EIFFEL
INVESTMENT GROUP

RULES OF PROCEDURE AND DEONTOLOGY

These rules of procedure are intended to fix within Eiffel Investment Group SAS (hereinafter “EIG” or “the Company”):

- the measures for the application of the rules in the field of health and safety;
- the disciplinary procedures and penalties and to recall the provisions relating to the rights of defence of the Company's employees;

These rules of procedure apply to all EIF employees. Its provisions relating to health, safety and working conditions apply also to any person present in the firm in the capacity of an employee of a temporary employment agency or a trainee and, generally, any external person who carries out work in the firm in whatever capacity. The provisions of these rules of procedures are notably applicable not only in the actual workplaces but also in the appurtenances (premises or areas outside the work premises, such as the car park, restaurants, etc.)

The SGP rules of procedure are available on the EIG Compliance network and may be accessed by all EIG employees.

1. HEALTH, SAFETY AND WORKING CONDITIONS

Any person subject to these rules of procedure must, in the context of their professional activity, refrain from negatively impacting their safety, health and that of the other persons which whom they are in contact when carrying out their duties.

The employees have the duty to respect the instructions that are given to them by the supervisory staff for the execution of their work and, notably, the safety instructions specific to this execution; hence, the respect of an instruction given by a line manager shall not have the effect of allowing the employees to be declared personally liable.

1.1. Use of means of protection

It is compulsory to implement all existing personal or collective safety and protection measures and to scrupulously respect the instructions on this point. It is prohibited, in particular, to remove or neutralise existing safety devices without the authorisation of those in charge of the firm's safety. It is prohibited to block access to safety equipment (extinguishers, first-aid kits, etc.), move them without good reason or put them to another use.

1.2. Repairs to equipment

Whilst the firm is responsible for maintaining all equipment in good working order, employees must ensure it is clean by respecting the instructions that have been given to them in this respect and notify their line manager or the manager of any failure or defect noted.

It is formally prohibited for those operating the equipment to attempt to repair any machine or equipment whose maintenance is entrusted to specialised staff. All halts in the functioning of machines or equipment and all incidents must be immediately notified to the line manager.

1.3. Accident at work or when going to or returning from work

Any accident at work, even minor or any other bodily injury or damage caused to a third party must be immediately, unless a case of force majeure, reported by the interested party or witnesses to the line manager.

1.4. Personal objects

Staff must keep their personal office cupboards and drawers perfectly clean; it is prohibited to keep perishable food or dangerous substances in the aforesaid. The firm reserves the right to have the aforesaid opened, if this is necessary for reasons of health and safety, in the presence of the interested party or, in the absence of the employee and in the case of exceptional circumstances, in the presence of two members of the firm, of which one a line manager. In this specific case, a formal report shall be drawn up and signed by these two people.

1.5. Alcohol and drugs

It is prohibited to enter or stay in the firm's premises in a drunken state or under the influence of drugs.

Alcoholic beverages may be brought into the firm's premises to be consumed at festive events with the authorisation of the line manager.

1.6. Tobacco

For health and safety reasons, and in application of decree n°92-478 of 29 May 1992, it is prohibited to smoke in work common rooms, notably in open-plan offices and areas for use by all employees, such as meeting rooms, reception room and entrance hall.

It is only possible to smoke in the rooms and places put aside for this purpose, in personal offices when other employees are not present and if the ventilation equipment is suitable.

1.7. Medical check-ups

Before being hired or, at the latest, before the expiry of the probationary period that follows hiring, each new employee must undergo a medical check-up by an occupational health doctor from the company's occupational health department.

All employees must undergo regular medical check-ups when requested to do so by the occupational health department.

After an absence of at least 21 calendar days due to a non-occupational accident or illness, or eight calendar days due to an occupational illness or accident, after maternity leave or in the case of repeated absences, the employee must undergo a check-up by the occupational health doctor. This check-up is carried out within eight days of the person's return to work.

Moreover, the employees assigned to work that is exacting or where there are special risks recognised by regulations or the firm's occupational doctor benefit from special monitoring by the occupational health department, to which they must submit.

1.8. Fire and other incidents

Employees must read the displayed safety and evacuation instructions that are to be respected in the case of fire or other incident.

In the case of an incident (fire or other), the employee must give the alert indicating the place of the incident, strictly respect the instructions and obey the evacuation orders that are given to him.

2. DISCIPLINE

2.1. General discipline

In the performance of their employment contracts, employees are bound to respect the instructions of their line managers, and all instructions given by the firm and circulated by memorandums and displayed on notice boards. Any act in contravention of the above may lead to penalties. All employees must be dressed appropriately and behave correctly in respect to their colleagues, their line managers and clients. Their relations, in the context of their professional activity with clients, suppliers, line managers and colleagues must not be of a type to harm the firm's image or work relations within the firm.

When performing their employment contracts, the employees are bound by a duty of loyalty to the firm which prohibits them from carrying out any rival business activity directly or through an intermediary, on own account or on behalf of a third party.

2.2. Working hours

Employees are bound to respect the provisions relating to the organisation of their working time specified in their contract.

The non-respect of the working hours constitutes the non-fulfilment of contractual obligations justifying the application of disciplinary measures.

The employer or the latter's representative is responsible for the proper application of provisions relating to regulations on working hours.

Any overtime worked must meet the department’s needs and be worked at the express request of the line manager.

2.3. Absence

Except in exceptional circumstances that prevent this, all absences, apart from those concerning illness, maternity, the application of regulatory provisions of collective agreements or agreements internal to the firm, must be previously authorised by the Management of the entity for which the employee works. Unauthorised absence constitutes a failure justifying the application of disciplinary measures.

Any unavailability due to illness or an accident, and any absence for a family event must be notified to the line manager within 24 hours at the latest, except in the case of a force majeure.

Except in cases of force majeure, a medical certificate justifying, from the first day, any absence for illness, or accident at work or going to or from work must be provided within 48 hours.

The same rules are applicable to successive extensions of absences from work; their non-respect shall lead to penalties.

Any employee who is found to have given an incorrect reason to obtain an authorisation for absence commits a serious failure, justifying the application of disciplinary measures.

2.4. Access to the premises; arriving and leaving

Access by staff to the firm's premises is reserved to employees who need access to perform their tasks; employees do not have the right to enter and stay in the workplace for any other reason, unless they provide proof of an authorisation from their line manager. This provision may not have the consequence of preventing an employee from entering the premises of the works council, employee representative body or trade union organisations.

Except for reason of service or reason linked to the Company's activity, employees may not bring into the premises individuals not part of EIG, apart from suppliers, service providers and couriers who must make known their identity and the reason for their visit.

In addition, access to the Company's trading platform is strictly reserved for EIG employees.

It is prohibited to sell merchandise inside the firm's premises.

Except in the conditions specified by the law, there must be no circulation, in any form whatsoever, of pamphlets containing political, commercial or religious propaganda, subscription, collection, lottery or petition lists, or membership cards or lists for any purpose whatsoever. This provision shall not affect the rights and entitlements, resulting from the law and/or collective agreements, of employees who hold an elected office or trade union responsibilities.

2.5. Protection of material and tools

Employees are bound to keep in good condition all the material with which they are entrusted to perform their employment contracts; this applies notably to headphones, mobile phones, or IT resources, the more so if they are portable, which may be placed at their disposal.

Any use of this material outside the firm's premises is subject to prior authorisation by the line manager.

Any disappearance or malfunctioning of such material or any other damage must be immediately notified to a line manager.

In the case of a business trip or other absence, notably during meal times, employees must ensure that confidential documents or files in their care are not accessible to persons to whom they are not destined.

Each employee is required to ensure the protection of the data and tools used by the company; access to the common network, emails, trading platforms (PrimeTrade, Bloomberg, etc.) and Orchestrade must be limited to authorised users. All employees are bound to lock their computers (⊞ + L) when they are absent from their workstation. The passwords must be regularly changed, they must not, under any circumstances, be passed on to others and must not be left in full view, or in an easily accessible place, when they are noted on a physical medium.

At the end of the working day employees must, before leaving, tidy up their offices and lock away confidential documents and objects of value, notably phones and portable computers.

When circumstances justify this, notably in the case of thefts or repeated disappearance of objects or material belonging to the firm, the Management shall, with the consent of the interested parties, check what employees are taking out of the premises. In the case of refusal, the Management shall have this check carried out by the officer of the competent criminal investigation department.

In the same circumstances, the firm shall check the content of employees' offices and cupboards in their presence or absence with their agreement. In the absence of an employee or the impossibility of obtaining the latter's agreement, this check shall take place in the presence of two people part of the firm. In this specific case, a formal report shall be drawn up and signed by these two people.

2.6. Correspondence

It is prohibited for employees to have the EIG bear the costs of their personal correspondence.

Personal communication via phone, fax, telex or any other means of telecommunication, notably email, may be received or given during working hours in conditions that do not negatively impact the normal performance of the employment contract and the proper professional use of these means of telecommunication.

2.7. Transport of objects

Employees may not remove and use outside the offices objects or equipment belonging to the firm without the authorisation of their line manager.

2.8. Relations with clients

In their contacts with clients, employees undertake:

- To only use documents issued by the firm,
- Not to accept from a client of the portfolio management company any payment in cash or other means of payment for their own personal benefit, except when exceptional circumstances justify this and the line manager has been informed.
- Not to accept from a client of the portfolio management company any personal contract of agency or power of attorney of any type whatsoever, except in the case of family link or in conditions expressly authorised by Management,

- To scrupulously use the computer applications taking care, in compliance with the data protection law n° 78-17 of 6 January 1978, not to record any unfounded indication, judgement of value or data of a personal nature revealing racial or ethnic origins, political opinions or such like, religious convictions or such like, or any information relating to health, sexuality or criminal record.

2.9. Prevention of sexual harassment

No employee, no candidate for a job, a placement or a period of in-company training may be penalised, dismissed or subject to a direct or indirect discriminating measure, notably in the field of remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract for having refused to be subject to the harassment of any person whose aim is to obtain sexual favours for their own benefit or that of a third party.

No employee may be penalised, dismissed or undergo a discriminatory measure for having been witness to the behaviour defined in the previous paragraph or having testified to such behaviour.

Any employee whose behaviour can be described as sexual harassment will be subject to a disciplinary measure specified in these regulations.

2.10. Prevention of moral harassment

No employee should undergo repeated moral harassment with the purpose or effect of deteriorating working conditions and negatively impacting the employee's rights and dignity, damaging their physical or mental health, or compromising their professional future.

No employee may be penalised, dismissed or be subject to a direct or indirect discriminatory measure, notably in the field of remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract for having undergone or refused to undergo the behaviour defined in the previous paragraph or for having witnessed or testified to such behaviour.

Any employee whose behaviour can be described as moral harassment will be subject to a disciplinary measure specified in these regulations.

2.11. Prevention of all discriminatory measures

No person may be refused access to a recruitment procedure, a placement or an in-house training period, no employee may be penalised, dismissed or be subject to any direct or indirect discriminatory measure, notably in the field of remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract due to their origin, sex, customs, sexual orientation, age, family situations, belonging or not belonging, effectively or supposedly, to an ethnical group, nation or race, their political opinions, mutualist or trade union

activities, religious convictions, physical appearance, name, or, unless inaptitude recorded by the occupational doctor, due to the person's state of health or handicap.

No employee may be penalised, dismissed or be subject to a discriminatory measure for having witnessed the behaviour defined in the previous paragraph or having testified to it.

Any employee who has had a discriminatory attitude is liable to a disciplinary measure specified in these regulations.

3. DEONTOLOGY

These regulations aim to ensure that any person carrying out work under the authority or on behalf of the management company Eiffel Investment Group SAS, whether or not the person is bound by an employment contract with the latter and wherever the person may be, in the premises of the Company at 4, rue Euler – – 75008 Paris or outside these, respects the following when performing their tasks:

- the professional obligations of the Company as they result from the provisions of articles L. 533-11 and following of the Monetary and Financial Code, the General Regulations of the Stock Market Authority (SMA): and
- the personal obligations that are applicable to the Employees pursuant to these same provisions.

The following provisions are applicable to the following persons:

- employees of the Eiffel Investment Group SAS,
- consultants, trainees and employees of other companies part of the Group, employees of service provider companies or any natural person placed at disposal or seconded,
- consultants, trainees or temporary workers with an assignment or function within Eiffel Investment Group SAS.

When a member of the Company, in the context of their professional activity, and taking into account their competence and level of knowledge, and for a sound reason, has doubts as to whether a transaction that they are performing respects the following principles:

- does not harm the Company's reputation and does not negatively affect it,
- respects the legal, regulatory, professional and deontological obligations and procedures,
- respects the integrity of the markets,
- respects investors' interests

they must consult their line manager or the Compliance Officer. Moreover, if a member of staff considers for a sound reason that a transaction of which they have knowledge does not respect the principles set out above, they must consult the Company's Compliance Officer. The employee may request the Compliance Officer to treat the query as confidential.

No member of the Company may be penalised, dismissed or be subject to direct or indirect unacceptable measures, whatever the type, for having taken the steps set out in this article.

3.1. Respect of professional secrecy and confidentiality

All staff are bound to strictly respect professional secrecy in the conditions and under threat of the penalties specified by law. All staff are therefore bound by a general duty of confidentiality in respect to information concerning investors, and the functioning of the Group and its subsidiaries.

Within the Company, employees who, in the exercise of their duties, must have excess to confidential and/or privileged information are bound to an obligations of discretion in respect to the other employees and more generally all third parties.

The following teams/departments are differentiated within EIG:

- investment teams (Portfolio Managers and analysts),
- risk-operations team and
- development-marketing department.

These teams/departments must be located on materially different and separated desks in order to prevent the circulation of any sensitive information. Moreover, the employees must be informed and made aware of the consequences that the improper circulation of privileged information could have or the harm to one or more clients that could result.

3.2. Market integrity

The respect of market integrity excludes all acts by employees that could disrupt the normal functioning of the markets or make it possible to acquire an undue advantage for oneself or the Company at the expense of one or more other players.

Articles L. 465-1 to 465-3 of the Financial and Monetary Code and the provisions of Book VI of the General Regulations of the Financial Market Authority define the framework for French regulations relating to market abuse.

The breach of these provisions could have serious legal consequences, and lead to civil and/or criminal liability and disciplinary measures for the Company and/or its Employees. Any market abuse shall lead to criminal penalties (up to two years' imprisonment and a fine of 1,500,000 euros, which could be increased to ten times the amount of any profit made) and disciplinary measures (up to 1.5 million euros or ten times the profits made and a penalty that could even be barring from the exercise of the profession) for the employees and/or the Company.

In addition to these penalties, this type of behaviour may lead to a negative image for the employees involved and the Company, and /or the dismissal of the employee concerned and other disciplinary measures.

3.2.1. Scope of application of the provisions relating to market abuse

The provisions relating to market abuse are applicable:

- to any natural person or legal entity;
- to the financial instruments indicated in article L. 211-1 of the Financial and Monetary Code;
    - admitted to trading on a regulated market as this is defined in article L. 421-1 of the Financial and Monetary Code or for which a request for admission to such a market has been made; or
    - admitted to trading on an organised multilateral trading system provided for by article 525-1 of the General Regulations of the FMA; or
    - admitted to trading on a regulated market of another member state of the European Community or party to the agreement on the European Economic Area or for which a request for admission to such a market has been presented in the cases indicated in d) of article L.621-15 of the Financial and Monetary Code:
- to transactions concerning these instruments, regardless of whether or not they have been effectively performed on a regulated market or when they have taken place on an organised multilateral trading system.

The obligation to refrain also applies to financial instruments not admitted to trading on a regulated market or an organised multilateral system of trading, but whose value depends on a financial instrument admitted to trading on such a market or system.

3.2.2. Insider trading operations

Pursuant to article 621-1 of the General Regulations of the FMA "*privileged information is precise information that has not been made public, which directly or indirectly concerns one or more issuers of financial instruments, or one or more financial instruments, and which, if it were made public, could have a significant influence on the price of the relevant financial instruments or the price of financial instruments linked to them.*

Information is deemed precise if it mentions a series of circumstances, or an event which has occurred or is likely to occur and if it is possible to draw a conclusion as to the possible effect of these circumstances or this event on the price of the relevant financial instruments or the financial instruments linked to these.

Information which, if it were made public, could have a significant influence on the price of the relevant financial instruments or the price of derivatives that are linked to them is information that a reasonable investor would be likely to use as a basis for their investment decisions."

All Employees must refrain from using privileged information that they hold when buying or selling or attempting to buy or sell, on their own account or on behalf of others, directly or indirectly, the listed financial instruments concerned by this information or the listed financial instruments to which these instruments are linked.

They must also refrain from:

- communicating this information to another person outside the normal context of their work, profession or functions or for purposes other than those for which the information was received;
- recommending to another person to buy or sell, or to have bought or sold by another person, based on privileged information, the listed financial instruments to which this information relates or the listed financial instruments to which these instruments are linked.

The obligations to refrain set out above do not apply to transactions carried out to discharge an obligation, that has fallen due, to buy or sell financial instruments when this obligation results from an agreement concluded before the relevant person held privileged information.

Non-published information must be processed within the Company and within the relevant team in the Company, in such a way that it is not disseminated outside the Company and only circulates within the Company to other Employees, teams or departments of the Company authorised to have such information.

In the exercise of their activities, with the exception of certain situations to which the following paragraph refers, and specifically known to the ICCO and management (notably for issuers who have also investable debt securities), the Company's Employees are not supposed to be the recipients of such privileged information, as this is defined by article 621-1, 622-1 and 622-2 of the General Regulations of the FMA. If a Company Employee is led to receive information that they consider to be "privileged" information as this is defined in the FMA regulations, they must promptly notify their line manager and the ICCO and not use, for themselves or third parties, such information.

The Company may be led (through a fund or a client or any other means) to invest (or contemplate an investment) in non-listed instruments (for example, debt securities, private shares, etc.) In this case, it signs (or the relevant client signs) a specific non-disclosure agreement. The Company (or the relevant client) is then in a so-called "Private" situation. All the information thus acquired must be treated as strictly confidential. Its improper use could constitute a market abuse. Employees are bound to respect, both in a personal and professional capacity, all the obligations imposed on the Company by the non-disclosure agreement signed by the company (or the relevant client).

In the context of its research, the Company is led to consult experts to obtain information useful for making its investment decisions. Since these consultations present a high risk of occurrence of situations of conflicts of interest and exchange of privileged information, the following rules must be applied:

- the CCO is invited to the phone consultation (participation is not automatic);
- the CCO is informed of the agenda, the participants' names (employees and experts) and the access codes for the phone consultation;
- the CCO grants or refuses the authorisation for the phone consultation;

- At the start of each consultation, a participating employee reads out the following warning stemming from the contract that provides the framework for the relationship between the expert and the Company;
    1) It is prohibited for any specialist to reply to questions or take part in a consultation, firstly, if they are an employee/shareholder/service provider/contracting party of the company for which the research is undertaken or one of its subsidiaries.
    2) It is prohibited for any specialist to reply to questions or take part in a consultation, if the consultation may lead to the disclosure of inside information or non-public information concerning a listed company.
    3) EIG undertakes not to take part in any consultation with an employee/shareholder/representative/service/provider/contracting party of the company for which the research is conducted.
    4) EIG undertakes not to participate in any consultation with its direct rivals or any clients of its direct rivals.
    5) EIG undertakes not to request, from the specialist, information which could constitute inside information or non-public information concerning a listed company.

3.2.3. Market manipulations

All employees must refrain from manipulating prices. A price manipulation is:

- performing transactions or issuing orders:
    - which give or are likely to give false or misleading information on the offer, the demand or the price of financial instruments; or
    - which fix, by the action of one or more persons acting together, the price of one or more financial instrument at an abnormally high or artificial level, unless the person who has performed the transactions or issued the orders can establish the legitimacy of the reasons for these transactions or orders and their compliance with market practices accepted on the relevant regulated market.
- performing transactions or issuing orders which call on procedures giving a fictive image of the state of the market or any other form of deception or contrivance.

All employees must refrain from communicating or consciously disseminating information, on any medium whatsoever, which gives or could give inaccurate, imprecise or misleading information on financial instruments issued by public offering, including by spreading rumours or disseminating incorrect or misleading information whereas the person knew or should have known that the information was incorrect or misleading.

The dissemination of false information is notably the fact of issuing, on any medium whatsoever, an opinion on a financial instrument or indirectly on the issuer of the latter, after having taken positions on this financial instrument and benefiting from the situation that results, without having simultaneously made public, in an appropriate and efficient way, the conflict of interest existing.

3.2.4. Declaration of a market abuse

The Company is bound to promptly declare to the FMA any transaction on financial instruments admitted to trading on a regulated market, or for which application for admission to trading on such a market has been submitted, performed on own account or on behalf of a third party, for which there are reasons to suspect that it could constitute an inside trading transaction or a manipulation of prices as defined in the general regulations of the FMA.

EIG is equipped with an identification and declaration procedure for a suspicious transaction making it possible:

- to detect and identify, notably by using a typology of suspicious transactions, those that must prompt a notification.
- to explain the measures and actions to be taken to make a declaration,
- to inform employees of their responsibilities and legal obligations as regards the identification and declaration of suspicious transactions.

This procedure may be consulted by all employees.

3.3. Personal transactions on financial instruments

Articles L. 533-10 2° of the Financial and Monetary Code and 313-9 to 313-12 of the General Regulations of the FMA require the Company to put in place a system for defining the conditions and limits in which employees may perform personal transactions on own account.

The purpose of this system is to prevent prohibited personal transactions from being performed directly or through an intermediary, that is to say transactions that constitute a market abuse, notably based on the use of confidential information, or proving incompatible with professional obligations notably in terms of conflicts of interest of the Company as defined by laws, regulations and professional rules approved by the FMA.

In order to prevent the occurrence of such transactions, the Company is bound to notify the relevant persons of prohibited personal transactions and the system to be respected. Moreover, the Company shall be able to request information relating to personal transactions performed by the relevant persons.

3.3.1. Scope of application

In compliance with articles 313-2, 313-9 and 313-10 of the General Regulations of the FMA, relating to the category of “relevant persons”:

- executive officers;
- salaried employees;
- non-salaried employees (service providers, etc.), and
- trainees.

Among these people, only those in one of the following situations are concerned by the procedures defined in this Article:

- they act in the context of activities that could lead to conflicts of interest;
- they have access to privileged information as this is defined in Book VI of the General Regulations of the MFA; or
- they have access to other confidential information relating to clients or transactions concluded with and for the client.

Nonetheless, in the case of Eiffel Investment Group SAS it was decided that all staff would be entered on the list of so-called "exposed" persons with the highest level of exposure; the system for monitoring personal transactions therefore applies to all and in the same proportions.

Even though the CCO is a so-called "exposed" person, it is decided that the CCO does not Personal Account trade.

The transactions targeted by this system are those performed by a relevant person and when at least one of the following conditions is fulfilled:

- the relevant person is acting outside the context of their functions;
- the transaction is performed for one of the following persons:
    - the relevant person on own account,
    - a person with whom the aforesaid has family links ([1]) or close links ([2]),
    - a person whose link with the relevant person is such that the latter has a major direct or indirect interest in the result of the transaction, other than the costs and commission for performing it.

3.3.2. System for supervising personal transactions and exemptions

Before any personal transaction, the employees are bound to notify the CCO in writing. In reply to the notification, the CCO issues a favourable or unfavourable recommendation. When the transaction has been performed, the employee must send the confirmation containing the characteristics of the latter to the CCO. The CCO makes the entry in the personal transactions register.

More precisely, for a favourable recommendation granted by the CCO, the conditions are as follows:

- The favourable opinion is valid 48h, that is to say that the order must be placed within this period. However, this may be adapted on a case-by-case basis, for instance be extended if the CCO considers that there is no risk of conflict of interest.
- When the order has been placed by the employee, the latter is duty-bound to retain the position taken for at least 60 days. This obligation may be adapted on a case-by-case basis, notably if the CCO considers that there is no risk of conflicts of interest.

This provision does not apply to personal transactions performed in the framework of a discretionary portfolio management service contract without any prior instruction concerning the transaction between the Company and the relevant person or another person for whom the transaction is performed.

Moreover, personal transactions concerning UCITS harmonised units or shares are not subject to this provision insofar as the relevant person or the person for whom the transactions are performed is not involved in the management of these UCITS.

3.3.3. Prohibited personal transactions

Prohibited personal transactions are:

- transactions carried out in breach of the provisions of Book VI of the General Regulations of the FMA.
- transactions incompatible with the Company's professional obligations. The prohibition targets in particular the use by an Employee, outside the framework of their functions, privileged information relating to financial instruments, the said information received when performing the employment contract or in the workplace.

The following are generally prohibited:

- Transactions implying a financial instrument (single name) in which a fund managed or advised by the Company (or a client through a contract of agency entrusted to the company, or a client following advice from the company, etc.) is invested or contemplates investing

- The investments involving the financial instrument of an issuer concerning which the Company is conducting research with a view to a possible investment.

All issuers/instruments on which transactions are prohibited appear in the restricted list updated and circulated every week by the CCO.

The prohibitions appearing in this paragraph also apply to advising and assisting any person with a view to performing a transaction that would breach these same obligations. In the case of doubt, the relevant employee may consult the CCO at any time.

3.3.4. System for checking personal transactions

Twice a year, the CCO collects the securities account statements from a sample of employees in order to compare these with the register of personal transactions.

Once a year, the CCO asks employees to certify that they are in compliance with the system for supervising personal transactions.

3.4. Identification of the various entities and measures of material separation:

The following departments are differentiated within EIG:

- the investment teams (Portfolio Managers and analysts).
- the risk-operations team and
- the development-marketing team.

Although they may be located in the same open space, these teams must have desks that are materially distinct and separated. Moreover, the staff are informed and made aware at the time of the annual training by the ICCO of the possible consequences of the improper dissemination of privileged information and they must therefore refrain from passing such information on to other teams or departments, or any third party whatsoever.

3.5. Conflicts of interest and priority of the clients' interests

As regards conflicts of interest, employees are bound to refer to the policy for managing conflicts of interest drawn up by the Company.

3.6. Communication with clients

3.6.1. Complaints

In the event that an existing or potential client or an employee detects an anomaly, the Company has put in place a "complaint handling" procedure; this procedure explains the measures to be taken when such an event occurs, explaining in detail the role of each player in each stage of the procedure.

It is the head of development who is designated as the person in charge of receiving external complaints; it is also the latter who will inform the person who made the declaration of the result. This is why the EIG website clearly provides full particulars of the person to be contacted and this information may be accessed by any existing or potential investor. This person has ten working days as of receipt of the complaint to acknowledge receipt and two months as of the date of receipt to send the reply to the client.

Each complaint is processed by the relevant team. At the same time, throughout the procedure, the ICCO inputs the information provided by the head of development into the incident database.

For Eiffel UCITS Opportunities SICAV the specific measures contained in the "Complaint Handling Procedure" must also be applied.

3.7. The Company's participation in the prevention of money laundering and the financing of terrorism

It is recalled that the Company is bound in the conditions fixed by articles L. 561-1 and following of the Financial and Monetary Code to declare to the TRACFIN department any transaction that appears to stem from an offence punishable by a prison sentence of more than one year or contributing to the financing of terrorism, or that could stem from a tax fraud corresponding to certain regulatory criteria, and any transaction for which the identity of the instructing party or the effective beneficiary is doubtful despite the Company's verification procedures,

Likewise, the Company must declare to the TRACFIN department the transactions that could be carried out for entities acting in the form or on behalf of trust funds or any other instrument for managing special purpose funds for which the identity of the settlors or beneficiaries is not known.

Consequently, each Employee must respect all the provisions on the prevention of money laundering and the financing of terrorism, and the indications on the type of transactions for which particular vigilance is required. In this respect, Employees' attention must focus more particularly on any particularly complex transaction or for an unusually high amount or not appearing to have any economic justification or legal purpose.

Each Employee is prohibited from making known to the person at the origin of the transactions for which a declaration was made to the TRACFIN department, the existence of the declaration of suspicions and from providing information on the penalties to be incurred.

In the case of a suspicion, each Employee must notify the TRACFIN correspondent of the characteristics of the transaction indicating the date by which it should be performed, the documents concerning the transaction that should lead to a declaration to the TRACFIN department. In the case of urgency, the Employee must provide this information and documents to a member of Management who is involved in the Company's internal control, even if the latter is not normally authorised to deal with such matters, so that the declaration of suspicions to TRACFIN can be made promptly.

The employees may also consult the Company's manual on the prevention of money laundering.

4. RULES RELATING TO THE PROPER USE OF IT EQUIPMENT

EIG's IT resources placed at the disposal of the Company's employees is essential for the proper functioning and the development of the firm, its trades and its functions. They help it achieve its performance and ensure its continued existence, and are part of the Group's assets. In this respect any information of a professional nature issued, received or stored on the workstation, and all IT resources are and remain the firm's property.

The use of the IT equipment must comply with the law and the firm's rules of deontology, and must also respect clients' and the firm's security.

By its activity, EIG is bound to professional secrecy and has the obligation to protect the confidentiality and integrity of the IT data relating to its clients.

These provisions are intended to protect the interests of the Company, its customers and its employees. They specify the rules and precautions that any users of the SGP IT resources must respect.

4.1. Scope of application

These rules apply to any user of EIG IT resources.

The term user refers to any EIG salaried employee or any person placed at the disposal of EIG by an external company, regardless of whether or not it is a member of the Group, including temporary workers, using the IT resources placed at disposal within and for EIG.

The expression IT resources refers to all IT resources, communication networks and information system: fixed or portable hardware, software, internal and external communication systems, information and data – whatever their medium – made available to users by the firm.

“Means of access” refers to any means allowing the use of the IT resources by a user (ID, password, etc.)

4.2. Use of EIG IT resources

Users must make proper use of the IT resources when used for professional or personal purposes inside or outside the firm. This use must not negatively impact the normal performance of their employment contracts or assignments, or the interests of the firm, its clients or its employees. Users undertakes to respect these rules:

Users are prohibited from modifying the IT resources placed at their disposal, notably by adding hardware or software that was not supplied or authorised by the firm’s competent technical departments. They undertake to only use the programs authorised by the said departments.

Users undertake not to make copies of the software placed at their disposal apart from backups for the needs of the department.

In all circumstances, wherever they may be, users must ensure the proper protection of the IT resources placed at disposal and the data that they contain on their means of access.

Users must not seek to circumvent security procedures and mechanisms implemented by the firm (antivirus, coding, back-up, signature, password, etc.). Users must in particular:

- use the means of authentication that must not be communicated,
- must never lend their ID or password to third parties
- must not use or attempt to use other users’ means of access,
- must not leave their workstation with a current work session accessible.

Users all contribute at their level to the general security of the Company's IT tools; they must notify any malfunctioning or any incident that appears abnormal. They put into application the rules and recommendations established by the IT system administrators and the firm’s competent technical departments.

4.3. Email

These rules do not affect those concerning the use of IT resources by SGP staff representatives in the context of the exercise of their tasks linked to this and resulting from specific provisions.

Email is part of the firm's IT resources and therefore its use must comply with the rules set out above. It is paramount that the interests of SGP, its employees or its clients are not negatively impacted by any email sent.

The user must refrain from any dissemination of confidential information concerning clients, the Group's strategy, a trade and the staff of the Company's partners, except when this dissemination is required in the context of its work relations.

The user is prohibited from activities, using email that could harm the reputation or image of Eiffel Investment Group, its clients or its employees. It is also prohibited to send, within the firm, messages of a pornographic, paedophile, xenophobic nature or inciting violence or racial hatred.

4.4. Internet

The websites are accessible to all users, unless special prohibition justified in writing by a line manager. The user is prohibited from accessing sites of a pornographic, paedophile, xenophobic nature or inciting violence or racial hatred.

Since the Internet is not a secure network for consulting public or private sites, or for sending or receiving email via a messaging service, the integrity of information sent by email cannot be guaranteed. As a result, messages transiting by the Internet may, at any time, be intercepted, viewed, recorded and used for other purposes by third parties. Moreover, all the user's activities and the data concerning the aforesaid (sites visited, messages sent and received, information provided on forms, data collected without the user knowing, etc.) may be recorded by third parties, analysed to deduce the user's centres of interest, the firm's concerns, etc. and used for commercial or other purposes. Internet users must therefore use this vehicle for communication wisely, under their own responsibility, and take all necessary precautions. Since each website may be subject to rules of law other than those of French law, the user must take all precautions in this respect.

5. SCALE OF PENALTIES AND EMPLOYEES' RIGHT TO PUT FORWARD THEIR CASE

5.1. Penalties

Any breach of the provisions of these rules of procedure and any action or failure deemed a fault by the employer may lead, in the respect of the provisions of laws and regulation, notably in matters of prior discussion, to one of the following disciplinary penalties being applied:

- Written warning
- Reprimand
- Demotion implying a change in post

- Dismissal for disciplinary reason

5.2. Precautionary measures

In serious cases which require a prompt provisional solution, the employer may order a precautionary suspension of the employee with or without remuneration; the suspension of the remuneration which may accompany this suspension may not be for more than one month. At the end of the suspension, the unpaid remuneration must be paid unless the employee is dismissed for gross misconduct or serious negligence.