his representative is required to conduct an immediate investigation with the CHSCT or CSE staff representative who reported the hazard to him/her and take the necessary steps to remedy this situation.

ARTICLE 31: WORK ACCIDENT DECLARATION

31.1 Any employee who suffers an accident at work or on his/her way to work must notify his employer within 24 hours, regardless of the severity of the accident.

31.2. Any employee who suffers a work accident must go to the Occupational Health Service (OHS) or have it reported by a third party for registration on the ledger of accidents at work as soon as possible.

TITLE 4 DISCPLINARY PROCEDURE

ARTICLE 32: GENERAL PROVISIONS

Pursuant to Article 76(1) of the Labour Agreement and Article 2.2.2 of these Rules of Procedure: Any employee whose behaviour is considered to be at fault, especially as a result of a violation of the labour and disciplinary rules in force at the Establishment, may, depending on the gravity of the violation and/or its repetition, be subject to one or another of the classified disciplinary sanctions mentioned hereafter.

Disciplinary proceedings must be launched within 2 months of the date at which the Head of the Establishment or his representative became aware of the violation involving an accusation of the employee.

ARTICLE 33: APPLICABLE SANCTIONS

33.1. The sanctions to be imposed on employees are those defined in Article 76 paragraph 2 of the Labour Agreement.
(a) warning issued;
(b) reprimand reported with entry in the file;
(c) disciplinary layoff for a maximum period of one month;
(d) termination for disciplinary reasons.

33.2. Any employee for whom a sanction provided for in Article 76 paragraph 2 of the Labour Agreement is envisaged must be granted a hearing, prior to any final decision, by the Head of Establishment or his representative. During this discussion, the employee may be assisted by a fellow employee or a representative of a trade union organisation who shall be allowed to attend the hearing providing this person is a member of the CEA personnel.

In accordance with Article 77 of the Labour Convention, only the enforcement sanctions on disciplinary grounds and dismissal may give rise to the application of the disciplinary procedure measures set down in Article 85 of the Labour Agreement.

33.3. The reference to the notified warning or reprimand will be removed from the file if the employee has not been the subject of a new sanction for a period of three years from the date of notification of the warning or reprimand.
No penalties, more than three years prior to the commencement of the disciplinary proceedings or subject to an amnesty measure, may be invoked in support of a new sanction.

ARTICLE 34: APPLICABLE PROCEDURES

34.1. Probationary suspension as a precautionary measure (Article 78 of the Labour Agreement):

In the context of disciplinary proceedings and without prejudice to any possible sanction as defined in Article 35, the employee may be suspended as a precautionary measure until the CEA has reached its final decision.

TITLE 4 DISCPLINARY PROCEDURE

The decision ordering the probationary suspension of an employee must specify whether or not the person concerned shall retain, during the period of suspension of the contract, his/her salary (basic salary, individual bonus or seniority bonus, special executive bonus or special non-executive bonus to the exclusion of any other element). Or a decision will be made determining what portion of the salary shall be subject to a reduction. This reduction may be equal to a quarter or at most, half of the employee's salary. In all cases, the employee shall continue to be entitled to all conventional family benefits.

The employee is entitled to a refund of the deductions made, unless the transfer to probationary suspension is deducted from the period of cautionary probationary suspension or in the event of termination of his/her contract on the grounds of serious or gross misconduct.

34.2. Procedure (Articles 85 and 86 of the Labour Agreement):
The CEA applies the legal provisions concerning disciplinary proceedings (in particular those relating to the preliminary interview and sanction provided for in Article L.1332-1 to -3 of the Labour Code).
The proposals for disciplinary sanctions provided for in Article 77-2 of the Working Agreements are forwarded to the President of the Conventional Council.

Sanctions are imposed by the Director of Human Resources and Social Relations, after a ruling by the Conventional Council. The interested parties must be notified of these sanctions within 30 days of the ruling issued by the Conventional Council.

TITLE 5

DEPOSIT – PUBLICITY AND ENTRY INTO FORCE

ARTICLE 35: FORMALITIES OF ENTRY INTO FORCE

In accordance with the provisions of the Labour Code, the present Rules of Procedure were:

- submitted for approval to the Work Council (COMET) on December 18th 2018 including the provisions under its jurisdiction at the CHSCT on December 7th 2018;
- communicated in duplicate to the Labour Inspector to whom the Establishment reports, accompanied by the approval of the Staff Representatives;
- filed with the Office of the Labour Court, which is responsible for the Establishment.

They shall enter into force on May 1st 2019 and shall be applicable from that same date.

In order ensure that all persons having access to the Institution may have full knowledge of the present Rules of Procedure, they are currently available at the Welcome Office (main gate), on the CEA intranet website, at the SRHS (The Personnel Department) and on file in all secretarial offices of the scientific and administrative services in Cadarache.

INDEX OF ACRONYMS

CEA: The French Commission of Atomic and Alternative Energies

CHSCT: The Health, Safety and Working Conditions Committee

CSE: The Social and Economic Committee

COMET: The Work Council

FLS: The Local Safety and Security Enforcement Corps

FPN: Nominative Professional Record

ISE: Institutional Safety Engineer

SRHS: Human Resources and Social Relations Department

OHS: Occupational Health Service

ZPR: Reinforced Protection Zone

APPENDICES:

- Charter for the use of it resources and internet services at the CEA
- List of high vigilance positions
- Anti-corruption code of conduct
- System for the collection and processing of reports within the framework of the Sapin low 2

APPENDICES

CHARTER FOR THE USE OF IT RESOURCES AND INTERNET SERVICES AT THE CEA (NIG 608)

The purpose of this charter is to specify all the rules pertaining to the use of IT resources and Internet services at the CEA and to define the associated responsibilities.

I DEFINITIONS

1.1 Computer equipment, software and applications are referred to as «computer means», databases, networks and digital files that are part of the systems of information from the CEA (stationary as well as mobile means, whether local or accessible, remote, under the responsibility of CEA services). These means are intended to process, store, exchange or destroy information. This information may concern all the CEA's fields of activity: scientific, technical, administrative, managerial, secretarial, etc.

1.2 Internet services refers to the various means of exchange and information (web, messaging, forums, telephony, video-conferencing, etc.) made available by local or remote servers.

1.3 «User» is defined as any person having access to or using the IT means and Internet services set up by the CEA, whatever his or her status: CEA employee, temporary staff, short or long-term trainee, PhD student and, under the conditions defined by agreement, a collaboration agreement or market, researcher in an associated laboratory, company personnel or a third party partner organization and subsidiary employee.

1.4. "Head of unit" refers to line managers with a rank greater than or equivalent to that of a department head. However, it is possible for a department head to delegate his or her powers and responsibilities under this charter, to a laboratory manager.

II GENERAL RESPONSIBILITIES

2.1. The Central Security Director, as a Qualified Authority1, is responsible for the security of all CEA information systems. As such, he/she defines the policy of these systems and the associated objectives, establishes the safety rules and ensures its control.

[1] In the context of the interdepartmental instruction n°1300/SGDSN/PSE/PSD of 23 July 2010 relating to the protection of secrecy of National Defence (published by decree on the same day - JORF of August 11th 2010).

APPENDICES

2.2.The heads of the services, assisted by the Systems Security Agents, (ASSI), Security Officers (SOs) and Correspondents of Security (CS), must:

• ensure compliance with the measures defined by the Qualified Authority;
• define the security objectives of their service information systems and implement appropriate measures.

III CONDITIONS OF ACCESS TO COMPUTER RESOURCES AND TO WEB SERVICES

3.1. The CEA may implement restrictions of access to certain internet services judged not to comply with the rules of use defined in this charter or presenting a risk to the security of the CEA.

3.2. The provision of IT resources and internet services to a user is under the responsibility of the head of the user's service of these resources, in accordance with the applicable safety rules.

3.3. Access to CEA IT resources and internet services are subject to the prior authorisation by the Head of Unit and therefore the Qualified Authority must in accordance with the rules defined by this Charter issue them. These access authorizations are strictly personal and under no circumstances whatsoever may be transferred, even temporarily to a third party2. They may be revoked at any time. All authorisations shall expire upon termination of the professional activity that justified them.

[2] In case of professional necessity, the user may be required to communicate his/her access codes to the ASSI and/or the Department Head.

3.4. Depending on the activity of the service or users, the Head of the Service may in addition, provide for special security measures and restricted access to IT resources and internet services.

3.5. The use and connection of computer equipment to CEA networks (computer, smartphone, USB keys, («flash drives or memory sticks» etc.) not belonging to the CEA are subject to prior authorisation of the head of the service concerned and to the safety rules prescribed for the network used.

3.6. The user must return all the computer resources that have been entrusted to him/her upon the cessation of the activity that justified the allocation of these resources, in accordance with the provisions in force at the headquarters of his/her designated centre.

APPENDICES

IV CONDITIONS FOR THE USE OF COMPUTER RESOURCES AND WEB SERVICES

4.1. General terms and conditions of use

4.1.1. Every user is responsible for the use of the computer resources and of the internet services to which he/she has access.

4.1.2. The use of these means and services must be rational, in order to avoid the risk of saturation and in accordance with the rules defined in this charter.

4.1.3. These means and services are for professional use in connection with the CEA's fields of activity, which specifically excludes any use for purposes that are private, remunerative or recreational. However, personal use is tolerated if confined to a limited and reasonable use and to the extent that no professional activity is affected in any way and this use is not likely to affect the security of information systems or damage the interests or image of the CEA. The management of this personal information is the sole responsibility of the user.
The information processed by CEA IT resources is presumed to be of a professional nature.

4.1.4. Users of these means and services must not consult or exchange information that may be subject to criminal prosecution (i.e. content that is offensive, racist or contrary to public order) or that may harm the interests or image of the CEA (i.e. particular sites or messages of pornographic content or online gambling sites).

4.1.5. These means and services must not be used to exchange, within the organisation or with the outside world, information of a political, social or religious nature. The terms and conditions for the use of these means and services in the context of the exercise of the right to organise are defined by collective agreement.

4.1.6. The user must not reproduce, download, copy, distribute, modify and/or use software, databases, web pages, images, photographs or other creations protected by copyright or private right, without having first verified that such material has been expressly authorised by the copyright owner. It is forbidden to copy or make use of other creations protected by copyright or private right, without having verified in advance that it has been expressly authorised by the holder of the rights attached to them.

4.1.7. The user or service that, in the course of his/her activities, is required to create files subject to the provisions of the French Data Protection Act3, must complete the required formalities with the National Commission for Data Processing and Liberties (CNIL) through the Central Service of the Intellectual Property and Agreements Directorate (SCPIA) of the Legal Affairs Department. Also included is the litigation (DJC) and in consultation with the Head of Unit to which he or she reports.

[3] Law No. 78-17 of January 6th 1978 relating to information technology, the files and freedoms, modified.

APPENDICES

He or she must also ensure that the data processing complies with the legal provisions.Furthermore, the CNIL must also be informed by declaration in the event of the deletion of these files.

4.1.8. The employee whose workstation undergoes remote maintenance while he or she is using it, is always informed in advance.

4.1.9. The professional use of private computer equipment for professional purposes must be strictly limited to mobile services accessible from the internet and explicitly designed for this purpose (collaborative space, general public sites and standard mobile services).

4.2 Special conditions for the professional use of electronic mail.

The use of professional e-mail must meet the following requirements:
all messages are considered professional;
the sending of electronic messages for personal use must be limited and is carried out under the full and entire responsibility of the user. It must not affect normal business message traffic;
the transmission of information of a sensitive nature, on an unauthorized network should only be performed using encryption, in compliance with the current safety regulations;
the user must use the utmost vigilance when opening messages and attachments of which he/she does not know the source;
he or she must ensure that the distribution of messages is limited solely to the recipients concerned in order to avoid mass messaging, unnecessary congestion of the messaging system and a degradation of the service.

4.3. Special conditions for the use of internet services

The user must respect the rules defined by the owners of the websites that he or she visits as well as the legislation in force. As such, he or she must not:
• connect or attempt to connect to a server other than through the provisions of this server and without formal authorisation of the line managers in charge;
• engage in actions that knowingly jeopardize the safety or the proper operation of the servers he or she is accessing;
• intercept communications between third parties;
• use internet services not validated by the Qualified Authority for the storage, processing or dissemination of CEA information;
• offer or make available to third parties sensitive data and information and that is contrary to the legislation in force;
• express personal opinions, in particular those unrelated to the employee's professional activity and that are likely to harm the CEA.

As a rule, only websites with a direct and necessary link to professional activity should be consulted. Occasional and reasonable consultation of the websites for personal reasons is tolerated, provided that the content is not contrary to public policy, does not compromise the security of the CEA information systems and does not jeopardize the interest and image of the CEA.

V SECURITY RULES FOR THE USE OF COMPUTER MEANS AND INTERNET SERVICES

5.1 The user shall contribute to the general safety of the CEA, in particular by observing the safety rules set down in this Charter or adopted by the Qualified Authority and the measures prescribed by the Head of Unit.

5.2 The user shall ensure, at his or her level, the hardware and / or software protection of the computer resources entrusted to him/her. In this capacity, he or she must ensure that:

• The protection of his/her various means of authentication is absolute. In particular, a password must be chosen in accordance with the regulations that aim at obtaining maximum safety and reliability;
• No access to computer facilities or internet services shall be granted to unauthorized users, through materials used by him/her;
• No use or attempt to use accounts other than his or her own may be made nor may his/her identity be concealed;
• The level of sensitivity of the information he/she processes is in compliance with the safety rules and recommendations referred to above;
• There is no access to information and documents kept on computer means other than those of his/her own, and those which are public or shared. Furthermore, he/she must not attempt to read, modify, copy or destroy them, even if access is technically possible.
• In the case of activity requiring resource sharing, the rights of access shall be limited only to the persons concerned and to the strict minimum necessary;
• The Head of Unit and the ASSI are informed as soon as possible of any attempt to violate his/her account and, in general, any anomaly which he/she may have observed;
• Sensitive information is protected by making sure that access is restricted to those persons authorised for the needs of his/her unit.
• He or she shall refrain from deliberately acquiring any knowledge of information held by third parties, in particular by intercepting a password or usurping another person's identity, including information exchanged by professional e-mail or by means of internet services;
• He or she shall never disclose to third parties nor to the public, in particular via internet services, any information subject to an authorisation for the dissemination or publication concluded under the terms of an agreement with the CEA or subject to the rules applicable in the CEA.

APPENDICES

5.3 The user is legally bound to preserve the integrity of the CEA computer resources, including means of access to internet services. To this end, he or she shall in particular:

• never impede the proper functioning of CEA computer resources, particularly by introducing non-professional documents, data, programmes and software, especially software designed for entertainment, parasitic software or by bypassing security devices and internet services, particularly by the use of the professional e-mail;
• refrain from any improper use or actions that degrade the computer means, their original configurations or their physical and software properties.

5.4 Information falling within the classification of Defence must be processed on computerized means subject to a decision of special registered approval. In particular, they should not be processed on the CEA Intranet or on internet services. There are special provisions for access to these approved, high security information systems.

5.5 The continuous evolution of information technologies currently provides users with new services that can be accessed from the CEA network. These new technologies involve risks and should therefore only be used with the prior consent of the Head of Unit and in strict compliance with CEA security rules governing information technology.

VI CONTROL AND TRACEABILITY OF THE USE OF COMPUTER MEANS AND INTERNET SERVICES

6.1 The CEA may carry out checks on the use of computer facilities and internet services available to users (network and hard disk space, internet traffic and connections, professional e-mail). The purpose of these checks is to ensure the security of the computer data of the public institution and at the same time, it will enable the CEA to detect any violations of this Charter.

6.2 The monitoring devices for individual analysis of user activity (surveillance of connections or sites visited, volume and the nature of files stored on network spaces or exchanged by courier, etc.), set up at the CEA, are subject to a prior declaration to the CNIL. They must specify their purpose, the data concerned, and the methods of access to this information as well as the specific period during which they are to be preserved.

6.3 These checks shall be carried out in accordance with the technical procedures approved by the Qualified Authority (based on a dossier, mentioning in particular the purpose of these checks, the personnel authorised to carry them out and the recipients of the results). The personnel authorized to carry out these operations are subject to a reinforced confidentiality obligation. Therefore, they cannot disclose the information they have come to know in the course of their duties, in particular all information relating to the secrecy of correspondence or the user's privacy. Only information that could interfere with the proper functioning of the applications, jeopardize security, the interests of the service or the correct application of this Charter is transmitted to the recipients of the results.

6.4 A system for logging internet access, professional e-mail and exchanged data is set up at the CEA in accordance with legal provisions.

6.5 IT administrators are responsible for ensuring the proper functioning and security of the computer resources. They are therefore required to have access to all the information stored or transiting there (messaging, internet connection, log files, etc.).
As such, they are subject to a reinforced confidentiality oath and therefore legally bound not disclose the information they have gained in the course of their duties, in particular those relating to the secrecy of correspondence or the privacy of users.

VII SPECIAL PROVISIONS

In view of the security requirements specific to information systems dealing with classified Defence information, special provisions are implemented, in particular, within the Military Applications Directorate (DAM) governing the use of computerized means.

APPENDICES

LIST OF HIGH VIGILANCE POSITIONS

DPSN DIR 2016-243 -1/4-

TOUCAN CODES THAT MAY QUALIFY PERMANENT HIGH DEGREE VIGILANCE ACTIVITIES AT THE CEA

ACTIVITIES REQUIRING A HIGH DEGREE OF PERMANENT VIGILANTE AT THE CEA	TOUCAN CODE	FAMILY CODE	TOUCAN FAMILY
High-level management functions, including research centre directors, institute directors, department and service heads **Responsibilities within the framework of security as defined according to the precise meaning of the NIG 613 of February 26th 2012, including those involved in crisis management and in the context of PMS and standby duty**			
Labels :			
- Responsibilities with decision-making	108 001	(CONPS)	*Work Conditions Psychological constraints*
- Time constraints	108 002		
- Requirements involving Reactivity and Initiatives in dealing with Multiple data	108 004		
- Hierarchical role	108 007		
- On-call Duty (standby constraints)	106 009	(MISSI)	*Work Conditions Work Hours*
Occupations involving the protection of persons, facilities and property			
Labels :			
- Shiftwork 24x48	101 014	(HORAI)	*Work Conditions Work Hours*
- Security station	201 011	(CONDU)	*Specific activities*
- Abuse investigation – Assaulting arrest	205 001	(SECUR)	*Specific activities Security, guarding*
- Dog trainer	205 002		
- Member of the ELPS	205 003		
- Firefighters	205 004		
- Carrying weapons (authorisation in the exercise of duties)	205 005		
- Carrying of tear gas bombs (authorisation in the exercise of duties)	205 006		
Professions consisting in the operation, monitoring or surveillance of processes involving substances dangerous to personnel or the environment (including those using hazardous chemical agents)			
Labels :			
- Radiological Emergency, Group 1	650 001	(ANORM)	*Radiological data Abnormal Work Situation*
- Radiological Emergency, Group 2	650 002		
- Radiological, security team	650 003		
- Concerted exceptional exhibition	650 004		
- Microbiological safety station 1	102 105	(EQUIP)	*Work Conditions Protective Equipment*
- Microbiological safety station 2	102 106		
- Microbiological safety station 3	102 107		
Activities requiring a certificate, special authorisation or accreditation to perform them : Electrical consignment and de-consignment operations			
Labels :			
- Electricity : High voltage B>50kV Ait or >75kV Continuous Current	302 004	(ELECT)	*Risk of a physical origin Electricity, electromagnetism*
- Electricity : high amperages	302 005		

APPENDICES

LIST OF HIGH VIGILANCE POSITIONS

DPSN DIR 2016-243 -2/4-

ACTIVITIES REQUIRING A PERMANENT HIGH DEGREE OF VIGILANCE AT THE CEA	TOUCAN CODE	FAMILY CODE	TOUCAN FAMILY
Activities requiring a certificate, special licence or accreditation for their proper execution - Professional driving of vehicles or machinery			
Labels : - Ambulance driving - Driving a vehicle in the workplace - Truck driving - Self-propelled driving, machinery - Driving public works machines - Crane driving	 201 001 201 002 201 007 201 003 201 005 201 006	(CONDU)	*Specific Activities* Operation of vehicles and machines

Activities requiring a certificate, special licence or accreditation for their proper execution. - Handling of heavy loads			
Labels :			
- Operating overhead cranes with port conductor	201 008	(CONDU)	*Specific Activities* Operation of vehicles and machines
- Operating overhead cranes, large hoists	201 009		
- Operating special handling equipment	201 004		
- Slinging/ Trussing	202 001	(MANUT)	*Specific Activities* Handling

Professions consisting in the operation, monitoring or surveillance of processes involving substances hazardous to the personnel or the environment (including those using dangerous chemical agents) Activities carried out in a restricted area, notably with regard to radiation protection, pyrotechnic enclosures, biological laboratories and animal facilities			
Labels :			
- Glove Boxes	102 101	(EQUIP)	Work Conditions *Protective Equipment*
- Clamping Boxes	102 102		
- Gloves Boxes	601 001	(CNDTR)	Work Conditions *Radiological Protection*
- Clamping Boxes	601 002		
- Remote manipulators	603 001		

Professions consisting in the operation, monitoring or surveillance of processes involving substances hazardous to the personnel or the environment (including those using dangerous chemical agents) Activities carried out in a restricted area, notably with regard to radiation protection, pyrotechnic enclosures, biological laboratories and animal facilities			
Category : - Chemical Products Selection to be made in the TOUCAN code	Code : 4xx xxx	One of the following criteria in the column marked information : CMR (professional illnesses) and SMR (heightened medical surveillance)	
Labels :			
- Firing of explosives	209 021	(AUTR))	Specific Activities
- Working with explosives	209 026		
Families :			
- Pathogens	521 001 at 521 154 522 001 at 522 134 523 001 at 523 026 524 001 at 524 069 525 001 at 525 005 531 001 0 539 032	(BACT) (VIRUS) (CHLEV) (PARA) (ATNC) (MEDBI)	Risks of a biological origin

APPENDICES

LIST OF HIGH VIGILANCE POSITIONS

DPSN DIR 2016-243 -3/4-

ACTIVITIES WITH A HIGH DEGREE OF PERMANENT VIGILANCE AT THE CEA	TOUCAN CODE	FAMILY CODE	TOUCAN FAMILY
Professions consisting in the handling, driving, monitoring or surveillance of processes involving substances hazardous to the personnel or the environment (including those using dangerous chemical agents) Activities carried out in a restricted area, notably with regard to radiation protection, pyrotechnic enclosures, biological laboratories and animal facilities Use or handling of controlled or hazardous substances or products			
Families : - External Exposure	610 001 at 610 009	(EXEXT)	Radiological Data
- Exposure at the extremities	620 001 at 620 002	(EXTRE)	
- Internal exposure	631 001 at 631 025 632 026 at 632 145 633 001 at 633 017 634 001 at 634 018 635 001 at 635 031 636 001 at 636 015 637 001 at 637 008 638 001 at 638 003	(INTER)	

Professions consisting in the driving, monitoring or surveillance of processes involving hazardous substances for the personnel or the environment (including those using hazardous chemicals) Activities carried out in a restricted area, notably for radiation protection, pyrotechnic enclosures, biological laboratories and animal facilities.			
Labels : - Self-contained breathing apparatus - Breathing apparatus with air supply - Filter Masks with cartridges	102 201 102 202 102 210	(EQUIP)	Work Conditions Protective clothing and wearing of protective clothing
- Self-contained breathing apparatus - Breathing apparatus with air supply - Non-ventilated protective clothing (overalls)	602 001 602 002 602 005	(CNDTR)	Work Conditions Radiological Protection
- Filter Masks with cartridges	602 010	(RADIO)	Radiological Data[2]

Professions consisting in the operation, control or monitoring of processes involving substances dangerous to personnel or the environment (including those using hazardous chemical agents) Activities carried out in a restricted area, notably with regard to radiation protection, pyrotechnic enclosures, biological laboratories and animal facilities Use or handling of controlled or hazardous substances or products			
Labels : - Non-ventilated protective suit - Anti-acid protective suit - Anti-sodium protective suit	102 205 102 203 102 204	(EQUIP)	Work Conditions Protective Equipment
- Workshop decontaminator - Site decontaminator - Scuba divers – divers	209 005 209 006 209 028	(AUTR)	Specific Activities
- Underwater work at relative pressure >100 hPa - Underwater work at relative pressure >100 hPa	303 201 303 202		Risks of a physical origin
- Anti-irradiation protective suit - Ventilated protective suit - Filter masks with no cartridge - Lead apron - Shielded containment	602 003 602 006 602 009 602 011 603 005	(CNDTR)	Radiological data

APPENDICES

LIST OF HIGH VIGILANCE POSITIONS

DPSN DIR 2016-243 -4/4-

PERMANENT HIGH DEGREE VIGILANCE ACTIVITIES AT THE CEA	TOUCAN CODE	FAMILY CODE	TOUCAN FAMILY
Handling of hazardous stationary or portable work equipment. This specifically includes portable electrical cutting or machining tools.			
Label :			
- Machine tools	203 003	(MECAN)	Specific Mechanical Activities
- Grinding, polishing	203 005		
- Torch brazing	206 001		
- Arc or plasma cutting	206 002		

APPENDICES

ANTI-CORRUPTION CODE OF CONDUCT

1. PROHIBITED BEHAVIOUR

CEA employees are required to comply with laws and regulations as part of the functions they perform within the organisation, particularly those that govern their behaviour with regard to integrity. The following chapter lists the issues of any type of conduct deemed unethical and, in particular, acts of corruption.

1.1. UNDER FRENCH LAW

Different types of behaviour, contrary to integrity and honesty, are prohibited by law and criminally sanctioned. These include the following types of behaviour:
• corruption;
• influence peddling;
• misappropriation;
• the illegal taking of interests;
• the misappropriation of public funds;
• favouritism.

Full legal definitions of these types of behaviour are given in the Appendix.

1.2. UNDER FOREIGN LAWS

The CEA's activities may be subject to foreign legislation, either by reason for the application of local law when the activities are carried out in the country concerned, or due to the extraterritorial application of certain laws such as the US Foreign Corrupt Practices Act of 1977. (FCPA) or the UK Bribery Act of 2010 (UKBA).

In case of doubt about the application of foreign practices or legislation, the employee must alert his or her line manager and, if applicable, the representative of the legal functional chain or the compliance officer, in order to check in advance the applicable rules and ensure compliance with them.

APPENDICES

2. RISK SITUATIONS AT THE CEA

The strengthening of laws and regulations to combat corruption requires vigilance in professional relations, both in France as well as on the international level. Every CEA employee must protect himself from any risk that is likely to involve him or her, directly or indirectly, in corruption or any other breach in his/her duty of honesty.

The situations described below are not all inclusive with regard to the circumstances to be addressed and risks that employees may encounter.

In case of doubt about the assessment of these situations at risk, employees are advised to contact their line manager or any other higher-ranking manager having power of decision.

2.1. THE ENTRY INTO A PROFESSIONAL RELATIONSHIP AND CONTRACTUALIZATION

What is it about?
It is crucial to know «who you are dealing with» when you enter into a professional relationship. It is a simple precautionary measure that we apply naturally enough in the personal domain when there are interests at stake.

In everyday language, the person with whom you enter into a relationship is called a «Third Party». It may be a supplier, a service provider or a subcontractor, a client, a consultant, an intermediary or a partner in the broad sense of the term.

Points of vigilance
When entering into a relationship with a French or foreign Third Party, the points of vigilance concern the following aspects that make it possible to assess the level of risk of the proposed relationship:
• the Third Party's reputation and financial strength;
• verifications on the transparency of shareholding, as well as that of the accounts, where the Third Party is a legal person;
• the compliance policy of the Third Party concerned;
• depending on the country of membership of the Third Party, anti-corruption legislation in force.

Proper conduct:
Any employee may be confronted with a wide range of very different situations of which it is not possible to draw up an exhaustive list. In case of doubt, the employee must notify his or her line manager and, if applicable, the representative of the legal functional chain or the person in charge.

APPENDICES

2.2. GIFTS AND INVITATIONS

What is the issue here?
Gifts can take on many forms and are considered to be advantages or favours, granted without consideration or compensation.

These may be objects offered occasionally or periodically in the framework of professional relations, business meals, invitations to events, exhibitions, sports events or trips that combine both leisure and professional purposes, commercial conditions or preferential rates, etc.

Vigilance Points
These gifts and invitations offered by suppliers, service providers or subcontractors or partners, or we may ourselves offer them with the intention of contributing to the good quality of professional relations. These are manifestations of courtesy and mutual appreciation which may sometimes be customary in some countries.

However, vigilance must be exercised to ensure that gifts and entertainment do not involve any consideration in any form whatsoever, explicit or implicit.

More specifically stated, they must not under any circumstances influence or convey an impression that might unduly influence the judgement or decision-making capacity of CEA employees.

These gifts and invitations must be made in a professional context, remain reasonable in both frequency and amount, be accepted in complete transparency and, if possible, they should be shared among a team.

Particular caution must be used in the case where the beneficiary holds a power of decision or influence over actions that may affect the interests of the CEA, in particular through the granting of an authorisation, the signing of an agreement or awarding a contract.

Proper Conduct:
Under no circumstances whatsoever may CEA employees accept or offer, on a personal basis, cash gifts, gift vouchers, discounts, gifts of a monetary nature, tariff advantages or financial rewards. Similarly, gifts or invitations during a period of a call for tender, in which the employees are directly or indirectly involved in the procedure, are formally prohibited.

APPENDICES

In other cases, the following rules should be observed:
• gifts or invitations with an estimated value of less than 50 euros may be offered or received without information or authorisation from the employee's line manager;
• gifts or invitations with an estimated value between 50 and 150 euros may be offered or received. In such cases the employee's line manager must be informed;
• the principle is that gifts or invitations with an estimated value of more than 150 euros must be refused and may not be offered.
However, if, for specific reasons (cultural, cyclical), the employee is forced to accept, he/she will have to report to his/her direct line manager and to the compliance officer at the CEA level, by providing the necessary justifications. Similarly, if for specific reasons, the employee is led to consider offering a gift or a gift to an invitation for an amount exceeding 150 euros, he or she may only do so after authorisation from the compliance officer at the CEA level has been granted.

In all cases, it is highly recommended to keep a record of these gifts to avoid any suspicion in the future.

In the event of a repetition of gifts or invitations from the same person or entity, the threshold to be used is then assessed based on the corresponding overall amount of gifts and invitations received or offered in the same year.

In case of doubt, or in order to obtain further information, the employee must contact his or her line manager or compliance officer.

Example:

Can I accept a VIP invitation from a supplier to see an exhibition or show for two people?

The answer to this type of question requires us to consider a number of points of vigilance, such as the estimated amount of this gift, its nature, as well as its context and frequency. Regarding an amount a priori close to 150 euros, it is essential to inform your line manager.

With regard to context, it is imperative to be at a distance from a period of time of any tender or negotiation in which we are involved.

Moreover, in terms of frequency this type of invitation must not occur more than once a year.

APPENDICES

2.3. CONFLICTS OF INTEREST

A conflict of interest situation is likely to alter a person's objectivity and therefore his or her ability to fulfil his or her mission.

What is it about?
An employee is in a conflict of interest when he or she has an interest in personal, financial or commercial matters that may have an influence on the objectivity of the decisions he or she makes or recommends or the advice he or she gives performance of his or her duties.

This situation can occur, for example, when the employee:
• carries out extra-professional or professional activities outside the CEA;
• has relatives in his or her circle who work for suppliers (or service providers, subcontractors) in his or her unit.

This situation may be such that it could conceivably lead the employee concerned to violate his or her oath of loyalty to the CEA. It may also incite the employee to commit acts of corruption and other related offences.

Points of vigilance
Before any decision is taken that involves the CEA, each party must consider the existence of any relationship, personal or otherwise and of any nature whatsoever, that might seriously influence his or her decision, recommendation or judgment.

Similarly, outside the professional context, every employee must take care not to create a situation or make commitments that could cause him to violate the law or his/her oath of loyalty to the CEA.

Proper Conduct:
Should an employee find himself (or herself) confronted with a conflict of interest situation concerning him directly or indirectly, he or she must alert his or her line manager and, if applicable, the compliance officer, about:
• any risk, suspicion or identified conflict of interest situation;
• any solicitation or inappropriate behaviour that could create such a conflict;
• any pressure, threat or act of blackmail, either internal or external.

Information relating to conflict of interest situations must be recorded in writing and kept within the units concerned. They must be presented at any subsequent inspection. In the event of a job transfer and if the conflict of interest situation persists, a new declaration must be made.

The employee must also abstain from any decision-making process, from any recommendation or professional advice that may affect this conflict of interest.

APPENDICES

Example
A conflict of interest situation may arise when:
• as a buyer or prescriber at the CEA, a member of my family works for a company bidding on a call for tender issued by the CEA;
• as a manager, I plan to hire a family member to hold a position in the unit I supervise or with whom I have ongoing relationships;
• I develop a friendly relationship with a supplier, service provider or subcontractor who is working in my unit;
• I take a financial stake or responsibility in a company supplier, a service provider, a subcontractor, a partner of the CEA or any organisation or company with which the CEA has a business relationship (start-up, investment funds in particular).

All cases of conflict of interest must be reported to one's line manager and inquiries must be made about the appropriate course of action to be taken.

APPENDICES

2.4. FACILITATION PAYMENTS

What are facilitation payments?
Facilitation payments consist of small payments made to public services in order to secure or accelerate the execution of standard administrative acts or the necessary formalities involved for this purpose.

Points of vigilance
Although the use of facilitation payments is a common practice in some countries, it remains a form of extortion that can be likened to acts of corruption.

The conduct to observe in such a situation
The CEA prohibits the use of this practice, which constitutes a form of corruption. Using the facilitation payment may expose CEA employees to criminal proceedings and damage the reputation of the CEA.

In such a situation, the CEA employee must contact his or her line manager.

Examples
• a public official requests a personal commission to issue the visa necessary for a professional mission;
• in the context of a forum taking place abroad, I need to transfer a demonstration prototype. On the spot, a local public official asks me for a payment for the technical approval of this equipment;
• I am asked for payments to speed up the clearance of equipment.

In all these situations where payments are prohibited by the CEA, I do not pay and I contact my line manager.

2.5. PATRONAGE AND SPONSORSHIPS

What constitutes patronage or sponsorship?
Patronage is financial or material support provided, without direct compensation on the part of the beneficiary, to a work or to a person for carrying out activities of general interest.

Sponsorship is financial or material support provided by a natural or legal person to a demonstration, to a person, to a product or to an organisation for direct benefit.

As part of its activities, the CEA may participate in structures such as an association the purpose of which is directly related to its activities and, on an exceptional basis, make donations or accept donations or bequests.

APPENDICES

The authorisation of the CEA to make donations is, according to the amount, under the jurisdiction of the Deputy Head or a senior member of one of the operational directorates.
Conversely, the CEA is entitled to receive any donation or bequest in cash or in kind. Any acceptance of donations or bequests by the CEA must be the object of an authorisation accorded by the CEA Board of Directors, subject to a delegation of powers granted to the Deputy Head up to a maximum of one specific amount.

Points of vigilance
Even if, under certain conditions, patronage or sponsorship actions can be presented as natural extensions to activities in the general interests of the CEA, they can provide favourable grounds for actions or attempts of corruption.
In addition to compliance with the procedures applicable to the CEA in authorising these actions, it is necessary to verify that they do not in fact constitute a means of receiving or granting undue advantages, favouring transaction influence or personal pecuniary interests.

Proper Conduct
Any employee involved in the acceptance of donations or bequests to the benefit of the CEA or, on the contrary, involved in a grant made by the CEA to a Third Party, must comply with applicable internal procedures.

He or she must also verify, at his or her level, that these operations comply with the principle of integrity and the CEA's policy in this area, by ensuring that in particular the patronage or sponsorship concerned:
• is directly related to the activities of the CEA;
• is entered into with a Third Party whose reputation has been previously verified;
• is not entered into in the presence of a conflict of interest;
• does not favour transactions of influence or pecuniary interests either personal or extra-professional;
• does not constitute an undue advantage.

In case of doubt in the application of these principles, the employee concerned must alert his line manager before proceeding with any patronage or sponsorship.

Examples
Increased vigilance in sponsorship operations must be exercised in operation when there are certain clues, for example when:
• the association or foundation for which a CEA grant is being considered carries out activities far from those related to the CEA;

APPENDICES

• suspicions exist as to the reputation or integrity of an association or foundation, or its staff, for whom a CEA grant is being considered;
• it is proposed to the CEA to receive a donation as part of the sponsorship, in exchange for a commitment by the CEA to carry out certain activities not directly related to the donation;
• suspicions exist as to the reputation or integrity of an entity that has expressed the wish to make a donation or bequest to the CEA.

In case of doubt in the application of these principles, you should alert your line manager before proceeding with any patronage or sponsorship activity.

2.6. LOBBYING

What is lobbying?
With regard to the Sapin II Law, the CEA is a «representative of interests» or lobbyist. Its employees' main activity is to influence public decision-making, including the content of a law or regulatory act (lobbying). To influence the decision, these employees can enter into communication with members of the Government, or parliamentarians, or with locally elected key officials and public decision-makers. In this respect, the CEA complies with its reporting obligations, including the registration of its employees concerned by a lobbying activity, in the digital directory of the High Commission Authority for the Transparency of Public Life (HATVP), as well as the presentation of an annual report describing the actions carried out over the past year and the amount of the corresponding expenses.

Points of vigilance
Anyone can have relationships with members of the Government, parliamentarians, locally elected officials and more generally public decision-makers, i.e. in the professional context or due to private activities.

In the professional context, any CEA employee not involved in a lobbying activity and not listed in the digital directory of the High Authority for the Transparency of Public Life (HATVP), must inform his line manager if contacts with public decision-makers become frequent, amounting to a primary or regular activity within the meaning of the law.

Proper conduct:
With regard to public authorities, when engaging in any lobbying action it is necessary to exercise one's functions in a loyal and responsible manner excluding any practice amounting to corruption or influence peddling.

No CEA employee is authorised to engage the organisation directly or indirectly in an activity supporting a party of any kind or a political organisation. Furthermore, he/she must never rely on nor take advantage of his or her status as a CEA employee for this purpose.

Example:
The mayor of my municipality, whom I know personally, calls on me at the time of the elections, to show my support as an employee of the CEA. What attitude should I adopt?

Such a request must be refused, as the CEA must respect a principle of absolute neutrality and therefore cannot, directly or indirectly, contribute its support to anyone.

The same rule applies if you are a candidate in an election.
In case of doubt, you should refer to your line manager.

3. COMPLIANCE WITH THE CODE OF CONDUCT

Every CEA employee must observe behaviour that respects the provisions of this code of conduct.

In addition to any criminal sanctions that may be applicable depending on the gravity of a breach of probity, any breach of this code of conduct is likely to result in disciplinary action that could even include outright dismissal.

4. THE REPORTING SYSTEM

4.1. WHO REPORTS WHAT?

The purpose of this system is to permit the collection of information, namely:
• alerts relating to the existence of a type of conduct or situations that enter into conflict with this code of conduct on the part of CEA employees. If it is a question of behaviour that may characterise acts of corruption (see § 1.1 Under of French law), the author of the alert may benefit from the protection of whistleblowers provided for by the Law n°2016-1691 of December 9th 2016 regarding transparency, the fight against corruption and the modernisation of economic life known as Sapin II;
• reports of crimes or misdemeanours, serious violations of the law or of a regulation, threats or serious prejudice to the general interest, brought to the authorities' attention by CEA employees or external and occasional collaborators (Article 6 of the Sapin II law). For this type of alert, the person issuing the alert may benefit from the protection of whistleblowers.

APPENDICES

In other words, deviations from the code of conduct can be the subject of a denunciation by CEA staff (regardless of their status: permanent contract, fixed-term contract, etc.), while alerts under Article 6 of the Act may be issued by CEA staff or by an external and occasional collaborator.

In all cases, the person issuing the alert must be a natural person. He must be acting in good faith and without interest. He must have first-hand, personal knowledge of the facts he or she is reporting.
Misuse of the system may expose the perpetrator to disciplinary action that can even include dismissal.

It must also be pointed out that any author of allegations that he or she knows to be false cannot be considered to be «in good faith» and is subject to prosecution under the law against slanderous denunciations (5 years' imprisonment and 45,000 € in fines).

Any person who obstructs, in any way whatsoever, the transmission of a report, is liable to one year's imprisonment and a fine of 15,000€.

An alert may not relate to items covered by the secrecy of the national defence, medical secrecy or the secrecy of relations between a lawyer and his client. The Directorate of Military Applications is concerned by the system of an alert as long as the subject of the alert is not covered by the secrecy of the national defence.

The system shall guarantee the strict confidentiality of the identity of the person issuing the alert, the facts subject to the alert and the persons concerned, including when required communication with third parties, without prejudice to the legal obligations to communicate to the judicial authorities.

4.2. HOW MUST ONE REPORT AN OFFENCE OR VIOLATION?

To issue an alert, several communication channels are available:
The person issuing the alert may use the telephone, the national postal service or internal mail, electronic mail and /or personal delivery.

In all cases, alerts should be sent to the Referent of the CEA report.

The system for collecting and processing alerts shall be subject to a procedure available based on the CEA's internal regulations «BRICEA».
(http://referentiel functional.intra.cea.fr/legal).

APPENDICES

5. APPENDIX

5.1. GENERAL DEFINITIONS

Ethics is the set of values and moral principles that form the basis of a person's conduct and which serve as the basis for life in society.
Professional ethics refers to the values and moral principles that motivate the conduct of people in the workplace, whether they belong to the same profession or work in a specific structure.

Deontology refers to the set of rules and duties governing conduct to be observed for members of a profession or for persons practising their activity in a given structure. It is confused with professional ethics.

Compliance is the action that consists in observing the rules and duties governing the conduct that must be imposed for members of a profession or for persons practising their activity in a given structure. It is confused with professional ethics.

Conformity refers to the action aimed at implementing measures or behaviours, within a given structure in accordance with an established standard (external and/or internal) applicable to the place and in the fields where this structure exercises its activity.

Compliance, inspired by Anglo-Saxon practices, and which is very similar to the concept of conformity, is defined as the set of processes that allow us to ensure the standards applicable to a given structure by all its members, but also values and an ethical spirit inspired by its leaders.

Probity is the quality of a person (and consequently his or her conduct) who observes and upholds the values and moral principles that underpin life in society, scrupulously respects his or her duties as well as the law, regulations and any standards applicable to the activity or in the structure where he or she is employed.

Integrity is the quality of a person (and his or her behaviour) who respects the values and moral principles that underpin life in society and who is faithful to his or her duties and commitments.

Scientific integrity is defined as the set of rules and values that must govern research activity in order to ensure its honesty and scientific rigour.

APPENDICES

5.2. OFFENCES PUNISHABLE BY THE PENAL CODE

Bribery is the behaviour of a person who consciously solicits, agrees or accepts a gift, an offer or promise, or a benefit of any kind, in exchange for performing, delaying or failing to perform an incoming act, either directly or indirectly, in the course of his duties and related responsibilities.

Criminal law distinguishes two types of **bribery**:

• **active bribery**, which consists of any individual proposing, directly or indirectly, offers, promises, gifts, presents or benefits to a person who exercises a function and holds power in exchange for something (Articles 433-1, 1 ° and 445-1 of the French Penal Code);
• **passive bribery** which may be defined by the behaviour of any person who, by virtue of his/her positiotn and power, solicits or agrees, directly or indirectly, to accept offers, pledges, donations, gifts, presents or benefits of any kind for himself or herself or for others (art. 432-11, 1°, and 445-2 of the French Penal Code).
The functions of the corrupt person may be public (persons holding public office, entrusted with a public service mission or invested with a public elective mandate - art. 433-1, 1°, and 432-11, 1°, of the French Penal Code) or private (art. 445-1 and 445-2 of the French Penal Code).

When the corrupted person is a person holding public office, corruption consists of an act of his or her function, mission or mandate, or facilitated by his or her function, mission or mandate. The corrupt parties may be convicted and sentenced to a penalty of ten years' imprisonment and a maximum fine of 1,000,000 euros. This amount may be increased to double that amount according to the profits gained from the offence.

When the corrupt person is a person working in the private sector, the bribery is an act involving one's activity or function or facilitated by one's activity or function, in breach of his or her legal, contractual or professional obligations. Both persons including the person accepting the bribe or the person who has offered it, are sentenced to five years' imprisonment and a fine of up to 500,000 euros, which may be increased to twice that amount according to the proceeds gained from their offence(s).
Influence peddling has characteristics very similar to the crime of bribery.
The difference is that in influence peddling, the perpetrator does not himself (or herself) actually have the power to perform or refrain from performing the act coveted by a third party.

The purpose of the manoeuvres lies here, for the one who has influence, real or supposed, to use this influence to the advantage of a third party in order to obtain from an authority or a public administration distinctions, jobs, contracts or any other public administration favourable decision (arts. 433-1, 2°, 433-2 and 432-11, 2°, of the French Penal Code) in exchange for an offer, a promise, gift or advantages of any kind.

APPENDICES

As in the case of bribery, influence peddling may be defined as passive with regard to the person who uses his influence and active towards the person who benefits from it.
When the person using his influence is a person in public office, the person receiving the bribe and the person providing the bribe shall be liable to a penalty of ten years' imprisonment and a fine of up to 1,000,000 euros. This amount may be doubled according to the profit obtained from the offence.
When the person using his or her influence is not involved in the public sector, the person receiving the bribe and the person providing it shall be sentenced each to five years' imprisonment and a fine of up to 500,000 euros, which may be increased to double that amount according to the profits obtained from the offence.

CONCUSSION is the unlawful forcing of another by threats of violence to give something of value. It differs from robbery in that in robbery the thing is taken by force, while in the case of concussion it is obtained by threatened violence.

In French «**Concussion**» consists in taking money that has been entrusted into one's care unlawfully and as such, it constitutes a breach of the duty of probity. It may occur when the perpetrator is acting for purposes of personal enrichment or when he or she is acting for unselfish purposes. For a public authority or any person entrusted with a public service mission, it consists in:
• receiving, requiring or ordering the collection of contributions as fees, public taxes, an amount that he or she knows not to be due or to be in excess of the actual amount due (Art. 432-10 (1) of the French Penal Code);
• granting in any form whatsoever an exemption or franchise, exemptions or public duties, contributions, taxes or duties, in violation of the legal texts (Art. 432-10, para. 2, of the French Penal Code).

Concussion is punishable by five years' imprisonment and a fine of not more than 500,000 euros, which may be doubled according to the amount gained from the offence.

The illegal taking of interests concerns in particular any public authority or any public official entrusted with a public service mission.

It consists in taking, receiving or keeping, directly or indirectly, any interest in a company's shares or in a company operation in whole or in part, for which he or she has been entrusted with the responsibility of ensuring its supervision, administration, liquidation or payment (s. 432-12 of the French Penal Code).

This offence is also likely to be committed after cessation of the activity and for a period of three years of one's functions as a member of the Government, as a member of an administrative and independent authority or as a public authority holding a local executive office, a civil servant, a member of the military or an officer of a public administration.

APPENDICES

In such a case, the individuals mentioned above are guilty of taking interests illegally if they acquire or receive shares by work, advice or capital in a private company over which they, during the previous course of their functions, had exercised supervision or control or concluded contracts.

This offence is punishable by five years' imprisonment and a fine of not more than 500,000 euros. This amount may be doubled according to the profits gained from the offence.

Misappropriation of Public Funds concerns in particular the following people: a person who is the depositary of a public authority or who is in charge of a public service mission, a public accountant, a public depositary or one of his or her subordinates (Article 432-15 of the French Penal Code).

For this person, this offence consists in destroying, embezzling or withholding, in particular public or private funds, effects, securities or any object that has been entrusted to them by virtue of their functions or mission.

This offence is punishable by ten years' imprisonment and a fine of not more than 1,000,000 euros. This amount may be increased to twice the proceeds of the offence.

Favouritism concerns in particular the following people: the depositary of a public authority or a person in charge of a public service mission or a person exercising the functions of representative of a Public Establishment and any person acting on behalf of the latter (Art. 432-14 of the French Penal Code).

It consists in procuring or attempting to procure for others an unjustified advantage in violation of laws and regulations intended to guarantee freedom of access and the equality of candidates in public procurement and concession contracts. This may include, for example, non-compliance with the rules of procedure for public procurement markets (non-compliance with the obligation to launch a call for tender) or the transmission of privileged information to one or more candidates.

This offence is punishable by two years' imprisonment and a fine of 200,000 euros at most, an amount that may be increased to twice the proceeds of the offence.

APPENDICES

SYSTEM FOR THE COLLECTION AND PROCESSING OF REPORTS WITHIN THE FRAMEWORK OF THE SAPIN LAW II

1. SCOPE OF THE REPORTING SCHEME

The Law No. 2016-1691 of December 9th 2016 pertaining to transparency, the fight against corruption and the modernisation of economic life, known as The Sapin II Law, requires legal entities to establish procedures for the collection and processing of alerts coming from:
• Its staff. Such alerts may report the existence of conduct or conflicting situations in violation of the Anti-Corruption Code of Conduct (art. 17).
• Whistle blowers. Such alerts may report the perpetration of a crime or misdemeanour, a serious and manifest violation of a regularly ratified international commitment or the violation of such a commitment approved by France, of a unilateral act of an international organisation taken on the basis of a commitment, a law or regulation, or a threat or serious harm to the general interest (art. 6).

In other words, deviations from the code of conduct may be reported by the CEA staff (regardless of their status as permanent employees, fixed-term contract employees, trainees, etc.), while the alerts falling under the terms of Article 6 of the Act may be issued not only by CEA staff but also by an employee from an outside firm and/or an occasional collaborator.

The CEA has chosen a specific procedure that is designed to receive the alerts mentioned above, to the exclusion of any other report.

2. CONDITIONS OF ADMISSIBILITY

To issue an alert, the person issuing the alert must:
• be a natural person;
• have personal knowledge of the facts that he or she is reporting. It is therefore not a question of reporting facts confirmed by others, but a faithful reporting of facts personally observed;
• act in a non-self-serving manner. He or she must not benefit from any advantage or compensation for their efforts. The support that the author is, the case as appropriate, likely to seek (such as, for example, support by a trade union organisation representative) does not question the lack of interest in the process;
• act in good faith. At the time the report is made, the facts disclosed must present a clear violation of the Anti-Corruption Code of Conduct or facts stated must justify an alert so that a posteriori, it cannot be alleged that the author of the alert had simply and dishonestly sought to harm others.

APPENDICES

3. CONTENT OF A REPORT

The alert must include the following information:
• identity, functions and contact details (including one's home address) for sending the letter acknowledging receipt of the alert) from the sender of the report;
• the identity, and to the greatest extent possible, the functions and contact details of the persons who are the object of the alert;
• a description of the reported facts.

An alert may not relate to items covered by National Defence secrecy, medical secrecy or the secrecy of relations between a lawyer and his client. However, the DAM is still concerned by the system of alert as long as the subject of the alert is not covered by the National Defence secrecy.

4. HOW DOES ONE MAKE A REPORT?

The Referee of the reporting system, designated by the CEA, is the addressee of the report. (The person to whom the alert report must be sent) The alert must be transmitted to him/her:
• by post to the referent of the alert system, by taking special care to specify in writing on the front of the envelope, «TO BE OPENED ONLY BY THE RECIPIENT OR HIS OR HER DEPUTY»;
• by email, preferably with an encrypted message, to signalement@cea.fr. The subject of the message must include the following information: «Personal and confidential»;
• by telephone. In this case, the alert must be formalised later in writing; or by hand-delivered mail.

Any other means used to issue an alert cannot ensure absolute confidentiality of the alert report.

The person issuing the alert shall provide, where appropriate, the information or documents substantiating the details of his or her alert report.

5. CONFIDENTIALITY

The identity of the person issuing the alert, the persons concerned by it and the information obtained during the alert is strictly confidential. Information that might identify the person who issued the alert may not be disclosed except to the judicial authority, with the consent of the latter.

Elements likely to identify the person accused by an alert may not be disclosed, except to the judicial authority, until the truthful basis of the report has been clearly established.

6. PROCEDURES FOR RECEIVING THE ALERT

The reporting mail/email can only be opened by the Referent or in the case where applicable, his deputy who is subject to the same oath of confidentiality.

Regardless of the transmission channel of the alert, the Referent or, where applicable his deputy must send its author the following:
• within 7 working days a letter acknowledging receipt of the alert;
• within one month, a letter acknowledging receipt and stating the foreseeable time required to examine the admissibility of the alert and how he/she will be informed of the action taken on it (rejection for inadmissibility or referral of the alert to the records - see below).

7. INFORMATION GIVEN TO THE PERSON CONCERNED BY THE ALERT

The person concerned by the alert is informed by the Referent or, where applicable his deputy, as soon as the data concerning him is recorded, whether it is computerised or not, so that he or she may exercise his or her right to object, for legitimate reasons, to the processing of such data.

Where provisional measures are necessary, in particular to prevent the destruction of evidence relating to the alert, informing that person takes place after these measures have been taken.

This information, which is provided in the context of an interview with the person who has been targeted by the alert, (and who may be accompanied by a CEA employee, after prior information has been given to the Referent), specifically states:
• the name of the Referent who is in charge of the inquiry;
• the alleged facts;
• the services to which the alert may be sent;
• the procedures for exercising all rights of access and rectification of data.

At the end of the interview, a report is drawn up by the Referent or, if necessary by his or her deputy, and submitted to the person concerned.

APPENDICES

8. PROCESSING OF THE ALERT REPORT - ANALYSIS AND INVESTIGATION

An alert/report is the subject of a preliminary analysis by the Referent or if necessary, his deputy who is bound by the same oath of confidentiality, in order to determine its admissibility and, where applicable, the provisional measures necessary.

As soon as an alert is deemed admissible by the Referent, he/she shall convene the Alert Processing Committee (APC). The role of the APC is to:
• take note of all alerts, whatever their origin
• validate the admissibility, within the terms of the law, of each alert as well as the criticality level;
• decide on any additional protective measures to be taken and establish the appropriate investigation program (designation of a pilot, review of the main actions to be carried out as part of the investigation);
• propose, at the end of the investigations, the follow-up to be undertaken and, if necessary, any possible sanctions;
• declare the files closed.

The members of the APC analyse the appropriate follow-up. Their task is to ensure that the data concerning the person issuing the alert and the accused employee are well founded, relevant and not excessive in relation to the purposes for which they were collected. If this is not the case, the data is as destroyed.

APC members may decide to conduct an investigation to ascertain the reality and materiality of the reported facts. Any possible further investigations are first managed “in house” (i.e. within the CEA establishment). They may benefit from the possible support of any external source, bound by the same oath of confidentiality.

The Deputy Head of the CEA («l’Administrateur Général») appoints members of the APC. They are subject to an oath of confidentiality that also applies to all other persons called upon to intervene in the processing of the alert.

9. CLOSURE OF THE PROCEDURE

Closure is decided by the APC. The Referent shall inform the author of the alert and the persons concerned by it, of the closure of the procedure within 15 days of the closure decision.

APPENDICES

10. DATA PRESERVATION PERIOD

When an alert is considered inadmissible by the Referent or the APC because it does not fall within the scope of the system, the corresponding data is immediately destroyed.

When an alert is not subject to disciplinary or judicial prosecution, deletion of the data takes place within two months after the closure of the verification of the alert under the conditions of the present procedure.

When disciplinary proceedings are initiated against the person accused of the offence or a perpetrator of an abusive alert, the data relating to the alert and its processing is stored, as part of an information system with restricted access. The data in question is to be stored for a period not exceeding the limitation period of any legal action challenging the disciplinary measure, if any, or until the end of the proceedings and the exhaustion all legal recourse.

In the event of legal proceedings being brought against or at the initiative of the person implicated or the person who issued an alert, the data relating to the alert and its processing is kept, within the framework of a system of separate information with restricted access, until the end of the proceedings and exhaustion of all legal recourse.

Data subject to archiving measures shall be kept, as part of a separate information system with restricted access, for a period not exceeding the time limits for litigation proceedings.

11. AUTOMATED PROCESSING OF ALERTS

The procedure requires the implementation of automated processing of reports. This processing meets the criteria set down in the single authorisation AU-004 of automated processing of personal data and it is implemented within the framework of the professional alert systems of The National Commission of Computer Sciences and Liberties (CNIL).