

NOTE
to the
Managerial and administrative Model
as per legislative decree no. 231 of June 8, 2001

The Board of Directors of Weather Investments S.p.A., with the resolution of April 7, 2008, has amended the General Section of the Model (par.2.3, 3° point; par. 2.4, letter a); par. 2.6) in order to delegate to the single companies of Weather Group the definition and updating of the specific Special Sections coherently with their business, without prejudice the exclusive competence of Weather Investments S.p.A. regarding the update and integration of the General Section.

Therefore, the following Wind Model 231/01 is composed by a General Section, in charge to the holding, and the Special Section (from A to I) regards exclusively the WIND's organisational structure (approved by Wind Board of Directors with the resolution of the February 20, 2008 and subsequent resolutions).

Moreover, it is pointed out that the Wind Compliance Officer (Internal Control Organ) is the Internal Auditing Director of Wind Telecomunicazioni S.p.a. (confirmed by Wind Board of Directors with the resolution of the October 10, 2005).



Managerial and administrative Model as per legislative decree no. 231 of June 8, 2001

Updated by Weather Investments S.p.A. Board of Directors the April 7, 2008 – General Section
Updated by Wind Telecomunicazioni S.p.A. Board of Directors the March 2, 2009 and subsequent
resolutions – Special Sections

INDEX

1. LEGISLATIVE DECREE NO 231/2001	6
1.1 THE ADMINISTRATIVE RESPONSIBILITY REGIME FOR CORPORATE BODIES, COMPANIES AND ASSOCIATIONS	6
1.2 THE ADOPTION OF THE “MANAGERIAL AND ADMINISTRATIVE MODEL” AS A POSSIBILITY TO AVOID ADMINISTRATIVE RESPONSIBILITY	7
2. ADOPTION OF THE MODEL BY WEATHER	7
2.1 OBJECTIVES PURSUED BY THE GROUP BY ADOPTING THE MODEL	7
2.2 FUNCTION OF THE MODEL	8
2.3 STRUCTURE OF THE MODEL: GENERAL SECTION AND SPECIAL SECTIONS ON THE BASIS OF DIFFERENT OFFENCES	8
2.4 ADOPTION OF THE MODEL WITHIN THE GROUP	8
2.5 APPROVAL OF THE MODEL AND ITS ADOPTION WITHIN THE GROUP	9
2.6 CHANGES AND INTEGRATION TO THE MODEL	9
2.7 APPLICATION OF THE MODEL BY THE INDIVIDUAL COMPANIES AND THEIR IMPLEMENTATION OF THE CHECKS ON THE AT-RISK ACTIVITY AREAS	9
2.8 CO-ORDINATION ON THE CONTROL AND VERIFICATION SYSTEMS ON GENERAL MODEL EFFECTIVENESS	9
3. INTERNAL CONTROL ORGAN (CO)	10
3.1 IDENTIFICATION OF THE INTERNAL CONTROL ORGAN	10
3.2 FUNCTIONS AND POWERS OF THE INTERNAL CONTROL ORGAN (CO)	10
3.3 FUNCTIONS OF THE CO: REPORTING TO THE CORPORATE BODIES	11
3.4 CO-ORDINATION FUNCTIONS OF WEATHER INVESTMENTS S.P.A. WITH THE COs OF THE OTHER GROUP COMPANIES	11
4. SELECTION, TRAINING AND REPORTING	11
4.1 PERSONNEL SELECTION	11
4.2 PERSONNEL TRAINING	11
4.3 SELECTION OF FREELANCERS AND PARTNERS	12
4.4 INFORMATIVE REPORT TO FREELANCERS AND PARTNERS	12
5. INFORMATION FLOWS TO THE CO	12
5.1 NOTICES BY COMPANY REPRESENTATIVES OR BY THIRD PARTIES	12
5.2 INFORMATION OBLIGATIONS RELATING TO OFFICIAL ACTS	12
5.3 PROXY SYSTEM	13
6. DISCIPLINARY SYSTEM	13
6.1 GENERAL PRINCIPLES	13
6.2 SANCTIONS FOR EMPLOYEES	13
6.3 MEASURES AGAINST MANAGERS	13
7. OTHER PROTECTION MEASURES IN THE EVENT OF NON COMPLIANCE WITH MODEL RULES	13
7.1 MEASURES AGAINST DIRECTORS	13
7.2 MEASURES AGAINST FREELANCERS AND PARTNERS	14
8. PERIODICAL CHECKS	14
9. MODEL AND CODE OF ETHICS	14
SPECIAL SECTION A	
A.1 TYPES OF OFFENCES IN THE RELATIONSHIPS WITH THE PUBLIC ADMINISTRATION (ARTICLES 24 AND 25 OF THE DECREE)	15
A.2 AREAS AT RISK	16
A.3 GENERAL REFERENCE PRINCIPLES	17
A.4 RECIPIENTS OF THE SPECIAL SECTION: GENERAL BEHAVIOURAL PRINCIPLES AND IMPLEMENTATION	18
A.5 ACTIVITY AREAS AT RISK: APPOINTMENT OF THE INTERNAL RESPONSIBLE	19

INDEX

A.6	THE CONTROL SYSTEM.....	20
A.7	INSTRUCTIONS AND VERIFICATION BY CO.....	21
B.1	THE TYPES OF CORPORATE OFFENCES (ARTICLE 25-TER OF THE DECREE).....	23
SPECIAL SECTION B		
B.2	AREAS AT RISK.....	26
B.3	RECIPIENTS OF THE SPECIAL PART: GENERAL BEHAVIOURAL PRINCIPLES AND IMPLEMENTATION.....	26
B.4	ACTIVITY AREAS AT RISK: APPOINTMENT OF THE INTERNAL RESPONSIBLE.....	28
B.5	CONTROL SYSTEM.....	28
B.6	INSTRUCTIONS AND VERIFICATION BY CO.....	32
SPECIAL SECTION C		
C.1	TYPES OF CRIMES OF TERRORISM AND SUBVERSION OF DEMOCRATIC ORDER.....	33
C.2	AREAS OF RISK.....	33
C.3	RECIPIENTS OF THE SPECIAL SECTION: GENERAL PRINCIPLES OF CONDUCT AND PERFORMANCE.....	34
C.4	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.....	35
C.5	THE CONTROL SYSTEMS.....	35
C.6	INSTRUCTIONS AND VERIFICATION OF THE CO.....	36
SPECIAL SECTION D		
D.1	TYPES OF CRIMES AGAINST INDIVIDUALS.....	37
D.2	AREAS OF RISK.....	38
D.3	RECIPIENTS OF THE SPECIAL SECTION: GENERAL PRINCIPLES OF CONDUCT AND PERFORMANCE.....	38
D.4	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.....	39
D.5	THE CONTROL SYSTEMS.....	39
D.6	INSTRUCTIONS AND VERIFICATION OF THE CO.....	40
SPECIAL SECTION E		
E.1	THE TYPES OF MARKET ABUSE CRIMES.....	41
E.2	RISK AREAS.....	42
E.3	SPECIAL SECTION RECIPIENTS: GENERAL PRINCIPLES OF BEHAVIOUR AND IMPLEMENTATION.....	42
E.4	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.....	43
E.5	THE CONTROL SYSTEMS.....	43
E.6	INSTRUCTIONS AND VERIFICATION OF THE CO.....	44
SPECIAL SECTION F		
F.1	THE TYPES OF CRIMES IN VIOLATION OF ACCIDENT PREVENTION RULES AND THE PROTECTION OF HEALTH AND HYGIENE IN THE WORK PLACE ARE LISTED BELOW:.....	45
F.2	RISK AREAS.....	46
F.3	SPECIAL SECTION RECIPIENTS: GENERAL PRINCIPLES OF BEHAVIOUR AND IMPLEMENTATION.....	46

INDEX

F.4	ACTIVITIES AREA AT RISK: APPOINTING THE INTERNAL PERSON IN CHARGE.	46
F.5	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.	46
F.6	THE CONTROL SYSTEMS	47
F.7	INSTRUCTIONS AND VERIFICATION OF THE CO.	47
SPECIAL SECTION G		
G.1	TYPES OF OFFENCES IN RECEIVING, LAUNDERING AND USING MONEY, GOODS OR BENEFITS OF ILLICIT ORIGIN	49
G.2	AREAS AT RISK	49
G.3	RECIPIENTS OF THE SPECIAL SECTION: GENERAL BEHAVIORAL PRINCIPLES AND IMPLEMENTATION	50
G.4	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.	51
G.5	THE CONTROL SYSTEMS	51
G.6	INSTRUCTIONS AND VERIFICATION OF THE CO.	52
SPECIAL SECTION H		
H.1	TYPES OF TRANSNATIONAL OFFENCES	53
H.2	AREAS AT RISK	54
H.3	RECIPIENTS OF THE SPECIAL SECTION: GENERAL BEHAVIORAL PRINCIPLES AND IMPLEMENTATION	54
H.4	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.	55
H.5	THE CONTROL SYSTEMS	55
H.6	INSTRUCTIONS AND VERIFICATION OF THE CO.	56
SPECIAL SECTION I		
I.1	COMPUTER CRIMES TYPOLOGY	57
I.2	RISK AREAS	58
I.3	RECIPIENTS OF THE SPECIAL SECTION: GENERAL BEHAVIORAL PRINCIPLES AND IMPLEMENTATION	58
I.4	ACTIVITY AREAS AT RISK: APPOINTING THE INTERNAL RESPONSIBLE.	59
I.5	CONTROL PROTOCOLS	59
I.6	INSTRUCTIONS AND VERIFICATION OF THE CO.	61

1. Legislative Decree No 231/2001

1.1 The administrative responsibility regime for corporate bodies, companies and associations

To enforce the delegated law as per Article 11 of Italian Law No. 300 of 29 September 2000, on 8 June 2001 Legislative decree No. 231 (hereunder the "Decree") was passed, which became effective on 4 July 2001. The Decree aims at bringing in line the Italian regulations in the area of corporate-body responsibility with some international agreements Italy has already signed, such as the *Brussels Convention of 26 July 1995* on the protection of European Community financial interests, the *Convention also signed in Brussels on 26 May 1997* on the battle against corruption, which has seen several officers of the EC or the member states involved, the *OECD Convention of 17 December 1997* on the battle against corruption of foreign public officers in economic and international operations.

This Decree, entitled "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (Discipline of the administrative responsibility of corporate bodies, companies and associations also of those not having a legal status) has introduced into the Italian law a regime of administrative responsibility (which broadly regards a criminal responsibility) for various bodies (companies, consortia etc., hereunder the "Bodies") for certain offences committed, in their interest or to their own advantage, (i) by individual persons having a representative, administrative or managerial position within the Bodies or within a business unit linked to them, albeit independent from a financial and functional viewpoint, as well as by individual persons who, also *de facto*, manage and control the Bodies, as well as (ii) by individual persons subject to the management or supervision by one of the subjects mentioned above. This responsibility is added to that of the individual person who has materially committed the offence.

The broadening of the responsibility aims at punishing - for certain criminal offences - also those Bodies that have benefited from the offence. The more serious of the fines provided for include various types of disqualification such as the suspension or withdrawal of licences and permissions, the prohibition from signing agreements with the Public Administration, the debarment from performing certain activities, the barring from or withdrawal of financings and contributions, and the prohibition from advertising goods and services. The responsibility provided for by the above mentioned Decree also relates to criminal offences committed outside Italy if the foreign country where the offence was committed does not take steps against them.

As to the type of offences coming within the above mentioned regime of administrative responsibility for the Bodies, in its original form the Decree refers to a series of offences perpetrated in the relationships with the Public Administration, more precisely:

- ✓ undue cashment of contributions, financings or other financial disbursements from the State or other public bodies (Art. 316-ter of the Italian penal code),
- ✓ fraud against the State or other public body (Art. 640, subsection 1, no. 1 of the Italian penal code),
- ✓ serious fraud to receive public funds (Art. 640-bis of the Italian penal code),
- ✓ fraud against the State or other public body (Art. 640-ter of the Italian penal code),
- ✓ corruption for official acts (Art. 318 of the Italian penal code),
- ✓ corruption in acts against official duties (Art. 319 of the Italian penal code),
- ✓ corruption in judicial acts (Art. 319-ter of the Italian penal code),
- ✓ inducement to corruption (Art. 322 of the Italian penal code),
- ✓ extortion (Art. 317 of the Italian penal code),
- ✓ embezzlement against the State or other public bodies (Art. 316-bis Italian penal code).

Afterwards, the regime of administrative responsibility for the Bodies has been extended to the following type of offences:

- ✓ offences relating to "forged coinage/notes, public credit cards and duty stamps", introduced by the art. 6 of Italian Law no. 409 of 23 November 2001, containing "Urgent provisions in view of the introduction of the Euro"
- ✓ corporate offenses, introduced by art. 3 of legislative decree no. 61 of 11 April 2002 within the scope of the new reform of the company law
- ✓ crimes of terrorism or crimes of democratic order eversion, introduced by art. 3 of Italian Law no. 7 of 14 January 2003, containing the ratification and execution of the International Convention for the suppression of the financing of terrorism ratified at New York the 9 December 1999
- ✓ crimes against individual personality, introduced by art. 5 of Italian Law no. 228 of 11 August 2003 containing measures against trafficking in persons
- ✓ crimes of market abuse, introduced by the Italian Law no. 62 of 18 April 2005 European Community Law 2004
- ✓ crime of feminine genital mutilation, introduced by art. 8 of Italian Law no. 7 of 9 January 2006

1.2 The adoption of the “Managerial and Administrative Model” as a possibility to avoid administrative responsibility

By introducing the above mentioned administrative responsibility regime, Article 6 of the Decree makes provision, however, for a specific form of exemption from said responsibility if the body proves that:

- a) prior to the offence being committed, the Board of Directors of the Body adopted -and effectively implemented -managerial and administrative models that were suitable for preventing offences of the same type as that/those perpetrated;
- b) the task of supervising the operations and ascertaining that the models were complied with - as well as of taking care of their updating - was entrusted to a compliance officer of the Body having independent powers of initiative and control;
- c) the persons who committed the offence have acted by fraudulently avoiding the above mentioned managerial and administrative models;
- d) the body indicated under letter b) above performed its supervisory task and did so in a non-insufficient manner.

The Decree furthermore makes provision that - with regard to the extension of the delegated powers and the risk of committing the offences - the models as per letter a), must meet the following requirements:

- 1) identify the activities wherein it is possible that the offences dealt with by the Decree are committed;
- 2) make provision for specific protocols aimed at planning decision making and related implementation by the body with regard to the offences to prevent;
- 3) identify management procedures of the financial resources suitable for stopping these offences from being committed;
- 4) make provision for information obligations for the committee delegated to supervise the operations and the compliance with the model;
- 5) introduce an internal disciplinary system to punish non-compliance with the measures indicated in the model.

The Decree itself makes provision that the managerial and administrative models may be adopted, thus guaranteeing the requirements mentioned above, on the basis of behavioural codes prepared by category associations, sent to the Ministry of Justice that, together with the competent Ministries, can express, within 30 days, remarks on the suitability of the models aimed at offence prevention.

Provision is also made that, in small-sized Bodies, supervision may be performed directly by the Board of Directors.

2. Adoption of the Model by Weather

2.1 Objectives pursued by the Group by adopting the Model

Weather - being sensitive to the need to guarantee conditions of professionalism and transparency in conducting its business activity, in order to protect Weather's position and the image and of its subsidiaries, as well as the expectations of its shareholders and employees - has deemed it to be in keeping with its own corporate policies to implement the managerial and administrative model provided for by Legislative Decree 231/2001 (hereunder the “Model”) within the Weather Group (hereunder the “Group”, which is made up of Weather Investments S.p.A. and its subsidiaries as per Article 2359, sub-sections 1 and 2 of the Italian Civil Code).

This initiative has been taken on in the firm belief that the adoption of this Model - irrespective of the provisions of the Decree that indicate the Model as an optional non-compulsory element -may constitute a valid awareness-enhancement tool for all those operating in the name and on behalf of Weather, so that they may behave in a professional and clear way while performing their activities, thus avoid the risk of offences envisaged in the Decree being committed. The above mentioned Model has been prepared by Weather taking account - in addition to the prescriptions of Legislative Decree 231/2001 - of the guidelines prepared in this field by trade associations and the vast US experience in drafting models to prevent criminal offences, of the US best practice and the Federal Sentencing Guidelines issued on 1st November 1991. This Model with the General Section and the Special Section A (regarding offences perpetrated in the relationships with the Public Administration) the Special Section B (regarding corporate offences), was adopted by the Board of Directors with resolution of 19 July 2006. Also to implement the provisions contained in the Decree, the Board of Directors, upon passing the above mentioned Model, has entrusted the Person in Charge of with the task of taking on the function of internal control body (*Compliance Officer - CO*), with the task of ascertaining that the Model works well and effectively, that it is complied with, and to supervise its updating.

2.2 Function of the Model

The Model aims at building a structured and organic system for both procedures and control activities, to be carried out also pre-emptively (*ex ante* control), to prevent different types of offences envisaged by the Decree. In particular, by identifying the “at-risk activity areas” and their consequent procedure definition, the Model aims at:

- ✓ creating, in all those who operate on behalf of Weather in the “at-risk activity areas”, the awareness as to the possibility to commit, should the provisions contained therein be infringed, an offence that is liable to both economic and penal sanctions, not only for themselves but also for the company;
- ✓ confirming that such illegal behaviours are strongly condemned by Weather in that (even if the Company appeared to benefit from them) are nevertheless against not only the legal provisions but also the ethical and social principles the Group intends to strictly adhere to in pursuing its corporate mission;
- ✓ allowing the Company, through monitoring the “at-risk activity areas” to intervene in a timely manner to prevent or oppose the such offences.

In addition to the aforementioned principles, the key points of the Model are:

- ✓ awareness-enhancement initiatives and spreading of the behavioural rules and the procedures set up at all company levels;
- ✓ map of the Company's “at-risk activity areas”, that is to say of those activities within which offences are more likely to be committed;
- ✓ assignment to the CO of specific supervisory responsibilities for Model efficiency and correct operation;
- ✓ checking and reporting of at-risk operations;
- ✓ observance of the function-separation principle;
- ✓ definition of empowerment in keeping with the delegated responsibilities;
- ✓ checking of company behaviours and the operations of the Model, with consequent periodical updating (*ex post* control).

2.3 Structure of the Model: General Section and Special Sections on the basis of different offences

The present Model is made up of a “General Section” and individual “Special Sections” which have been prepared for the different types of offence considered by Decree 231/2001.

The first Special Section - called Special Section “A” - can be applied to specific types of offences as provided for under Articles 24 and 25 of the Decree, i.e. for the offences that can be committed against the Public Administration. The second Special Section - called Special Section “B” - can be applied to specific types of offences as provided for under Article 25-ter of the Decree, i.e. corporate offences.

The Boards of Directors of the different Group companies are entrusted with integrating this Model at a later stage, by way of an *ad hoc* resolutions, with further Special Sections relating to other types of offences that, for the effect of other regulations, can be included or somehow connected to the scope of application of Decree 231.

2.4 Adoption of the Model within the Group

The adoption of the Model within the Group is implemented according to the following criteria:

a) Preparation and updating of the Model

The Parent company is assigned the task of preparing and passing the Model that will be later adopted also by the other companies of Group with regard to at-risk activities they perform, by applying the formalities stated in paragraph 2.5 below. The Parent company will also update the General Section of the Model so it can meet possible new requirements.

The individual Group companies is assigned the task of preparing and update the Special Sections of the Model in relation to their particular business and risk activities; le Special Sections will be adopted by the individual Group companies by applying the formalities stated in paragraph 2.5 below.

b) Application of the Model and checks on its implementation

The individual companies of the Group shall be responsible for implementing the Model with regard to the specific activities it carries out. To this end, the COs of the individual Group companies are assigned the main task of carrying out checks on the Model's implementation according to the procedures described therein.

c) Co-ordination of the control functions and check on the Model's effectiveness

The CO of Weather Investments S.p.A., as holding company of the Group, is entrusted the task to generally promote and co-ordinate - also by way of contacts on the IT network - the control activities on Model application within all the Group companies to ensure that the Model is correctly and uniformly implemented, as well as to carry out, in special cases, specific checks on the individual Group companies.

In compliance with the criteria mentioned above, the model is implemented as follows.

2.5 Approval of the Model and its adoption within the Group

This Model, which is made up of the General Section and the Special Section "A" and "B", has been approved by the Board of Directors of Weather Investments S.p.A. with resolution of 19 July 2006.

The Model will be adopted also by the other Group companies with regard to the at-risk activities carried out by them.

In particular, the Boards of Directors of the different Group companies is assigned the task - also on the basis of criteria and directives that may be passed in this area by the Chairman or Managing Director of Weather Investments S.p.A. - of adopting, by way of an *ad hoc* resolution, this organisational Model as well as its individual special sections, depending on the risk profiles of each of the activities carried out by the different companies.

In adopting the Model, the Boards of Directors of the individual Group companies will at the same time also appoint their Compliance Officer (CO) who, within the scope of the company he/she belongs to, be assigned with performing checks at to the performance of the above activities and the Model's application.

2.6 Changes and integration to the Model

Since this Model is a "document passed by a resolution of the Board of Directors" (in compliance with the provisions contained in Art. 6 paragraph I, letter a of the Decree) the subsequent changes and integration to the General Section of the Model - if of noteworthy importance - are the responsibility of the Board of Directors of Weather Investments S.p.A., while those related to the Special Sections are the responsibility of the Boards of Directors of the different Group companies.

Within the area of its competence, the Chairman and/or the Managing Director of the Group companies has the right to make formal changes or integration to the text. The model makes also provision, in some of its parts, for the sole competence of the Chairman and/or of the Managing Director of Weather Investments S.p.A. and, in other sections, for the sole competence of the CO of Weather Investments S.p.A. as to the inclusion of specific integration to the text. All the changes and integration mentioned above are immediately adopted by the various subsidiaries by effect of the initial resolutions adopted by the respective Boards of Directors that, upon Model adoption, shall provide for the Model to be directly subject to changes and integration made by Weather Investments S.p.A.

Weather Investments S.p.A. will notify the subsidiaries in a timely manner of all modifications made to the Model.

2.7 Application of the Model by the individual companies and their implementation of the checks on the at-risk activity areas

The individual Group companies are assigned responsibility for implementing the Model within their scope of responsibility depending on the activities they concretely enact in the at-risk areas. To this end, the respective residents and/or Managing Directors and respective COs may - subject to approval by the Weather Investments S.p.A. CO - make possible integration to the Model in the specific parts or issue appropriate instructions regarding the points for which express provision is made for this possibility in their regard. It remains the main task of the respective COs to carry out the checks on the activities of the individual companies in the at-risk areas according to the procedures hereunder described.

2.8 Co-ordination on the control and verification systems on general Model effectiveness

Subject to assignment of the responsibility to the individual Group companies with regard to the Model implementation in regard to activities the it basically implements in the at-risk areas and the main responsibility of the respective COs to perform checks on these activities according to the procedures described below, is assigned to the CO of Weather Investments S.p.A., as group holding, the task of give direction and coordinate - also by way of contacts on the IT network - the Model's application within the scope of all the Group companies so to ensure that it is correctly and uniformly implemented, with the possibility of directly carrying out specific checks on the individual Group companies. In particular the CO of Weather Investments S.p.A., while respecting

General Section

the autonomy of the different Group companies and the limits set by legal provisions (for example, as far as company secrecy, the protection of the privacy, etc.), is entrusted the following powers towards the subsidiaries:

- ✓ power to promote and carry out the coordination functions regarding the control and verification activities as well as the application of the Model;
- ✓ power to propose, on the basis of the checks mentioned above, the updating of the Model should it be found that it requires amendment;
- ✓ power to carry out, either personally or jointly with the CO of the Company concerned, special control actions on the individual Group subsidiaries in the at-risk activity areas, with possibility of accessing the relevant documentation of all the Group companies, without any intermediation.

3. Internal control organ (CO)

3.1 Identification of the internal control organ

To implement the provisions contained in the Decree -which, under Article 6, letter b, sets as a prerequisite for exempting Weather from the administrative responsibility, that the task to supervise on the operation and Model compliance, as well as to look after its updating be assigned to a body having independent initiative and control powers - within Weather the most suitable subject for taking on this task and thus for carrying out (according to the terminology used in this Model) the functions of Compliance Officer – CO, has resulted in being the person in charge of the..... This choice was brought about by the fact that this subject resulted as being the most suitable for taking on the role of CO due to the autonomy, independence, professionalism and requirements of continuity demanded by this role.

In case of Weather Investments S.p.A. the above mentioned person in charge of..... - while for the subsidiaries the corresponding subjects - therefore assigned the task, as CO, to perform supervisory and control activities as provided for the Model, the only exception being small-sized companies where, after receiving specific authorisation from the CO of Weather Investments S.p.A., this task will be carried out directly by the Board of Directors (as provided for by the Decree under Article 6, sub-paragraph 4).

Due to the special character of the tasks assigned to the CO and of their specific professional contents, in performing his/her supervisory and control activities, the CO of Weather Investments S.p.A. is backed up by a dedicated staff (used, also part-time for these specific tasks, and usually chosen from among the resources within the Internal Auditing), in addition to the support of the other Managerial Functions of the Holding that, on a case-by-case basis, might result as necessary.

Similarly also within the other Group companies the COs will avail themselves of supporting elements within their staff according to criteria suitable to the various companies.

3.2 Functions and powers of the internal control organ (CO)

The CO of Weather Investments S.p.A. is entrusted in general with the task to check:

- a. that the provisions contained in the Model are complied with by those it is aimed at, as specifically identified in the individual Special Sections in relation to the different types of offences indicated in the Decree;
- b. that, with regard to the corporate structure, the Model is actually effective and capable of preventing offences as envisaged in the Decree from being committed;
- c. on whether it is appropriate to update the Model, should it be found it requires adaptation in regard to changing conditions within the company.

On a more operative level, the CO of Weather Investments S.p.A. and, under his co-ordination, the COs of the other subsidiaries, is entrusted with the task of:

- ✓ activating the checking procedures, taking account that a primary responsibility for activities control – including those concerning the at-risk activity areas – nevertheless remains the responsibility of operative management and constitutes an integral part of the company process (“*line control*”); this confirms the importance of a personnel training process;
- ✓ conducting reconnaissance initiatives of the corporate activities for the purposes of the updated mapping of the at-risk activity areas within the company context;
- ✓ carrying out periodical checks on certain operations or specific actions in the at-risk activity areas as defined in the Model’s individual Special Sections;
- ✓ promoting suitable initiatives for spreading knowledge and understanding of the Model and preparing the internal administrative documentation necessary for the Model operations, with all the instructions, clarifications or updates;

- ✓ collecting, processing and storing the information (including the recommendations contained in the chapter 5 below) regarding compliance to the Model, as well as updating the list of information that must be sent to the CO (see chapter 5 below) or made available to him/her;
- ✓ co-ordinating with other company functions (also through appropriate meetings) for the best monitoring of the activities in the at-risk areas. To achieve this, the CO is constantly informed as to the progress of the activities in the above at-risk areas, and has clear access to all the relevant company documentation. The COs must also be informed by the management as to possible situations in the company operations that might place the company in an "offence risk" position;
- ✓ checking that the necessary documents do exist, that they are regularly kept and effective, in compliance with the provisions contained in the individual Special Sections of the Model for the different types of offences. In particular, the CO must receive notification of the most significant activities or the operations considered in the Special Sections, and the updated documentation data must be made available to allow the checks to be carried out;
- ✓ conducting the internal investigations for checking on alleged violations of this Model's provisions;
- ✓ checking that the elements provided for by the individual Model Special Sections for the different types of offences (adoption of standard clauses, fulfilment of procedures etc.) are however suitable and conform with the needs to comply with the provisions contained in the Decree, and, should this not be the case, update such elements;
- ✓ co-ordinating with the Persons in Charge of the other corporate Functions with regard to other aspects relating to the implementation of the Model (definition of the standard clauses, personnel training, disciplinary measures, etc.).

3.3 Functions of the CO: Reporting to the corporate bodies

The CO of Weather Investments S.p.A. has two lines of reporting:

- ✓ the first, on a continuous basis, directly with the Chairman and/or Managing Director;
- ✓ the second, periodically, to the Internal Audit Committee, the Board of Directors and the Statutory Board of Auditors.

The presence of the above mentioned functional relationships, also with top bodies not having operational tasks and therefore not connected with managerial activities, is a guarantee of the CO's being able to carry out its assignment under very independent conditions.

The CO of Weather Investments S.p.A. may be called at any time by the above mentioned bodies or may, in its turn, present application for it to report on specific situations or how the Model operates.

Furthermore, each year the CO of Weather Investments S.p.A. sends the Board of Directors, through the Internal Audit Committee, a written report on the implementation of the Model at Weather Investments S.p.A., as well as at other Group companies.

Similarly, in addition to their reports to their respective Managing Directors on a continual basis, also the CO of the other Group companies will be required to report more on a periodical basis to the respective Board of Directors and Board of Auditors on the Model implementation within the scope of their respective company.

3.4 Co-ordination functions of Weather Investments S.p.A. with the COs of the other Group companies

The CO of Weather Investments S.p.A. is entrusted with the task of coordinating, also by way of contacts on the IT network, the activities of the other Group's companies for the purposes of implementing a coherent control system within the scope of the Group itself.

The CO of Weather Investments S.p.A. is entitled to acquire documentation and information and to carry out periodic and *ad hoc* checks on the at-risk activities of the different Group companies.

4. Selection, training and reporting

4.1 Personnel selection

The CO of Weather Investments S.p.A., in liaison with the Department of Human Resources, assesses whether a specific evaluation system should be put into place for personnel selection to take account of the company's requirements with regard to the Decree's application.

4.2 Personnel training

Within the scope of the Model's implementation, personnel training is managed by the Department of Human

Resources in close co-operation with the CO, and will be addressed to all the personnel with the access to an intranet website dedicated, internal training, informative report in the employment letter for the new staff; moreover, for the managerial personnel, personnel having representation functions and personnel working in risk activities, with updating e-mails, internal information note and update seminar

4.3 Selection of freelancers and partners

Within the company, on the CO's proposal, after resolution of the Chairman and/or the Managing Director, suitable evaluation systems might be put in place for the selection of agents, consultants and the like ("Freelancers") as well as partners with which the Company intends to strike a partnership (for example, a joint-venture, also in the form of a temporary company association, consortium, etc.) and to be used to cooperate with the company in the performance of at-risk activities ("Partners").

4.4 Informative report to freelancers and partners

On the basis of this organisational Model as well as the texts of the contract clauses usually employed in this regard, independent subjects (Agents, Consultants and Partners) might be supplied with informative reports on the policies and procedures adopted by Weather.

5. Information flows to the CO

5.1 Notices by company representatives or by third parties

In addition to the documents indicated in the individual Special Sections of the Model according to the procedures provided for therein, within the company any other information should be reported to the CO, irrespective of the type and whether it comes from third parties, if such information relates to the Model implementation in the at-risk activity areas.

In this regard, the following prescriptions apply:

- ✓ all indications should be gathered regarding the committing of the offences as provided for by the Decree in regard to the Group activities or behaviours that are not in line with the regulations adopted by the Group itself;
- ✓ inflow of notices, including un-officious ones, must be channelled to the CO of the Company concerned and by him to the CO of Weather Investments S.p.A.;
- ✓ at his discretion, the CO of the Company concerned will assess the indication received and any possible resulting provisions, possibly listening to the informing person and/or the person who allegedly committed the offence and reporting in writing any decision to not carry out an internal investigation; the initiatives taken on in this regard shall be shared with the CO of Weather Investments S.p.A. Telecomunicazioni S.p.A.. who will have the power to take the case upon himself;
- ✓ in compliance with the provisions contained in the ethical code, the reports may be in writing and have, as their subject, any breaches or suspected breaches of the Model. The CO of the Company concerned and the CO of Weather Investments S.p.A. will act to guarantee the informing of persons against retaliation, discrimination or penalisation, by guaranteeing confidentiality as to the identity of the informing party, subject to the law provisions and the protection of the Company or of the persons mistakenly and/or falsely accused;
- ✓ provision is made for setting up "dedicated informative channels" ("Dedicated channel") both by the CO of Weather Investments S.p.A. and the CO of the individual companies involved. Such channels will perform a dual function: that of facilitating the flow of information towards the CO and of quickly solving doubtful cases.

5.2 Information obligations relating to official acts

In addition to the indications, however unofficial, as stated in the previous chapter, the CO of the individual company concerned must be sent the information and, in turn, he shall report to the CO of Weather Investments S.p.A. the informative reports regarding:

- ✓ measures and/or news from the criminal police or from any other authority from which one might infer that investigations are being conducted, also against unknown persons, for the offences envisaged in the Decree;
- ✓ requests of legal assistance submitted by the managers and/or the employees in the event of legal procedures for the offences provided for by the Decree;
- ✓ reports prepared by the persons in charge of other company functions within the scope of their control activities and from which serious facts, acts, events or omissions may emerge with respect to non-compliance of the rules contained in the Decree;
- ✓ news relating to the actual implementation, at all company levels, of the organisational Model reporting the disciplinary proceedings carried out and any fines inflicted (including measures against Employees) or any

General Section

dismissal decisions regarding such proceedings with the relative grounds.

If necessary, the CO Periodically proposes possible changes to the above list to the Chairman and Managing Director.

5.3 Proxy system

Finally, the CO must be notified as to the proxy system adopted by each Group company.

6. Disciplinary system

6.1 General principles

The main feature for Model effectiveness is the preparation of an appropriate fine system to punish breaches to the ethical code with the aim of preventing the offences envisaged in the Decree and, in general, the infringement of the internal procedures provided for by the Model itself.

The application of the disciplinary sanctions is not linked to the result of any penal proceedings in that the behavioural rules imposed by the Model are taken on by the company in completely independently, irrespective of the offence that such conducts might bring about.

6.2 Sanctions for employees

The behaviours by employees in breach of the individual behavioural regulations stated in this Model are defined as disciplinary offences.

With reference to the fines inflicted against such employees that fall within those provided for by the company's disciplinary code, in compliance with the procedures provided for by Article 7 of Italian Law no. 300 of 30 May 1970, (Employees Statute) and any special applicable rules.

With reference to the above, the Model makes reference to the categories of deeds that can be fined as provided for in the current fines system, and that is the agreement rules as per the CCNL (see Art. 46,47 and 48 of CCNL Telecommunication).

In particular, in application of the "Provvedimenti disciplinari" in force in Weather and mentioned by the CCNL, provision is made that to the Employees who infringe the internal procedures provided for by this Model (for example by not complying with the procedures prescribed, by failing report the prescribed information to the CO, by failing to carry out controls, etc.) or, in performing activities in the at-risk areas, do not conform with the behavioural prescriptions contained the Model, or, in by acting against Weather's interests, which damages the Company or caused an objectively-dangerous situation for the company assets, the following measures will be taken:

- ✓ verbal reproach
- ✓ written reproach
- ✓ penalty not above three hours of the base salary
- ✓ suspension from work and remuneration up to maximum three days
- ✓ dismissal (with or without notice) as foreseen in article 48 of CCNL Telecommunication

since such behaviors are considered as a "non compliance with the law, contract or company regulations and internal rules...." as indicated under paragraph 1 of article 46 of the CCNL Telecommunication.

The "provvedimenti disciplinari" will be applied depending on the degree of seriousness of the deeds.

6.3 Measures against managers

In the event that managers infringe the internal procedures provided for by this Model or, in performing activities in the at-risk areas, that they adopt a behaviour not in keeping with the Model rules, steps will be taken against the persons responsible as provided for in the national collective labour agreement for Industrial Managers.

7. Other protection measures in the event of non compliance with Model rules

7.1 Measures against Directors

In the event of infringements to the Model by Directors of the holding company, the CO will refer this to the Board of Directors and Statutory Board of Auditors, who will be responsible for taking the appropriate measures as provided for by current Legislation.

Should the above infringements be made by Directors of subsidiaries, the CO of Weather Investments S.p.A shall be informed immediately and he/she will inform the company bodies Weather Investments S.p.A. so as to adopt the necessary measures within the Group.

7.2 Measures against Freelancers and Partners

Any behaviour by Freelancers or Partners that contrasts with the behavioural guidelines stated in this Model and such as to entail the risk of committing an offence punished by the Decree, might result - according to the provisions contained in the specific clauses of the job orders or in the partnership agreements - in agreement cancellation subject to the possibility for the company to apply for damages if such behaviours cause concrete damages to the company, as in the event of the judge applying the measures provided for by the Decree.

8. Periodical checks

This Model will be subject to two types of check:

- ✓ **checks on the deeds:** on a yearly basis a check will be made on the main company deeds and the most important agreements entered into by the company within the at-risk activity areas;
- ✓ **procedures checks:** periodically the CO will verify the effective operation of this Model. Also, a review will be undertaken of the eventually notices received during the year, any actions by the CO and other interested subjects, the events considered to be at risk, the awareness of the personnel concerning cases of offences as provided for in the Decree, also with sample interviews.

As a result of the check, a report will be signed and submitted to Weather Investments S.p.A 's Board of Directors. It will state any omissions and provide recommends on action to take.

9. Model and Code of Ethics

The behaviour rules contained in this Model are integrated with those of the Code of Ethics although - for the purposes that it pursues in implementing the Decree provisions - the Model presents a scope that is different to that of the Code.

Under this profile, indeed:

- ✓ the Code of Ethics is a tool adopted independently and thus one that is generally applied by the Group companies in order to express the "company ethics" principles which the Group acknowledges as belonging to it and which it requires its Employees to observe;
- ✓ the Model instead responds to specific rules contained in the Decree that aim at preventing specific types of offence from being committed (for actions that, being apparently committed to the advantage of the company, might entail administrative responsibility as per the Decree's provisions).

Special Section “A”

Offences in the relationships with the Public Administration

A.1 Types of offences in the relationships with the Public Administration (articles 24 and 25 of the Decree)

With regard to this Special Part “A”, hereinbelow we provide a brief description of the offences contemplated therein, set forth in articles 24 and 25 of the Decree.

Misappropriation causing prejudice to the State or European Union (article 316-bis of the Criminal Code)

The offence is committed when, after receiving funding or contributions from the Italian State or European Union, the sums thus obtained are not used or allocated for the purposes for which they were intended (indeed, the practice consists in having embezzled such funds, including part thereof, without there being any proof that the planned activity is actually carried out). Considering that the culminating point of the offence coincides with the operational stage, the offence may also be committed with regard to funding previously obtained which is no longer intended for the purposes for which such funding had been provided.

Fraudulent appropriation of funds causing prejudice to the State or European Union (article 316-ter of the Criminal Code) 316-ter of the civil procedure code.

This offence is committed when, through the use of or submission of declarations or false documents or through failing to provide required information, contributions, funding, loans on favourable terms or other funds of the same type granted or provided by the State, by other public bodies or by the European Union, are obtained fraudulently. In this case, unlike what has been seen with regard to the previous point (article 316-bis), the use to which the funds are put is immaterial as the offence is committed when the funding is obtained. Lastly, it is worthy of note that this possible offence is residual in relation to the hypothetical fact situation involving fraud causing prejudice to the State, in the sense that this offence is committed only when the practice does not establish the necessary elements to demonstrate that an offence has been committed against the State.

Extortion (article 317 of the Criminal Code)

The offence is committed when a public official or a public service representative, taking advantage of his/her position, compels someone to obtain for him/her or for others, money or other benefits to which he/she is not entitled. This offence is applied in a purely residual manner within the framework of the hypothetical fact situation contemplated by the Decree; more specifically, this form of offence could be surmised, according to the Decree, when an individual working for a Company or an Agent of a Group Company takes part in the offence committed by the public official who, taking advantage of his/her role, requests services or some other thing, to which he/she is not entitled, from third parties (obviously considering that an advantage for the Group Company derives in some way from such behaviour).

Corruption on the grounds of performance of an official act or an act which runs counter to official duties (articles 318-319 of the Criminal Code)

An offence is committed in the event that a public official receives for themselves or for others, money or other benefits for performing, failing to perform or delaying official acts (thereby creating an advantage for the offeror).. Activity on the part of the public official may manifest itself either in the form of an act which the official is duty-bound to perform (for example: rapidly dealing with a matter over which the official has authority), or in the form of an act which runs counter to the official's duties (for example: a public official who accepts money for guaranteeing that a call for tenders will be awarded). Corruption should be distinguished from extortion, inasmuch as between the corrupted party and the corrupter there is an agreement, the purpose of which is to achieve something to the parties' mutual advantage, whilst in cases of extortion a private individual is subjected to the actions of a public official or a public service representative.

Corruption in legal proceedings (article 319-ter c.p.)

This possible offence is committed when a Group Company is involved in legal proceedings and, in order to obtain an advantage corrupts a public official (not only a magistrate but also a clerk of the court or another official).

Punishments for the briber (art. 321 of the Criminal Code)

The established punishments in the first paragraph of the article 318, in the art. 319, in the art. 319-bis, in the article 319-ter and in the art. 320 of the Criminal Code, in relationship to the aforesaid hypotheses of the arts. 318 and 319 of the Criminal Code, they are also applied to whom gives or it promises to the official public or to the entrusted of a public service the money or other utility.

Inducement to commit acts of corruption (article 322 of the Criminal Code)

Such hypothesis of crime shapes him towards whoever offers or promises money or other utility non due to an official public or entrusted of public service that the quality of public dresses again employee to induce to complete, to omit or to delay an action of its office, or to make an action contrary to its duties and such offer or promised is not accepted.

Fraud committed against the State, other public bodies or the European Union (article 640, paragraph 2 n° 1 of the Criminal Code)

The offence is committed when in order to obtain unlawful profit for oneself or for others, stratagems or tricks are employed such as are likely to cause others to commit errors and cause damage to the State (or to another Public Body or to the European Union). By way of example this offence may be committed if, when preparing documents or data in order to take part in a tender, information is provided to the Public Administration which is false (such as, for example, using forged documentation) in order to be awarded the tender.

Aggravated fraud to obtain public funds (article 640-bis of the Criminal Code)

This possible offence is committed when the fraud is carried out in order to unlawfully obtain public funding. This hypothetical fact situation obtains when an offence is committed when stratagems or tricks are employed, for example by communicating false data or by preparing false documentation, in order to obtain public funding.

Computer fraud causing prejudice to the State or other public bodies (article 640-ter of the Criminal Code)

The offence is committed when the perpetrator, altering in some way the functioning of a computer system or data transmission system or manipulating the data contained therein, obtains for himself/herself an illegal profit thereby causing damage to others. In practical terms the offence in question could be surmised, if having obtained funding, the perpetrator were to violate the computer system in order to enter an amount, in respect of funding, greater than the legitimately obtained amount.

A.2 Areas at risk

In order to be considered offences the aforementioned require there to be relations with the Public Administration (interpreted loosely and in such a manner as to include the Public Administration of Foreign States). What is more, considering the multiplicity of relations that the various Group companies have with Public Administrations in Italy and abroad, the areas of activity which can more specifically be considered at risk in relation to this Special Section "A", are:

1. negotiating/entering into and/or performance of contracts/concession agreements with public entities, arrived at by means of negotiated procedures;
2. negotiating/entering into and/or performance of contracts/concession agreements with public entities, arrived at by means of published procedures;
3. managing relations with public entities in order to obtain authorisation, licences, occasional/ad hoc administrative measures as are required to perform typical corporate activities and activities relating to the achievement of the corporate purpose, and relating to compliance with legal requirements such as communications, declarations, filing deeds and documents, dossiers etc and the checks/investigations/sanctions arising therefrom.
4. managing relations with public bodies with regard to matters of safety and workplace hygiene (for example legislative Decree 626/94) and complying with legal requirements, checks and inspections relating to solid, liquid or gaseous waste, or otherwise the emission of fumes or acoustic/electromagnetic pollution;
5. managing the social security situation of personnel and/or handling related investigations/inspections and dealing with public entities with regard to the employment of people (included people belonging to

Special Section "A"

- protected categories or who may be employed on favourable terms);
6. handling relations with regulatory bodies with regard to undertaking activities regulated by law;
7. engaging in activities relating to acquisition and/or management of contributions, subsidies, funding, insurance or guarantees granted by public entities;
8. preparing income tax returns or withholding tax returns or other declarations the purpose of which is to ensure payment of taxes in general;
9. handling legal proceedings or arbitration;
10. overseeing institutional activities with Italian and foreign public entities;
11. other sensitive activities

Any additions to the aforementioned risk activity areas may be decided by the Chairman and/or the Managing Director of the Company who is charged with identifying related situations and determining the details of suitable operational measures.

Furthermore, processes for handling funds ("Support Processes") impacting indirectly the offences contemplated under legislative Decree 231/200 have been analysed. The Support Processes analysed are:

1. procurement of goods and services;
2. awarding contracts for the provision of consultancy or professional services;
3. managing payments and financial resources;
4. managing benefits (free gifts, publicity, sponsorship, entertainment expenses etc);
5. selecting and hiring personnel and providing compensation policy incentives.

A.3 General reference principles

A.3.1 The general organisational system

The Company must have in place organisational instruments (company organisation chart, organisational communications, procedures, etc) informed by general principles of:

1. clear description of the reporting lines;
2. vested powers (within the company and in dealings with associated third parties) must be knowable, transparent and publicised;
3. clear and formal demarcation of roles, with a complete description of the tasks for each function, related powers and responsibilities.

The internal procedures must be characterised by the following elements:

- a) separation, within each process, between the party taking the decision (decision-making driver), the party executing the decision and the party which is tasked with verifying the process (known as "function segregation");
- b) written trace of each important stage in the process (known as "traceability");
- c) suitable level of formalisation.

More specifically:

- a) the corporate organisation chart and the spheres of activity and responsibilities of the corporate functions must be defined clearly and precisely through special organisation communications, made available to all employees;
- b) guidelines must be determined in detail in addition to procedures regulating, inter alia, selection and qualification of the main corporate suppliers, processes for assigning tasks on the basis of specific evaluation criteria, processes for handling the first contact and commercial activities vis-à-vis public clients, managing institutional or occasional relations with Public Administration entities;
- c) selection of suppliers, referred to in loose terms, use of goods and services and verification of

Special Section "A"

compliance with contractual conditions (both inward and outward) must preferably be segregated by stages and spread over several functions when the invoices are prepared/received;

- d) the Internal Managers and the Internal Sub-Managers for each risk area must be formally appointed, by means of a specific letter.

When performing all the operations associated with ordinary operations, regulations pertaining to the corporate administrative, accountants, financial and financial control system must be complied with, in addition to, in general, all applicable laws.

A.3.2 The system relating to delegation of authority and powers of attorney

In principle, the system relating to delegation of authority and powers of attorney must be characterised by "certainty" in order to prevent offences and in order to allow efficient conduct of corporate activity.

"Delegated authority" means an internal act vesting functions, duties and responsibilities. "Power of attorney" means the unilateral legal transaction with which the Company vests representative power in a single party.

The essential requirements of the system relating to delegation of authority and powers of attorney are the following:

- ✓ all those who, on behalf of the Company have institutional relations with the Public Administration, whether Italian or foreign, must hold formal delegation in that respect;
- ✓ every power of attorney granting power to represent the Company in dealings with third parties must be supported by an internal document describing the related management power;
- ✓ each attorney in fact must hold expenditure powers in keeping with the powers vested in him or her;
- ✓ delegated authority, powers of attorney and organisational communications must be promptly updated and must be consistent with the activity actually carried out.

A.4 Recipients of the Special Section: general behavioural principles and implementation

This Special Section refers to conduct on the part of directors, senior executives and employees ("Corporate Personnel") operating in the activity areas at risk and also refers to Outside Contractors and Partners, as already defined in the General Part (hereinbelow all defined as "Recipients").

The objective of this Special Section is that all Recipients, as identified above, adopt rules of conduct which are consistent with prescriptions set down in same in order to prevent the occurrence of offences contemplated in the Decree and more specifically they are required to comply with the following general principles:

- ✓ strict compliance with all laws and regulations regulating corporate activity, referring specifically to activities entailing contact and relations with the Public Administration;
- ✓ initiating and maintaining relations of whatsoever type with the Public Administration on the basis of criteria of utmost probity and transparency;
- ✓ initiating and maintaining relations of whatsoever type with third parties in all activities relating to the public functions or the provision of public services on the basis of criteria of utmost probity and transparency guaranteeing that the function or service is correctly performed and that such are characterised by impartiality.

This Special Part expressly prohibits Corporate Personnel, either directly or acting through outside contractors and Partners, by means of specific contractual clauses, from:

- 1) behaving in such a manner as may be construed as representing one of the aforementioned offences (articles 24 and 25 of the Decree);
- 2) behaving in such a manner as, though not per se amounting to an offence included amongst the aforementioned, may potentially become an offence;
- 3) giving rise to any conflict of interest vis-à-vis the Public Administration with regard to the matters covered by the aforementioned offences.

Special Section "A"

Within the framework of the aforementioned behaviours (also confirmed by the Ethics Codes adopted by the Group) there is an express prohibition on:

- a) providing, receiving or soliciting gifts in monetary or non-monetary form or advantages of whatsoever type if such fall outside standard business practices and commonly accepted courtesy in dealings with public officials;
- b) distributing gifts above and beyond what is customary corporate practice (meaning, in accordance with the provisions of the ethics code, all forms of gifts which are offered or received if such fall outside standard business practices and commonly accepted courtesy, or in any case if they are intended to obtain favourable treatment for any corporate activity). More specifically, it is prohibited to give any kind of gifts to Italian and foreign public officials (including in those countries in which providing gifts represents customary practice), or to members of their families, when such may influence that official's impartiality or may induce him to provide an advantage to the Company. The distinctive feature of permitted gifts is always their low financial value or the fact that they are designed to promote artistic initiatives (for example, distribution of art books), or the Group brand image. All gifts offered – except for those of a very low financial value – must be suitably documented in order to allow necessary verification;
- c) agreeing other advantages of whatsoever type (promises to hire employees etc) in favour of representatives of the Public Administration which may have the same consequences as contemplated in point b) above;
- d) providing services to the Partners which are not justified within the framework of the relations with the Partners;
- e) making payments to Outside Contractors which are not justified with regard to the type of task assigned and in relation to practices which are customary in a particular area;
- f) issuing false statements to national or European Union public organisations in order to obtain public funding, benefits or funding on favourable terms;
- g) allocating sums received from national or European Union public organisations by way of funds, benefits or funding for purposes other than those to which they are intended;
- h) altering the working of information technology and data transmission systems or manipulating data contained therein;
- i) no kind of payment may be made in cash or in kind;
- j) those who perform an oversight and supervision function in respect of compliance with legal obligations connected to carrying out the aforementioned activities (payment of invoices, allocation of funding obtained from the State or from European Union organisations etc) must pay particular attention to such compliance and must immediately report any irregularities to the CO.

A.5 Activity areas at risk: appointment of the Internal Responsible

For every risk area, as identified in point A.2, the Managing Director of the Company, or a senior executive tasked by same, is required to appoint somebody from within the Company (the "Internal Responsible").

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the oversight and supervision system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

A.6 The control system

The control system applicable to the risk areas identified has been defined using as a reference the Guidelines published so far by the leading industry associations, in addition to the international best practices in the field of fraud and corruption risks.

For each one of the risk areas the following control standards have been identified:

- a) segregation of activities: there must be segregation of activities between personnel who execute, who oversee and who provide authorisation;
- b) rules: there must be corporate rules to at least provide general reference principals for purposes of regulating sensitive activities;
- c) signing authorisation and powers: there must be formalised rules regulating signing authorisation and internal powers;
- d) traceability: the individual who signs the communications intended for the Public Administration must ensure that the related sources and information elements are traceable.

Hereinbelow, for each process for managing funding, the applicable control standards are set forth.

Procurement of goods and services

- a) Specific procedures: there must be corporate rules relating to procurement of specific types of goods and services (consultancy, professional services) or otherwise relating to procurement adopting specific procedures (for example referring to a sole supplier, or when urgent);
- b) transparency and traceability: for each phase of the procurement process, the corporate rules must be informed by transparency criteria (precise identification of individuals holding responsibility, evaluation of procurement requests; verification that requests are made by individuals authorised to do so, determination of the criteria which shall be employed in the various stages of the process and expressing an assessment of the technical and economic offers) and traceability of operations carried out;
- c) procurement procedures: the choice of the procurement procedure to be adopted (call for tenders; sole supplier, the use of qualified vendor lists) must be formalised and authorised at an appropriate level;
- d) determination of short vendor list: the determination of the short vendor lists must be carried out by using transparent procedures and must be authorised at an appropriate level;
- e) "sole supplier" procedures: resorting to the "sole supplier" procedure must be restricted to a limited number of cases which are clearly identified, suitable reasons must be given and documented, and procedures must be subject to suitable control systems and authorisation systems at an appropriate level;
- f) reporting proceedings and managing calls for tenders: the principal stages of calls for tenders - opening the technical bids, determination of the technical opinion and opening the economic bids - must be recorded and parties with conflicting interests must be present (both procurement and unit making the request);
- g) rotation of personnel: criteria for rotating persons involved in the procurement process must be defined;
- h) rotation of suppliers in the lists: suitable monitoring systems must be formally created in order to ensure correct, normal rotation of suppliers included in the vendor lists;
- i) reports: there must be suitable monitoring systems and reports to be submitted at an appropriate hierarchical level for monitoring must be formalised (for example number of calls for tender, winning supplier, awarding commission, amount and body requesting a sole supplier etc);
- j) procurement in the event of urgency: urgent conditions in respect of which it is possible to commission goods or services directly must be clearly defined and suitable authorisation tools and monitoring tools (reports submitted at an appropriate hierarchical level) must be defined.

Awarding contracts for the provision of consultancy or professional services

- a) Formal authorisation: there must be formalised authorisation for engaging a provider of consultancy or professional services, with a limit on expenditure, restrictions and responsibility;
- b) list of suppliers: the provider must be engaged on the basis of a list of suppliers / consultants / professionals, managed by the relevant Unit. Entry/cancellation from the list must be based on objective

Special Section "A"

- criteria. Reasons must be given for identification within the list and must be documented;
- c) documentation: there must be supporting documentation for engagements providing reasons, certificates demonstrating relevance and appropriacy, approved by the superior and these must be archived.

Managing payments and financial resources

- a) Formal authorisation: there must be formalised authorisation for expenditure/engaging a provider of consultancy or professional services, with a limit on expenditure, restrictions and responsibility;
- b) documentation: there must be supporting documentation for the financial resources employed, providing reasons, certificates demonstrating relevance and appropriacy, validated by the superior and these must be archived;
- c) rules: there must be a procedure providing for involvement of all parties and/or functions for payment instructions.

Handling free gifts/publicity/donations/sponsorship and entertainment expenses

- a) formal authorisation: there must be formalised authorisation (by the Managing Director or a Director tasked by same) before benefits can be given;
- b) list of gifts: gifts must be selected from a special list – supervised by the relevant Function and by an individual other than the one having relations with the Public Administration;
- c) documentation: there must be supporting documentation for expenditure relating to the provision of benefits, providing reasons, certificates demonstrating relevance and appropriacy, validated by the superior and these must be archived;
- d) supplier list: any suppliers of benefits must be chosen from a list supervised by the appropriate function. Entry/cancellation of suppliers from the list must be based on objective criteria. Reasons must be given for identification within the list of the supplier of the specific benefit and this must be documented;
- e) reports: there must be regular reports on expenses incurred in providing benefits, with reasons given and names/beneficiaries, and they must be sent to the superior hierarchical level and archived;
- f) budget and final balance: in the budget and in the final balances the amount spent on each type of benefit must be recorded separately.

Selection and hiring of personnel

- a) Authorisation: there must be formalised authorisation for hiring personnel;
- b) procedures: there must be procedures with objective criteria for selecting candidates;
- c) documentation: there must be supporting documentation for all employees hired.

A.7 Instructions and verification by CO

It is the duty of the Company's CO:

- a) to regularly check compliance with internal procedures;
- b) regularly verify – with the support of the other related functions – the current delegated authority/power of attorney system as well as organisational communications, recommending modifications should management power and/or status not correspond to the powers of representation vested in the Internal Responsible or the sub Responsible;
- c) regularly verify, with the support of the other related functions, the validity of the standard clauses with a view to:
- d) ensuring compliance on the part of the Recipients with the provisions of the Decree;
- e) enabling the Company to effectively control the Recipients of the Model in order to verify compliance with the prescriptions contained therein;
- f) implementing sanctions (such as withdrawal from the contract in respect of Partners or outside contractors) should it be established that the prescriptions have been breached;
- g) informing the management of appropriate additions to the systems for managing financial resources (both incoming and outgoing), which are already present in the Group, introducing devices likely to

Special Section "A"

detect any transfer of funds which are irregular, providing greater discretion compared to standard procedure.

Special Section “B” Corporate offences

B.1 The types of corporate offences (article 25-ter of the Decree)

With regard to this Special Part “B”, hereinbelow we provide a brief description of the offences contemplated therein, set forth in article 25-ter of the Decree (hereinafter the “Corporate Offences”), grouping them, for purposes of greater clarity, into 5 different types.

B.1.1 Fraudulent information in communications and reports

False Company communications (article 2621 and 2622 of the Civil Code)

These are two possible offences, commission of which typically coincides almost totally and which can be distinguished by whether (article 2622 of the Civil Code) or not (article 2621 of the Civil Code) financial losses are incurred by the shareholders or creditors. These offences are committed (i) through setting out in the financial statements, reports or other corporate communications provided for by law, intended for shareholders or the public, false material facts even being covered by evaluation, or otherwise through (ii) omitting legally required information relating to the economic or financial situation of the Company or Group to which they belong; the conduct described above (relating to both commission and omission) must be engaged in in both cases with the intention of deliberately misleading shareholders or the public and in addition there must be evidence that it is was done in a manner which is likely to induce those receiving such communications to commit errors as to the actual situation, being in short intended to enable the perpetrators to obtain for themselves or for others an unlawful profit.

In this regard it should be noted that:

- ✓ the false information or omissions must be such as to materially alter the description of the economic or financial situation of the Company or Group to which it belongs.
- ✓ criminal liability may also be extended to cases in which the information concerns assets in the possession of or administered by the Company on behalf of others;
- ✓ the offence referred to in article 2622 of the Civil Code is punishable if a complaint is lodged, unless it is committed to the prejudice of the State, other public bodies, or the European Community or if the shares of the Company in question are listed on the stock exchange in which case prosecution is initiated automatically.

Perpetrators of the offence are the directors, the general managers, the senior executives responsible for drawing up the Company’s account documents, the auditors and the liquidators in addition to all those who according to article 110 of the criminal code participate in the offence committed by the aforementioned.

Fraudulent reports or fraudulent communications issued by the auditing firm (article 2624 of the Civil Code)

This possible offence involves fraudulent certification or concealing information, in reports or other communications issued by the auditing Company, concerning the economic, asset-related or financial situations of the Company being audited, in accordance with procedures likely to mislead the Recipients of these communications.

In this regard it should be noted that:

- ✓ there must be awareness of fraudulent information and the intent to deliberately mislead those receiving the communications;
- ✓ the purpose of the fraudulent act must be to obtain for oneself or for others an unlawful profit;
- ✓ the offence in question can be viewed as a crime or a misdemeanour according to whether it has occasioned financial losses for the Recipients.

The perpetrators of this offence are the senior management of the auditing firm, but it is possible that the members of the Board of Directors and the statutory auditors of the Company and employees thereof may also be jointly responsible. In fact it is possible that pursuant to article 110 of the Criminal Code, the directors, auditors or other individuals working for the Company being audited, participate in the offence, having caused or induced the unlawful conduct on the part of the head of the auditing Company.

B.1.2 Protection of the share capital against criminal acts

Fraudulent return of contributions (article 2626 of the Civil Code)

This offence consists in proceeding, aside from cases of legitimate reduction in share capital, to return or feigning to return, contributions to shareholders or releasing same from the obligation to make contributions.

The perpetrators of the offence can only be the directors. In other words the law did not intend to also punish shareholders benefiting from return of the contributions or release from the aforementioned obligation, excluding necessary participation. Nevertheless the possibility remains of participation whereby shareholders who induced or occasioned illegal conduct on the part of the directors are held criminally liable in accordance with the general rules on participation in offences as per article 110 of the criminal code.

Illegal distribution of profits or reserves (article 2627 of the Civil Code)

This offence consists of distributing profits (or advance payments of profits) which have not actually been obtained or allocated by law to reserves or otherwise distributing reserves, (even if not set up with profits) which by law cannot be distributed.

It should be considered that:

- ✓ return of profits or recreation of reserves before the time-limit provided for approval of the financial statements extinguishes the offence.

The perpetrators of the offence are the directors. In other words the law did not intend to also punish shareholders benefiting from distribution of the profits or reserves, excluding necessary participation. Nevertheless the possibility remains of participation whereby shareholders who induced or occasioned illegal conduct on the part of the directors are held criminally liable in accordance with the general rules on participation in offences as per article 110 of the criminal code.

Unlawful operations in respect of shares or quotas or the parent company (article 2628 of the Civil Code)

This offence consists in preceding, aside from cases permitted by law, to acquire or subscribe for shares or quotas issued by the Company (or by the parent Company) causing losses to be made to the share capital or reserves which by law may not be distributed.

It should be considered that:

- ✓ the offence is extinguished if the share capital or the reserves are recreated before the time-limit laid down for approval of the financial statements relating to the operating period during which the offence is committed.

The perpetrators of the offence are the directors. Furthermore criminal liability can be found when the directors of the parent company act in concert with the directors of the subsidiary, in the event that the unlawful transactions on the parent company's shares are committed by the latter when induced by the former.

Operations carried out occasioning prejudice to creditors (article 2629 of the Civil Code)

This offence consists in implementing, in breach of provisions of law safeguarding creditors, reductions in share capital or mergers with other companies, to such an extent as occasions prejudice to the creditors.

It should be considered that:

- ✓ indemnification of losses to creditors before the judgment extinguishes the offence.

Again, the perpetrators of the offence are the directors.

Fictitious formation of capital (article 2632 of the Civil Code)

This offence is represented by the following practices: a) fictitious formation or increase in share capital by means of conferring shares or quotas and in an amount which is lower than their nominal value; b) mutual subscription for shares or quotas; c) significant overvaluing of non-cash contributions or receivables or otherwise of Company assets in the event of Company reorganisation.

The perpetrators of the offence are the directors and the shareholders making contributions.

It is important to note however that failure on the part of the directors and auditors to check and carrying out revision of the assessment of the non-cash contributions contained in the appraisal report drawn up by the

Special Section "B"

expert appointed by the law court is not prosecutable, pursuant to article 2343, 3rd paragraph of the Civil Code.

Fraudulent distribution of Company assets by liquidators (article 2633 of the Civil Code)

This offence consists in distributing Company assets amongst shareholders before payment of Company creditors is made or allocation of such sums as are required to satisfy Company creditors, thereby causing damage to creditors.

It should be considered that:

- ✓ indemnification of losses to creditors before the judgment extinguishes the offence.

The perpetrators of the offence are solely the directors.

B.1.3 Safeguarding the Company's regular operations

Hindering auditing activities (article 2625 of the Civil Code)

This offence consists in hindering or preventing, by concealing documents or, adopting other stratagems, control activities or auditing activities which are legally conferred on shareholders or other Company bodies or auditing firms, when such practice occasions prejudice to the shareholders.

The wrongdoing can be committed solely by directors.

Unlawful influence over the shareholders' meeting (article 2636 of the Civil Code)

This possible offence consists in determining the majority in the shareholders' meeting with sham or fraudulent acts, in order to obtain for oneself or for others, an unfair profit.

The offence is considered a common offence, which can be committed by "whosoever" engages in criminal conduct.

B.1.4 Criminal protection against fraud

Market manipulation (article 2637 of the Civil Code)

It is considered an offence to disseminate false information, or otherwise carry out simulated operations or other such stratagems as are likely to bring about a significant change to the price of non-listed financial instruments or for which no request has been submitted for admission to trading on a regulated market, or otherwise have a significant impact on the trust that the public places in a banks' or bank Groups' economic stability.

Also this offence is considered a common offence, which can be committed by "whosoever" engages in criminal conduct.

B.1.5 Safeguarding regulatory functions against criminal acts

Placing obstacles in the way of Public Regulatory Authorities performing their functions (article 2638 of the Civil Code)

These are two cases of offences which are distinct in terms of modus operandi and the culminating moment:

- ✓ the first comes about (i) through inclusion in communications required by law to public regulatory authorities (in order to hinder the latter performing its functions) of material facts which are untruthful, even though being evaluated, relating to the economic, asset-related and financial situation of the persons or entities being regulated, or otherwise (ii) through concealing, with other fraudulent means, facts which ought to have been notified and which concern the same economic, asset-related or financial situation. Criminal liability may also be extended to cases in which the information concerns assets in the possession of or administered by the Company on behalf of others;
- ✓ the second comes about by simply hindering the activities of public authorities, deliberately and in any manner, including neglecting to give such communications as the aforementioned persons are legally bound to provide to the authorities.

Perpetrators of the offence in both the aforementioned cases are the directors, the general managers, the auditors and the liquidators.

B.1.6 Failure to notify of conflict of interest (article 2629-bis of the Civil Code)

This possible crime consists of a breach of the obligations provided for under article 2391, first paragraph of the Civil Code on the part of the director of a Company with securities listed on regulated markets Italy or in another member State and the European Union or widely distributed to the public pursuant to article 116 of the Unified Finance Law (or otherwise other entities subject to supervision), if the aforementioned breach gives rise to loss or damage for the Company or third parties.

Article 2391, first paragraph, of the Civil Code lays down that directors of joint stock companies must inform the others directors and the Statutory Auditors of every interest they have on their own behalf or on behalf of a third party in a given operation of the Society, specifying the nature, the terms, the origin and the significance. The Managing Directors must also abstain from conducting the operation, directing the board to do so. The sole director must also give notice thereof at the first possible shareholders' meeting.

B.1.7 Extension of the subjective qualifications (article 2639 of the Civil Code)

For all the anticipated crimes from the paragraph B.1, to the subject formally invested of the qualification or titular of the anticipated function from the civil law it is compared both who is kept to develop the same function, otherwise qualified, both who practices in continuous and meaningful way the inherent typical powers to the qualification or to the function.

Out of the concerning cases of application of the rules related to crimes of the official public against the public administration, the sanctions related to the administrators are also applied to those people who are legally entrusted from the judicial authority or from the public authority of vigilance to administer the company or its goods managed by itself ore on behalf of third.

B.2 Areas at risk

With regard to the offences and the criminal activities clearly Stated above, the areas considered most specifically at risk prove to be, for purposes of this Special Part "B" of the Model, the following:

1. drawing up the financial statements, reports and other Company communications provided for by law, intended for shareholders or the public;
2. managing relations with shareholders, auditing companies and the panel of auditors;
3. preparing and publicising outside the Company data and news relating to the Company and the Group;
4. transactions on financial instruments.
5. handling relations with regulatory bodies with regard to undertaking activities regulated by law;
6. transactions on capital and allocation of profits.

Any additions to the aforementioned activity areas at risk may be decided by the Chairman and/or the Managing Director of the Company who is charged with analysing the applicable control system and determining the details of suitable operational measures.

B.3 Recipients of the Special Part: general behavioural principles and implementation

This Special Part refers to conduct on the part of the Company's directors, auditors, liquidators, senior executives and employees ("Corporate Personnel") operating in the activity areas at risk and also refers to Outside Contractors and Partners, as already defined in the General Part (hereinbelow all defined as "Recipients").

More specifically, the purpose of this Special Part is to:

- a) Provide a list of general principles and procedures which the Recipients are required to comply with in order for the Model to be correctly applied.
- b) Provide the CO, and the heads of the other corporate functions called on to cooperate with the CO, with the operational tools to carry out required control activities, monitoring and verification.

In carrying out all the operations pertaining to operating activities, in addition to the rules set out in this Model, the Recipients must, generally speaking, know and comply with all the rules and principles contained in the

Special Section "B"

following documents:

- ✓ the Group's Ethics code;
- ✓ corporate governance rules;
- ✓ operational instructions relating to preparing financial statements, the half yearly report and the quarterly report;
- ✓ all other documentation relating to the internal control system in use in the Company.

This Special Part places an express prohibition on all Recipients, as identified above (restricted to the obligations stated in the specific procedures and in the codes of conduct adopted and the obligations set forth in the specific contractual clauses) from:

- ✓ behaving in such a manner, or collaborating or causing such behaviour as – considered either individually or collectively – amounts to one of the offences included in the offences referred to above (article 25-ter of legislative Decree 231/2001);
- ✓ breaching the corporate principles and procedures provided for in this Special Part.

This Special Part consequently entails the placing of an obligation on the Recipients to scrupulously comply with all laws in force and more specifically to:

1. behave in a correct, transparent and collaborative manner in compliance with legislation and corporate procedures, in all activities required to prepare the financial statements and other corporate communications, in order to provide the shareholder and third parties with accurate, truthful information on the economic, asset-related and financial situation of the Company;
2. scrupulously comply with all regulations laid down under the law to safeguard the integrity of the share capital and to preserve actual existence of same, in order not to prejudice security interests held by creditors and third parties in general;
3. ensure that the Company and the corporate bodies function effectively, assuring and facilitating every kind of internal control over operations pertaining to operating activities in accordance with the law, in addition to encouraging the will of general assemblies to be expressed freely and correctly;
4. every member of the Board of Directors must inform the others directors and the Statutory Auditors of every interest that he has on his/her own behalf or on behalf of a third party in a given operation of the Society, specifying the nature, the terms, the origin and the significance; in the case of the Managing Director, he must also abstain from carrying out such operations, charging the board of directors with doing so;
5. make all communications to the regulatory authorities required by law and the regulations, promptly correctly and in good faith, placing no obstacles in the way of these regulatory functions.

Within the framework of this conduct, there is a specific prohibition on:

referring to point 1 above:

- a) representing or transmitting to be drawn up and represented in financial statements, reports and prospectuses or other corporate communications, any and all false data or data containing omissions or, in any manner not reflecting the real situation, as to the economic, asset-related and financial situation of the Company;
- b) omitting data and information required by law as to the economic, asset-related and financial situation of the Company;

referring to point 2 above:

- c) returning contributions to shareholders or releasing same from the obligation to make contributions, apart from cases of legitimate reduction in share capital;
- d) distributing profits or advance payments on profits which have not actually being earned or which are intended for reserves by law;
- e) making reductions to share capital or carrying out mergers with other companies or demergers, in

Special Section "B"

- breach of legal provisions safeguarding creditors, thereby causing them to incur losses;
- f) proceeding to form share capital or a fictitious increase in share capital, allocating shares at a value which is lower than their par value;

referring to point 3 above:

- g) behaving in such a manner as to materially prevent, by concealing documents or through use of other fraudulent means, control activities from being carried out by the shareholder, Panel of Auditors or by the auditing firm;

referring to point 4 above:

- h) omitting or concealing any interest which, on his own account or on behalf of third parties, the director has in a given Company operation;

referring to point 5 above:

- i) failing to make, with due thoroughness, accuracy and promptness, all periodic reports provided for by law and applicable regulations vis-à-vis the Regulatory Authority, in addition to transmission of data and documents provided for under regulations and/or specifically requested by the aforementioned authority;
- j) stating in the aforementioned limitations and transmissions facts which are not true, or otherwise concealing materially important facts relating to the economic, asset-related or financial conditions of the Company;
- k) behaving in such a manner as hinders the regulatory functions including during inspection by public regulatory authorities (deliberate opposition, specious refusal or other obstructionist conduct or failure to collaborate, such as delaying communications or delays in making documents available).

B.4 Activity areas at risk: appointment of the Internal Responsible

For every risk area, as identified in point B.2, the Managing Director of the Company, or a senior executive tasked by same, is required to appoint somebody from within the Company (the "Internal Responsible").

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

B.5 Control System

The control system applicable to the activities identified has been defined using as a reference the guidelines published so far by the leading industry associations, in addition to the international best practices.

Hereinbelow are set forth, for each risk area, the applicable control standards.

Drawing up the financial statements, reports and other company communications required by law, intended for shareholders or the public

Special Section "B"

- a) Group rules: Group rules clearly defining account principles to be adopted to determine details of entries in the Company's own financial statements and the operating procedures for accounting of same must exist and must be disseminated to the personnel involved in preparing the financial statements. These regulations must be promptly added to/updated by information provided by the relevant office on the basis of new developments in the area of financial reporting regulations and disseminated to the above-mentioned Recipients;
- b) accounts closure instructions: there must be instructions to the Functions (or the subsidiaries for the consolidated figures) with which it is established which data and information must be provided to the Finance Department with regard to the annual and interim annual closures (for the Company's own financial statements and for the consolidated statements), stating procedures and related timeframes;
- c) declarations of reliability: The Managing Director acquires from the finance director (and from senior management in the Group companies for the consolidated figures) the letter attesting to the truthfulness and completeness of the information provided for purposes of drawing up the financial Statements. More specifically by means of this declaration the following is certified:
 - ✓ the truthfulness, correctness, accuracy and completeness of the data and the information contained in financial statements or otherwise in the other accounts documents referred to above and in the related documents, in addition to items of information made available by the Company;
 - ✓ that these declarations relating to the truthfulness, correctness, accuracy and completeness have been gathered by the administration directors of the subsidiaries;
 - ✓ there are no elements from which one could infer that the data and declarations gathered contain incomplete or imprecise elements;
 - ✓ preparation of a suitable control system designed to provide reasonable certainty as to the data contained in the financial statements;
 - ✓ compliance with the procedures set out in this Special Part B of the Model.

The declaration must be:

- ✓ submitted to the Board of Directors to be voted on in the resolution approving the budget;
 - ✓ sent to the CO of the related Company in the form of a copy;
 - ✓ sent to the CFO of the parent company in the form of a copy;
- d) meetings between auditing firm and Panel of Auditors, Finance Director and Regulatory Organisation: one or more meetings must be held between the auditing firm, the panel of auditors, the Finance Director and the Regulatory Organisation prior to the meeting of the Board of Directors to approve the financial statements, having as its purpose the assessment of any critical situations coming to light during auditing;
 - e) traceability; the IT system used to transmit data and information must assure traceability of each step as well as identification of the workstations entering the data in the system. The head of each Function involved in the process must assure traceability of all data and financial information. The procedure relating to the circulation of this data and financial information must provide for simple transmission of same, entailing automatic certification of the sender with regards to completeness and truthfulness of the aforementioned data and information (both automatically generated and not automatically).
 - f) changes to accounts data: any modification to the accounts data can be made only by the Function which generated the data;
 - g) training: in addition to the functions involved in drawing up the financial statements and the related documents, basic training activity must be carried out (with regard to the key legal and accounts notions and problems relating to the financial statements) on the functions involved in determining the details of the financial statement evaluation entries;
 - h) keeping the financial statements set of ledgers: there must be formalised rules identifying roles and responsibilities regarding drawing up, keeping and updating the financial statements set of ledgers from approval by the Board of Directors to filing and publication (including electronically) by same and related storage;
 - i) rules of conduct: there must be rules of conduct for directors, auditors and liquidators requiring utmost accuracy in drawing up necessary communications or communications which are anyhow required by law and intended for shareholders or the public. These rules must provide that clear, precise, truthful and complete information is entered in the communications.

Managing relations with shareholders, auditing firms and the panel of auditors

- a) Roles and responsibilities: roles and duties for all those involved in related positions of responsibility must be clearly and precisely provided for;
- b) an obligation to cooperate: there must be directives laying down an obligation to provide utmost cooperation and transparency in dealings with auditing firms and with the panel of auditors and when shareholders make requests;
- c) selection of the Auditing Firm and independence of same: there must be a corporate rules regulating the stages of the auditing firm selection process and there must be rules to maintain the independence of the auditing firm during its engagement, and as provided for by law¹;
- d) a prohibition on entering into independent or salaried employment contracts with employees of the companies carrying out mandatory auditing which must be affective for 36 months thereafter:
 - ✓ upon termination of the contract between the Company and the auditing firms, or otherwise
 - ✓ upon termination of the contract between the employee and the auditing firm.
- e) traceability and storage: traceability of sources and information in relations with the shareholders, panel of auditors and the auditing firm must be guaranteed;
- f) an obligation to provide information to the internal auditing function: systematic communication to the Internal Auditing Department of every request for information or documentation coming from shareholders, from the panel of auditors and requests for information or documentation which are particularly significant coming from the auditing firm;
- g) reports: there is an obligation on functions tasked with working with the auditing firm for periodic senior management reporting on the state of relations with the auditing firm.

Preparing and publicising data and news relating to the Company and the Group outside the Company ;

- a) Roles and responsibilities: rules and duties for those holding responsibility who are involved in the task of preparing and disseminating data and news relating to new developments must be clearly and accurately put in place and there must be separation between the function supplying the data, the function charged with preparing the press releases and the function authorising dissemination of same;
- b) traceability: the individual responsible for issuing the press releases and other similar information must ensure that the related sources and information are traceable;
- c) communication outside the Company and storage; there must be a formalised corporate rule to identify roles and responsibilities, with regard to providing communications outside the Company and storage of approved documents;
- d) confidentiality obligations: there must be formalised obligations (procedures or internal memoranda, contractual clauses) in order to maintain confidentiality of important information of which employees/external consultants gain knowledge. These obligations must expressly provide for a prohibition on disseminating important information both inside and outside the Company, unless it is done through the correct institutional

1 Article 160 Unified Finance Law 1 paragraph: "In order to assure the company's and the auditing head's independence, an auditing firm finding itself in one of the incompatible situations contemplated under Consob's [Italian Regulatory Authority] regulations can not be engaged"

[...]

"1-ter. The auditing firm and the entities belonging to the auditing firm's network, the partners, the directors, the members of the auditing bodies and employees of the auditing firm and the auditing firms, in addition to associated firms or parent companies or companies jointly controlled, cannot provide any of the following services to the company appointing the auditing firm or to subsidiaries of the same or parent companies or firms jointly controlled:

- a) bookkeeping and other services relating to accounts postings or financial statements reports;
- b) designing and developing information technology account systems;
- c) assessment and appraisal systems and provision of independent opinions;
- d) actuarial services;
- e) outsourcing of internal control services;
- f) consultancy and services regarding corporate organisation focusing on selection, training and management of personnel;
- g) intermediation of securities, investment consultancy or investment banking services consultancy;
- h) providing judicial defence;
- i) other services and activity including consultancy, legal services, unconnected with auditing, identified in compliance with principles set down under the eighth directive n° 84/253/CEE of the Board on 10 April 1984 relating to independence of auditing firms, by Consob under the regulation adopted pursuant to paragraph 1".

Article 149-decies Issuing Companies Regulations

"Consultancy services involving granting powers to represent clients and legal assistance services in the context of disputes are included among other services as per article 160, paragraph 1-ter i) of the Unified Law"

Special Section "B"

channel;

- e) information technology security: there must be appropriate security measures relating to electronic data-processing, such as the measures contained in legislative Decree n° 196 of 2003 and in the international best practices (relating to the network information system and to access to electronically archived privileged data).

Transactions on financial instruments

- a) Segregation of activities: there must be segregation of activities between personnel who execute, who oversee and who provide authorisation;
- b) rules: there must be corporate rules to at least provide general reference principals for purposes of regulating the activities;
- c) signing authorisation and Powers: there must be formalised rules regulating signing authorisation and powers;
- d) traceability: traceability and verifiability after the event in respect of transactions by means of appropriate documentary/information technology supports.

Handling relations with regulatory bodies with regard to undertaking activities regulated by law;

- a) Compliance with legal requirements and regulations concerning communications, both periodic and non-periodic, to be sent to the aforementioned authorities;
- b) compliance with obligations to send data and documents required under the applicable rules to the aforementioned authorities or otherwise such material as is specifically requested by these authorities (for example: financial statements and minutes of the meetings of the corporate bodies);
- c) compliance with obligations to cooperate during inspections, if any.

In addition the Company adopts procedures to manage and check communications sent to the Public Regulatory Authorities.

The procedures to be complied with in order to guarantee compliance with the aforementioned points must meet the following criteria:

1. all such organisational/accounts action must be implemented as is necessary to ensure that the process for acquiring and processing data and information assures that communications are prepared correctly and thoroughly and that they are sent to the public regulatory authorities in a timely manner, in accordance with procedures and the timeframes provided for under the relevant sector regulations;
2. suitable evidence must be provided of procedures adopted to implement the requirements laid out under the previous point 1, referring specifically to identification of those holding responsibility who gather and process the data and the information required therein;
3. in the event of inspections carried out by the authorities in question, there must be cooperation from the related Company units. Specifically, on a case-by-case basis, for each inspection ordered by the authorities, within the Company a manager shall be identified who is responsible for ensuring coordination between those working in the various Company units in order to ensure that they correctly carry out the tasks coming under their authority. This manager is also responsible for ensuring that there is coordination between the various related Company offices and the public authority officials, in order to ensure that the latter are able to acquire all requested elements;
4. the person holding responsibility referred to in point 3) above shall draw up a specific written notice on the inquiry initiated by the authority, which shall be updated on a regular basis with regard to inquiry developments and the outcome; this written notice shall be sent to the CO as well as to the other related Company offices regarding the matter.

Transactions on capital and allocation of profits

- a) Segregation of activities: there must be segregation of activities between personnel who execute, who oversee and who provide authorisation;
- b) rules: there must be a formalised Company rule, aimed at those functions involved in preparing documents on which Board of Directors meetings base their resolutions relating to advance payments on dividends, contributions, mergers and demergers, establishing responsibilities and procedures for preparing said documentation;

Special Section "B"

- c) traceability: traceability and verifiability after the event in respect of transactions by means of appropriate documentary/information technology supports.

B.6 Instructions and verification by CO

The CO's supervisory duties with regard to compliance with the Model regarding Corporate Offences are as follows:

- a) proposing that standardised instructions are issued and updated relating to conduct required within the framework of the risk activities, as identified in this Special Part. These instructions must be written and kept in hardcopy form or electronically;
- b) referring to the financial statements, reports and other corporate communications required by law, by reason of the fact that the Company's financial statements are verified by an auditing firm, the CO is responsible for ensuring that the following tasks are performed:
 - ✓ monitoring the efficacy of internal procedures designed to prevent the offence of false corporate communications;
 - ✓ examining any specific alerts coming from the auditing bodies or from an employee and carrying out such verification as is considered necessary or advisable as a consequence of same;
 - ✓ supervising and checking that the conditions for guaranteeing that the auditing firm enjoys real independence during its control functions are met;
- c) referring to the other risk activities:
 - ✓ regular checking of compliance with internal procedures;
 - ✓ periodic verification that communications are actually sent to the public regulatory authorities and that the procedures adopted during possible inspections carried out by the officials working for these authorities are complied with;
 - ✓ monitoring the efficacy of the procedures designed to prevent offences from being committed;
 - ✓ examining any specific alerts coming from the auditing bodies or from an employee and carrying out such verification as is considered necessary or advisable as a consequence of same.

Special Section “C”

Crimes of terrorism and subversion of democratic order

C.1 Types of crimes of terrorism and subversion of democratic order

As regards this special section C, article 25-quater of the Decree does not list all the crimes for which the company is responsible, but lists in the first subsection all the crimes named by the penal code and the special laws. The third subsection relates to all the crimes that are not in the first subsection but violate the provisions of article 2 of the New York Convention.

Below is a list of crimes present in the first subsection of article 25-quater:

Associations for acts of terrorism and subversion of democratic order (art. 270-bis penal code)

Anyone that promotes, instigates, organizes, directs or finances associations that propose actions of violence for the purposes of terrorism and subversion of democratic order is committing an offence under this law. Furthermore, anyone taking part in the above associations is similarly punishable. According to criminal law, these are considered acts of terrorism even when such crimes are committed against a foreign state, institution, or international organization.

Support to the associates (art 270-ter penal code)

Art. 270-ter was added which concerns support for such associations. It provides that besides cases of participation and support, anybody who gives refuge or food, hospitality, means of transportation or communication to a person participating in associations indicated in Art. 270 & 270-bis is committing an offence under this law.

As regards crimes included in special laws, Art. 1 of L. 6 February 1980, No. 15 states that an aggravating circumstance of any crime is when it is committed for the purposes of terrorism and subverting democratic order. As a result, any crime included in the penal code or in special laws, even those laws not directly related to punishing crimes of terrorism, if committed with this purpose, can become one of those implying the entity's responsibility, pursuant to Art. 25-quater.

The crimes in the third subsection of Art. 25-quater, which are included the Convention of New York, are crimes for financing, whether directly or indirectly but voluntarily, subjects that intend to commit crimes of terrorism. In particular, the Convention makes reference to crimes covered in other international conventions, such as: hijacking of aircraft, attacks against diplomatic staff, taking of hostages, illegal production of nuclear devices, hijacking of ships, setting off explosive devices, etc.

From a subjective point of view, crimes of terrorism are described as intentional. Therefore, for such a crime to be intentional, the person responsible must be fully aware of and intent on committing the crime. To be such, terrorism must therefore be viewed as intentional, because it is a conscious act.

C.2 Areas of Risk

With respect to the above mentioned criminal actions, for the purposes of the present special section “C” of the Model, the areas considered specifically most at risk are those relating to financial or commercial transactions realized by companies based in countries with high security risk or with other subjects - individuals or companies – with a risk of terrorist connections (as named in the “country lists” and the “lists of names” published by the “Ufficio Italiano Cambi”-Italian Exchange Bureau). There have been identified all those areas that could imply payments to subjects at risk, and this has included operations for identifying suppliers, management of personal data on the IT system, invoice processing and the corresponding payments and revenues. Details of these operations at risk are contained in an internal mapping document produced for implementing a management and control system for specific risks.

Special Section "C"

1. Supplier Data Management (data entry and update on the system in use)
2. Procurement of goods and services from third parties and within the group (operations for selecting, negotiating and posting purchase invoices in accounts)
3. Payment Management (financial expenses against goods and services supply)
4. Customer Data Management (data entry and update on the system in use)
5. Fixed and mobile telephone service contract management in favor of third parties and within the group (front-end and billing system data entry)
6. Revenue receipt management (activity related to non automated collection management)
7. Asset disposal and sale (buyer identification and contract drawing up)
8. Sales channels relationship management (commission management)
9. Revenue Sharing (reverse amount definition to be acknowledged to customers, accounting practice and payment of corresponding invoices)
10. Management of real estate leasing to use as offices and for technological use (identification of the owner of the real estate and contract drawing up)
11. Management of roaming, interconnection and wholesale agreements (identification, contract drawing up and invoice accounting)
12. Relations with the Judiciary (data transmission to magistrates)
13. Management of Libero Portal, I-mode platform and IPTV (management of portal and publication of contents).
14. Human Resources Management (selection, recruiting and administration)
15. Collecting charity funds through SMS (management of sums collected)

C.3 Recipients of the special section: General principles of conduct and performance

The present Special section refers to the conduct of administrators, auditors, liquidators, managers and employees of the company ("Corporate Personnel"), and external consultants and partners as already defined in the General section (all of these are considered as "Recipients").

The present special section has the function of:

- a) giving the above Recipients a list of general principles and specific procedures to adhere to for the correct application of the model.
- b) providing the CO, and the management structures of other CO company functions that work in association, the means to conduct the control, monitoring and verification operations necessary.

All the Recipients, in order to do their jobs, not only have to follow the procedures in the special section, but have to know and adhere to the rules and principles contained in the following documents:

- ✓ The Group's Code of Ethics;
- ✓ The corporate rules of governance;
- ✓ Supply chain management;
- ✓ All other documents that are related to the company's internal audit system.

The present special section expressly prohibits the above Recipients from the following (limited to the obligations included in the special procedures and in the codes of conduct adopted and to the obligations included in specific contract clauses):

- ✓ putting in place, cooperating with or being responsible for behaviour which – considered individually or collectively – includes the specific crime forming part of those considered above (Art. 25-quater of leg. dec. 231/2001);
- ✓ supplying, directly or indirectly, finance for subjects that intend to commit crimes contained in the present special section.
- ✓ providing services to consultants, partners, and suppliers which cannot be sufficiently justified within the context of the contractual relationship, or in relation to the type of task to complete.
- ✓ violating the principles and the company procedures detailed in the present special section.

Furthermore the company has adopted control procedures that guarantee the monitoring of trade operations or financial operations with residents in the countries at risk of terrorism, or whose names are contained in the Lists

Special Section "C"

of the Italian Exchange Bureau. Every operation that, by its intrinsic characteristics, could relate to such occurrences must be reported to the Compliance Officer beforehand for advice.

Below are shown the procedural principles that the Recipients must comply with and which may, where appropriate, be implemented in specific corporate procedures:

- 1) Every financial transaction must presume knowledge of who the beneficiary of the sum will be.
- 2) Operations that are considered 'significant' according to current procedures must be held with either a physical person or company whose suitability has been previously checked, controlled and ascertained;
- 3) For transactions with subjects at risk, the transaction must be suspended and submitted to the Compliance Officer's internal evaluation.
- 4) The data collected about relations with customers, consultants and partners must be complete and up to date to ensure correctly and rapidly identifying them and correctly evaluating their profile.
- 5) In contracts with partners, suppliers and consultants, there must be included a specific declaration stating that they have never been convicted or charged with crimes contained in the present special section, so that WIND may have greater information if a business or consultancy relationship is subsequently created.

C.4 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

C.5 The control systems

The control systems applicable to the activities selected were defined using as a benchmark the current guidelines from the main trade associations and the best international practices.

Below are the applicable control standards:

Separation of duties:

There must be a separation of duties between those who authorise, those who perform, those who enter in accounts and those who control a specific operation so that no one person will be in charge of managing an entire process alone.

Rules of conduct:

All operations must be formalised, highlighting the appropriate points of control. The operations must be regulated by a defined procedure and temporary events must at least comply with the principle of being verifiable.

Powers of authorization and signature:

The delegation and proxy system for the company's external activities must correspond to the organization and management responsibilities assigned, and include a precise threshold for approval of expenses.

- Traceability:** Every operation, transaction or action must be verifiable, documented, consistent and congruous so that it is possible to make checks at any time in order to endorse the motivation and the characteristics of the same.
- Notification of anomalies:** A system of management control must be in place able to identify any critical issues emerging
- Training and communication:** There must be put in place an employee training plan together with internal communication about the contents of the decree and the Model.

C.6 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through *adjustment proposals* to company functions able to actually implement them within the corporate structure, or by means of a *follow-up* to check that the solutions proposed have been implemented and actually work).

Special Section “D” Crimes against individuals

D.1 Types of crimes against individuals

Article 5 of law no. 228/2003, concerning measures against exploitation of people, adds Art. 25-quinquies to decree 231/01. This makes provision for applying fines to companies and associations for committing crimes against individual persons.

Art. 25-quinquies was later supplemented with Art. 10, law No. 38 of 6 February 2006 which contains “Dispositions concerning the fight against sexual exploitation of children and child pornography, including by means of the internet”, which modifies the applicable scope of child pornography crimes and possession of pornographic material (Art. 600-ter and 600-quater penal code) to also include the hypothesis that these crimes are committed with pornographic material using virtual images of minors under the age of 18 years or part of them (known as “virtual pedo-pornography”, according to the new art. 600-quater.1, penal code):

The aforementioned law No. 38/2006 has also modified the provisions of Art. 600-bis, 600-ter and 600-quater, concerning the crimes of child prostitution, child pornography and possession of pornographic material, for which entities already had administrative responsibility.

The crimes punished are:

Subjugating a person to slavery (art. 600 penal code)

This crime is committed by anyone who exerts what can be considered total proprietorial hold over another, and who reduces that person to a state of complete and continued subjection, forcing the person to provide work or sexual services, to beg for charity or in any other way be exploited. This crime is committed when forcing a person into slavery using violence, threats, deception, abuse of authority or taking advantage of physical or psychological inferiority, or through the promise of money or other benefits.

Child prostitution (Art. 600-bis penal code)

This crime is committed by anyone who forces into, encourages or procures prostitution of a person under the age of 18.

Child pornography (Art. 600-ter cp) and Virtual pornography (Art. 600-quater.1 penal code)

This crime is committed by anyone who, using minors below the age of 18, puts on pornographic exhibitions or produces pornographic material or otherwise induces minors to take part in pornographic exhibitions; also anyone who sells the above pornographic material shall be punished. This law also punishes anyone who distributes, discloses, spreads or advertises such type of pornography, including by electronic means, or who distributes or discloses information with the aim of sexually soliciting or exploiting minors; it is also an offence for anyone who, apart from the situations described above, knowingly offers or gives (even free of charge) pornographic material obtained by exploitation of minors. The crime is also committed when the images are displayed virtually, using images or part of images of minors (virtual pornography). An image is considered virtual if it is realized with graphic techniques not completely associated with real situations, but the results of which make them look like real situations.

Possession of pornographic material (Art. 600-quater penal code)

This crime is committed by anyone who, apart from the provisions of Art. 600-ter penal code, knowingly obtains or holds pornographic material of minors, even in the case of virtual pornography.

Tourism with the aim of exploiting child prostitution (Art. 600-quinques penal code)

This crime is committed by anyone that organizes or advertises trips with the aim of exploiting juveniles for prostitution.

Exploitation of persons (Art. 601 penal code)

This crime is committed by anyone who is using another person that is in the same conditions described in Art. 600 penal code: by this is meant, with the aim of committing the crimes described in the same article, inducing by deception, or forcing through violence, threats, abuse of authority or taking advantage of physical or psychological inferiority, or through the promise of money or other benefits, to enter or stay or leave the country or travel within it.

Trading in slaves (Art. 602 penal code)

This crime is committed by anyone who, outside the cases included in article 601 penal code, purchases or sells a person that is in the same conditions described in article 600 of the penal code. It is important to bear in mind that this crime is also committed by anyone who knowingly encourages it, even if only financially. This means that the company could commit the crime by making payments to third parties with the knowledge that such money may be used to commit this crime.

D.2 Areas of Risk

Regarding the criminal actions and behaviour described above, for the current special section "D" of the model, the areas considered most at risk are listed below. The details of these risk areas are contained in an internal mapping document prepared for implementing a management and control system for specific risks:

1. Management of Libero Portal, I-mode platform and IPTV (management of portal and publication of contents).
2. Human Resources Management (selection, recruiting and administration)
3. Management of informative systems (management of access to the intranet and or other internal networks)

D.3 Recipients of the special section: General principles of conduct and performance

The present Special section refers to the conduct of administrators, auditors, liquidators, managers and employees of the company ("Corporate Personnel"), and external consultants and partners as already defined in the General section (all of these are considered as "Recipients").

The present special section has the function of:

- a) Giving the above Recipients a list of general principles and specific procedures to adhere to for the correct application of the model.
- b) Providing the CO, and the management structures of other company functions that work in association, the means to conduct the control, monitoring and verification operations necessary.

While carrying out all the operations for corporate management, all Recipients must not only adhere to the rules of the present Model, but have to know in general and comply with all the rules and principles contained in the following documents:

- ✓ The Group's Code of Ethics;
- ✓ Corporate governance rules;
- ✓ The procedures for human resource hiring management
- ✓ The CNL (National Labour Agreement) for the group employees;
- ✓ The certification SA8000;
- ✓ Any other documentation relating to the company's internal auditing system

The present special section expressly prohibits the above Recipients from the following (limited to the obligations included in the specific procedures and in the codes of conduct adopted and to the obligations included in specific contract clauses):

- ✓ putting in place, collaborating or instigating behaviour that – considered individually or collectively - directly or indirectly includes the specific crime forming part of those considered above (Art. 25- quinquies of the leg. Dec. 231/2002).
- ✓ violating the principles or the procedures of the company included in this special section.

Special Section "D"

The following principles, with which the Recipients must comply, may be implemented - when considered appropriate - in specific corporate procedures:

- 1) Partners and vendors must be required to comply with the law regarding the protection of minors and women, including workplace conditions, hygiene, safety, trade union rights or the rights of association and representation required by the law of country where they work.
- 2) Selecting vendors, whether partners or suppliers, supplying specific services (i.e. companies that have numerous unskilled labourers employed), requires close and prior scrutiny that they are trustworthy.
- 3) In the contracts with partners, vendors, and consultants, there must be a declaration that they have never been convicted, charged with, or committed a crime under this special section, so there is total clarity for WIND in all subsequent relations with partners, vendors, and consultants
- 4) When the company directly employs staff, WIND must comply with all labour regulations and laws and trade union agreements as regards hiring and working relationships in general. It must also be ensured that the rules of correctness and good behaviour are maintained in the working environment and, in any case, all anomalous and abnormal working situations must be managed with all due care and attention possible.
- 5) In the case where a partner is working aboard for WIND, the partner must comply with the local laws and, if stricter, all ILO conventions on minimum age for access to work and on the worst forms of child employment ("C 138 convention of minimum age 1973" and "C 182 convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour")

D.4 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

D.5 The control systems

The control systems applicable to the activities selected were defined using as a benchmark the current guidelines from the main trade associations and the best international practices.

Below are the applicable control standards:

Separation of duties:

There must be a separation of duties between those who authorise, those who perform, those who enter in accounts and those who control a specific operation so that no one person will be in charge of managing an entire process alone.

Rules of conduct:

All operations must be formalised, highlighting the appropriate points of control. The operations must be regulated by a defined procedure and temporary events must at least comply with the principle of being verifiable.

Powers of authorization and signature:

The delegation and proxy system for the company's external activities must correspond to the organization and management responsibilities assigned, and include a precise threshold for approval of expenses.

Traceability:

Every operation, transaction or action must be verifiable, documented, consistent and congruous so that it is possible to make checks at any time in order to endorse the motivation and the characteristics of the same.

Notification of anomalies:

A system of management control must be in place able to identify any critical issues emerging

Training and communication:

There must be put in place an employee training plan together with internal communication about the contents of the decree and the Model.

D.6 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through *adjustment proposals* to company functions able to actually implement them within the corporate structure, or by means of a *follow-up* to check that the solutions proposed have been implemented and actually work).

Special Section “E” Market abuse crimes

E.1 The types of market abuse crimes

Art. 9 of Italian law No. 62, 18 April 2005, (EC law for 2004), implementing directive 2003/6/CE of the European Parliament and the Council of 28 January 2003, dealing with the abuse of privileged information, and with the manipulation of the market (so called market abuse) introduces art. 25-sexies into the decree 231/2001. This provision extends the scope of regulation of the administrative responsibility of the corporate body to behaviours to include conduct involving market abuse.

The system of sanctions for market abuse defined by the European Legislator is much more complex and it goes beyond the integration of the decree No. 231/2001. In fact, EU Law intervenes on both the civil code and the consolidated acts of financial brokerage (TUF).

The discipline for the responsibility of the entity has been split into two parts; in the case of alleged illicit act acquires criminal relevance, the responsibility of the entity will be assessed in court (Art. 25-sexies of decree No. 231/2001). If it is, instead, an administrative offence – to the benefit or advantage of the entity – the investigation and application of fines will be the responsibility of CONSOB (Art 187-septies of TUF).

Below are given the crimes stated by Art. 25-sexies of the decree.

Insider trading (Art. 184 TUF)

This crime is committed by anyone who, coming (directly) into possession of privileged information due to being a member of the board, of the management or controlling the entity or participation in its capital, or while performing work, a profession, or a function even public, or of a department:

- purchases, sells or performs other operations, directly or indirectly, on his own behalf or of a third party, on financial instruments using the same information – in other words, trading;
- communicates such information to others, outside of ordinary situations of work, profession, function or department to which they are dedicated (in whatever way the third parties actually use the information received – known as “tipping”).
- recommends or induces others, based on the information, to do the above mentioned operation – tuyautage

The above subjects, as a result of their direct access to the source of the privileged information, are called primary insiders. In addition to these subjects the new Art. 184 TUF extends the prohibitions of trading, tipping, tuyautage to whoever has acquired privileged information with the purpose of preparing or putting in place criminal activities – so called criminal insider (i.e. the hacker who obtains price sensitive information).

Market Manipulation (Art. 185 TUF)

This crime is committed by anyone who circulates false information (so called stock manipulation) or simulates transactions or other devices able to provoke serious alteration of the financial instrument price (so called operational stock manipulation). With reference to the circulation of the false or misleading information, this type of market manipulation also includes the cases which creation of misleading information comes from non-compliance with the obligations of communications by the issuer or other subjects or by omission.

Below are the crimes referred to in Art. 187-*quinques* TUF:

Administrative offence of abuse of privileged information (Art. 187-*bis* TUF):

This type of crime differs from market abuse cases because there must be seen, in the active subject, the intent of fraud. Furthermore the prohibition on trading, tipping, and tuyautage also applies to those subjects who,

Special Section "E"

coming into possession of information, knew or could have possibly known, with normal due diligence, about the privileged nature of this information (secondary insider).

Lastly, it is pointed out that even the simple attempt to commit any of the above acts can be subject to such rules, because it is considered having committed the deed.

Administrative offence of market manipulation (art. 187-ter TUF):

Such criminal cases includes, among others:

- operations or trading orders which can provide or can lead to give false indications or, give misleading information's either on price, demand and supply of financial instruments.
- operations or trading orders which allow, through the action of a person or several persons jointly, to fix the market price of one or more financial instruments at an abnormal or artificial level.
- operations or trading orders that use artifice or any other kind of deception or expedient
- other devices able to mislead about supply, demand or financial instruments price.

With the two first cases, a person who can demonstrate having acted lawfully in accordance with the best practice of the market concerned, cannot be the subject of an administrative fine.

As regards the notion of privileged information (price sensitive information i.e. information which, if published, could seriously affect the financial instrument's price), Art 181 TUF means information that a reasonable investor would use, among others, to plan his own investment decisions.

Regarding the notion of financial instrument, below are some of the elements stated in Art. 180 Tuf (for the complete list, refer to Art. 1, sub-section 2 in TUF):

- stocks or other shares representative of equity capital negotiable on the capital market.
- bonds, government securities or other securities negotiable on the capital market.
- futures on financial instruments, on interest rates, on currencies, on goods and their index, even when the execution of the order takes place by paying the balance in cash.
- swaps on interest rates on currencies, on goods and on equity swaps, even when the execution of the order takes place by paying the balance in cash.

E.2 Risk Areas

In relation to crimes and to the misconducts mentioned above, for the purpose of the present Special Section "E" of the Model, the area specifically considered at risk is as follows:

1. transaction on financial instruments

E.3 Special Section recipients: general principles of behaviour and implementation

The present special section deals with the conduct of administrators, auditors, liquidators, directors and employees ("Corporate Personnel") of the company, as well as external consultants and partners, as already defined in the special section (all hereafter defined "Recipients").

In particular the following special section has the function of:

- a) providing a list of the general principles and of specific procedures which must be adhered to by the Recipients, for the correct implementation of the model,
- b) providing the CO, and the management structures of other company functions working in association, the operative instruments for conducting the control, monitoring and verification operations necessary.

While carrying out all the operations for corporate management, all Recipients must not only adhere to the rules of the present Model, but have to know in general and comply with all the rules and principles contained in the following documents:

- ✓ The Group's Code of Ethics;
- ✓ Corporate governance rules;
- ✓ The procedures for management for financial disclosure and external communication of privileged information.
- ✓ Every other document relating to the company's internal audit system.

Special Section "E"

The present special section expressly prohibits the above Recipients from the following (limited to the obligations included in the specific procedures and in the codes of conduct adopted, and to the obligations included in specific contract clauses):

- ✓ putting into effect, collaborating or being the source of the behaviour which – considered individually or collectively - constitutes, directly or indirectly, a criminal offence according to the above mentioned laws. (Art. 25-sexies of Lgs. Dec. 231/2001);
- ✓ violating the principles and procedures included in the present special section.

With the purpose of avoiding such crimes as per leg. Dec. 231/01, for all the recipients of the present special section it is prohibited to:

- 1) Use privileged information, as defined in the company procedures created for this purpose, acquired as a result of their duties or position inside the group or company, for the purposes of negotiating, directly or indirectly, shares or financial instruments of the company, customer or competitors companies, other companies, or in any way that may lead to personal advantage, or for that of third parties, or the company or other intergroup companies.
- 2) Disclose privileged information about the Group to third parties, except for where required by law, other regulatory provisions, or specific contractual agreements with counterparts who have undertaken to use such information exclusively for the purpose for which the information was provided, and to maintain confidentiality.
- 3) conclude operations or give orders in such a way as to prevent the market prices of the Group's financial instruments from dropping under a certain plateau, principally to avoid the negative consequences coming from the related reduction of the financial ratings. This behaviour is to be kept distinct from transactions regarding the programme for purchasing own shares, or the stabilization of financial instruments as permitted by law.
- 4) Spread false or misleading market information through media, internet, or any other medium.

E.4 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

E.5 The control systems

The control systems applicable to the activities selected were defined using as a benchmark the current guidelines from the main trade associations and the best international practices.

Below are the applicable control standards:

Separation of duties:

There must be a separation of duties between those who authorise, those who perform, those who enter in accounts and those who control a specific operation so that no one person will be in charge of managing an entire process alone.

Special Section "E"

Rules of conduct:	All operations must be formalised, highlighting the appropriate points of control. The operations must be regulated by a defined procedure and temporary events must at least comply with the principle of being verifiable.
Powers of authorization and signature:	The delegation and proxy system for the company's external activities must correspond to the organization and management responsibilities assigned, and include a precise threshold for approval of expenses.
Traceability:	Every operation, transaction or action must be verifiable, documented, consistent and congruous so that it is possible to make checks at any time in order to endorse the motivation and the characteristics of the same.
Notification of anomalies:	A system of management control must be in place able to identify any critical issues emerging
Training and communication:	There must be put in place an employee training plan together with internal communication about the contents of the decree and the Model.

E.6 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through *adjustment proposals* to company functions able to actually implement them within the corporate structure, or by means of a *follow-up* to check that the solutions proposed have been implemented and actually work).

Special Section “F”

Crimes in violation of accident prevention rules and the protection of health and hygiene in the work place.

F.1 The types of crimes in violation of accident prevention rules and the protection of health and hygiene in the work place are listed below:

As regards the present special section “F”, below is the list of crimes included, as stated in Art. No. 25-septies of the decree.

Manslaughter (art. 589 penal code)

The crime of unintentionally causing a person's death.

Unintentional personal injury (art. 590 penal code)

The crime of seriously or particularly seriously injuring a person without intention. The injury is considered serious if it has occurred in the following areas; a) the injury is an illness that puts the person's life in danger or makes the person unable to work for a period over 40 days; b) the damage is permanent to a single internal organ, or sensory organ (Art. 583, subsection 1, penal code).

The injury is considered particularly serious if causing a) an illness that is probably or certainly permanent, b) the loss of a sensory organ, c) the loss of a limb or a mutilation making the limb unusable, or the loss of use of an internal organ or the ability to procreate, or permanent loss or grave impediments to speech, d) permanent deformity of the face, in part or total (Art. 583, subsection 2, penal code).

For the purposes of integrating the above crimes, it is not necessary to prove malice or awareness and intention to cause the injury, but just negligence, imprudence, lack of experience of the active subject or failure to comply with laws, regulations, orders or procedures (Art. 43 penal code).

The applicability of these crimes to WIND is directly established by the law as specified in Articles 3 & 30 of leg. Dec. 81/2008 (Testo Unico sulla Sicurezza sul Lavoro – Consolidated Text on Safety at Work):

Field of application (Art. 3)

1. The present legislative decree is applied to all companies, public or private, and all types of risks.

There is just one essential and unifying element in the various and possible forms of responsibility by the employer as regards applying Art. 25-septies of Leg. Dec 231/2001, which is the failure to adopt all the safety and prevention methods technically available that can be implemented (as specified in Art. 3, subsection 1, b), of the leg. Dec. 626/1994) resulting from the experience and the latest technical and scientific knowledge.

The responsibility of the employer is not only guaranteeing the correct implementation of the regulations, but also means informing and training employees about the relevant risks in the work place, and about all the safety equipment required to prevent or minimise risks of injury.

Management and organization Models (Art. 30)

1. The model of organization and management suitable for ensuring effective administrative responsibility (...) as per Leg. dec 8 July 2001, No. 231, must be adopted and properly implemented, ensuring a company system for fulfilling all the relevant legal obligations.

5. On first application, the organisation models considered in compliance with the guidelines from UNI-INAIL (...) or British Standard OHSAS 18001:2007 are presumed to comply with the requirements of the previous paragraphs for the corresponding parts.

F.2 Risk areas

All the areas of the company that have a potential exposure to risk of non compliance with the regulations about health and safety in the workplace

F.3 Special Section recipients: general principles of behaviour and implementation

The present special section deals with the conduct of administrators, auditors, liquidators, director, and employees ("Corporate Personnel") of the company, as well as external consultants and partners, as already defined in the special section (all hereafter defined "Recipients").

The Recipients must generally know and comply with all the rules and principles contained in the following documents:

- ✓ The Group's Code of Ethics;
- ✓ Corporate governance rules;
- ✓ The regulations on protecting health and safety in the workplace.
- ✓ Certification OHSAS 18001;
- ✓ Every other document relating to the company's internal audit system.

The present special section expressly prohibits the above Recipients from the following (limited to the obligations included in the specific procedures and in the codes of conduct adopted, and to the obligations included in specific contract clauses):

- ✓ putting into effect, collaborating or being the source of the behaviour which – considered individually or collectively - constitutes, directly or indirectly, a criminal offence according to the above mentioned laws (Art. 25-*septies* of Lgs. Dec. 231/2001);
- ✓ violating the principles and procedures included in the present special section.

WIND has a company structure that is responsible for compliance with the regulations on protecting health and safety in the workplace, to eliminate or reduce and, thus, manage all risks in the workplace for all its employees. WIND has also defined all the roles of responsibility in protecting health and safety in the workplace, from the employer right through to the individual employee.

For the general principles of conduct, reference is made to the General Document of Risk Valuation conforming to leg. Dec 81/08, and all other internal rules about health and safety in the workplace (also prepared for the purposes of securing the OHSAS 18001 certificate) published in the company intranet.

F.4 Activities area at risk: Appointing the internal person in charge.

In relation to crimes of this sort, with a view to creating an integrated control system, reference should be made to the Person responsible for prevention and protection services (RSPP) who is responsible for the technical and operative controls (or first grade control). The other institution that has responsibility for the efficiency and effectiveness of the procedures is the "Organismo di Vigilanza-Supervisory Body", as required by leg. Dec. No. 231/2001 (or second grade control).

F.5 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform

Special Section "F"

supervisory functions;

- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

F.6 The control systems

The control systems applicable to the activities selected were defined using as a benchmark the current guidelines from the main trade associations and the best international practices.

Below are the applicable control standards:

Separation of duties:	There must be a separation of duties between those who authorise, those who perform, those who enter in accounts and those who control a specific operation so that no one person will be in charge of managing an entire process alone.
Rules of conduct:	All operations must be formalised, highlighting the appropriate points of control. The operations must be regulated by a defined procedure and temporary events must at least comply with the principle of being verifiable.
Powers of authorization and signature:	The delegation and proxy system for the company's external activities must correspond to the organization and management responsibilities assigned, and include a precise threshold for approval of expenses.
Traceability:	Every operation, transaction or action must be verifiable, documented, consistent and congruous so that it is possible to make checks at any time in order to endorse the motivation and the characteristics of the same.
Notification of anomalies:	A system of management control must be in place able to identify any critical issues emerging
Training and communication:	There must be put in place an employee training plan together with internal communication about the contents of the decree and the Model.

F.7 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through *adjustment proposals* to company functions able to actually implement them within the corporate structure, or by means of a *follow-up* to check that the solutions proposed have been implemented and actually work).

In order to guarantee periodical monitoring of the correct implementation of the prevention system adopted by WIND, the Compliance Officer must receive a copy of the periodical report on the subject of health and safety in

Special Section "F"

the workplace and, particularly, all minutes of the periodical meeting as per Art. 35 of TU, and all data about incidents that have occurred within the company.

Special Section “G” Crimes of receiving, laundering and using money, goods or benefits of illicit origin

G.1 Types of offences in receiving, laundering and using money, goods or benefits of illicit origin

Legislative Decree n. 231/2007 (in force from 29 December 2007) implemented the Directive 2005/60/EC of the European Parliament and of the Council dated 26 October 2005, concerning the prevention of the use of the financial system for the purpose of laundering the proceeds of criminal activities and for financing terrorism (Third EU Money Laundering Directive), as well as Directive 2006/70/EC which established measures of execution.

The new set of rules simplifies the complex Italian anti-money laundering regulations.

Art. 64 subsection 63 of Legislative Decree n. 231/2007 introduces in this Decree the new Art. 25-octies, which extends administrative responsibility of Companies to the offences of receiving, laundering and using money, goods or benefits of illicit origin.

More in detail, the following articles are cited:

Receiving (art. 648 Italian Criminal Code)

This offence is committed by those individuals who - aside from accessory acts to the crime - acquire, receive or hide money or goods deriving from any crime whatsoever to obtain profit for themselves or others, or who at any rate become involved in the acquisition, receipt or hiding of these monies or goods.

In order to correctly define the crime of receiving stolen goods, the doctrine deems necessary the knowledge on the part of the author of the “illegal origin” of the monies and the goods being received and the presence of “specific” malice on the part of those who act, that is to say the knowledge and the will to draw profit (even though not patrimonial), for themselves or others, from the acquisition, receipt or hiding of goods of illegal origin.

Money-laundering (Art. 648-bis Italian Criminal Code)

This offence is committed when a person, aside from accessory acts to the crime, substitutes or transfers money, goods or other services deriving from a non-negligent offence, or who carries out other operations in this regard, so as to impede the identification of their illegal origin.

As for the offence of receiving, the money, assets or other proceeds (the provision covers fixed assets, companies, bonds, credit rights etc.) must be the product of some unintentional offence (i.e. fiscal crimes, crimes against patrimony, etc.), not subsequently specified.

In order to correctly define this crime, the doctrine deems necessary the knowledge of the illegal provenance of the asset and performance of the prohibited conduct.

Use of money, goods or benefits of illicit origin (Art. 648-ter Italian Criminal Code)

Article 648-ter P.C. punishes, aside from accessory acts to the crime (i.e. theft, fiscal crimes, forgery, etc.) and cases pursuant to Articles 648 and 648-bis, those individuals who use in economic or financial activities money, assets or other proceeds of illegal origin.

From a subjective point of view, the doctrine deems necessary the knowledge of the illegal provenance of the asset and performance of the prohibited conduct.

G.2 Areas at risk

With reference to the abovementioned offences, the areas of activity which can more specifically be considered at risk in relation to this Special Section “G” of the Model, are: those areas in which financial expenses in favor of risky subjects could take place, including selection of suppliers, IT data management, billing and correspondent payments and cashing. The following detail of activities at risk are mapped in a document drawn up to implement the risk control and management system described in the this Special Section:

Special Section "G"

1. Supplier Data Management (data entry and update on the system in use)
2. Procurement of goods and services from third parties and within the group (operations for selecting, negotiating and posting purchase invoices in accounts)
3. Payment Management (financial expenses against goods and services supply)
4. Customer Data Management (data entry and update on the system in use)
5. Fixed and mobile telephone service contract management in favor of third parties and within the group (front-end and billing system data entry)
6. Revenue receipt management (activity related to non automated collection management)
7. Asset disposal and sale (buyer identification and contract drawing up)
8. Sales channels relationship management (commission management)
9. Revenue Sharing (reverse amount definition to be acknowledged to customers, accounting practice and payment of corresponding invoices)
10. Management of real estate leasing to use as offices and for technological use (identification of the owner of the real estate and contract drawing up)
11. Management of roaming, interconnection and wholesale agreements (identification, contract drawing up and invoice accounting)
12. Human Resources Management (selection, recruiting and administration)
13. Collecting charity funds through SMS (management of sums collected)

G.3 Recipients of the Special Section: general behavioral principles and implementation

This Special Section refers to conduct on the part of directors, senior executives and employees ("Corporate Personnel") and also refers to Outside Contractors and Partners, as already defined in the General Part (herein below all defined as "Recipients").

More specifically, the purpose of this Special Section is to:

- a) Provide a list of general principles and procedures which the Recipients are required to comply with in order for the Model to be correctly applied.
- b) Provide the CO, and the heads of the other corporate functions called on to cooperate with the CO, with the operational tools to carry out required control activities, monitoring and verification.

In carrying out all the operations pertaining to operating activities, in addition to the rules set out in this Model, the Recipients must, generally speaking, know and comply with all the rules and principles contained in the following documents:

- ✓ Group's Code of Ethics;
- ✓ Corporate Governance rules;
- ✓ Suppliers Management procedure;
- ✓ all other documentation relating to the internal control system in use in the Company.

This Special Section places an express prohibition on all Recipients, as identified above (restricted to the obligations stated in the specific procedures and in the codes of conduct adopted and the obligations set forth in the specific contractual clauses) from:

- ✓ behaving in such a manner, or collaborating or causing such behavior as – considered either individually or collectively – amounts, directly or indirectly, to one of the offences included in the abovementioned offences;
- ✓ breaching the corporate principles and procedures provided for in this Special Section.

The following principles, with which the Recipients must comply, may be implemented - when considered appropriate - in specific corporate procedures:

- 1) agreements with consultants, suppliers, commercial Partners and all other counterparty (also in the case of foreign counterparties and companies belonging to the same Group) are subject to the principles of transparency, correctness and loyalty;
- 2) with reference to trade correctness and professionalism, the Company shall require all necessary information and will take all suitable measures;
- 3) agreements with Partners, suppliers and consultants must contain a special clause in which they declare

Special Section "G"

that they have never been implicated in legal actions involving the Criminal Offences set out in this Special Section, so that WIND may exercise greater caution if a consulting or partnership relationship is established.

- 4) all assignments to service companies and physical persons in charge of promoting and favoring the economic and financial interests of the Company must be recorded in writing, and include details on the agreed contents and economic terms;
- 5) competent functions must guarantee that regular payments are made in favor of all counterparties (including Companies belonging to the same Group); more in detail the subject who cashes the relative amounts must coincide with the subject to whom the order is payable;
- 6) With reference to financial management and payments to third parties and companies belonging to the Group, formal and substantial control must be guaranteed (counterpart's head office, banking intermediaries, trust companies must be verified).

G.4 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

G.5 The control systems

The control systems applicable to the activities selected were defined using as a benchmark the current guidelines from the main trade associations and the best international practices.

Below are the applicable control standards:

Separation of duties:	There must be a separation of duties between those who authorise, those who perform, those who enter in accounts and those who control a specific operation so that no one person will be in charge of managing an entire process alone.
Rules of conduct:	All operations must be formalised, highlighting the appropriate points of control. The operations must be regulated by a defined procedure and temporary events must at least comply with the principle of being verifiable.
Powers of authorization and signature:	The delegation and proxy system for the company's external activities must be correspond to the organization and management responsibilities assigned, and include a precise threshold for approval of expenses.
Traceability:	Every operation, transaction or action must be verifiable, documented, consistent and congruous so that it is possible to make checks at any time

in order to endorse the motivation and the characteristics of the same.

Notification of anomalies: A system of management control must be in place able to identify any critical issues emerging

Training and communication: There must be put in place an employee training plan together with internal communication about the contents of the decree and the Model.

G.6 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through *adjustment proposals* to company functions able to actually implement them within the corporate structure, or by means of a *follow-up* to check that the solutions proposed have been implemented and actually work).

Special Section "H" Transnational Crimes

H.1 Types of Transnational Offences

Law no. 146 of 16 March 2006 "ratifying and executing the Convention and Protocols of the United Nations against transnational organized crime, adopted by the general Assembly on 15 November 2000 and 31 May 2001", extends administrative responsibility of companies to transnational criminal offences.

The purpose of the United Nations Convention against Transnational Organized Crime ratified by Law no. 146 of 16 March 2006, is to promote cooperation between states to prevent and combat transnational organized crime more effectively.

Within the definition of Transnational Crimes, the Legislative Decree n. 231/2001 concerning the administrative responsibility of companies refers to crimes indicated by article 10 of Law no. 146 of 16 March 2006: association to commit offences, aiding and abetting of illegal immigration and obstruction of justice, when expressly committed in the interest or to the advantage of the company by individuals in top positions and under the command of others.

With the approval of Legislative Decree, the administrative responsibility of companies is extended to the following offences: receipt of stolen property, money-laundering, and the use of money, assets or profits of illicit origin regardless of whether the case involves transnational elements or is purely domestic.

Art. 10 of the Law against Transnational Organized Crime requires Legislative Decree n. 231/2001 to apply its provisions to the new administrative offences legal entities can be held liable for.

An offence is transnational in nature if it involves an organized criminal group and:

- it is committed in more than one State;
- it is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
- it is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State, or
- it is committed in one State but has substantial effects in another State.

The Offences that can take place are the following:

Association to commit crimes (Art. 416 of the Italian Criminal Code)

This offence is envisaged when three or more persons associate for the purpose of committing crimes.

Mafia-type Association (Art. 416-bis of the Italian Criminal Code)

This offense is said to exist when three or more persons take advantage of the intimidating power of the association and of the resulting condition of submission and silence to commit criminal offences, to manage, at all levels, control, either directly or indirectly, of economic activities, concessions, authorizations, public contracts and services, or to obtain unlawful profits or advantages for themselves or for others, or with a view to preventing or limiting the freedom to vote, or to get votes for themselves or for others on the occasion of an election.

Trafficking in migrants (Art. 12 paragraphs 3, 3-bis, 3-ter, and 5 of Legislative Decree no. 286/1998)

This offense is committed when a person commits acts aimed at bringing a person into national territory in violation of immigration laws or at facilitating a foreigner's illegal stay in a state, or acts aimed at procuring illegal entry in another state where the person is not a citizen or does not have authorization for permanent residence.

Inducement not to make statements or to make false statements to judicial authorities (Art. 377-bis Italian Criminal Code)

This offense is committed when a person uses offensive or persuasive actions to induce another person to make false statements in criminal proceedings.

Assisting an offender (Art. 378 Italian Criminal Code)

This offence is envisaged when a person is helped to avoid investigation or avoid searches by the authorities.

H.2 Areas at risk

With reference to the abovementioned offences, the areas of activity which can more specifically be considered at risk in relation to this Special Section "H" of the Model, are: those areas in which financial payments in favor of risk-prone subjects could take place, including when selecting suppliers, IT data management, billing and correspondent payments and cashing. The following detail of activities at risk is mapped in a document drawn up to implement the risk control and management system described in this Special Part:

1. Supplier Data Management (data entry and update on the system in use)
2. Procurement of goods and services from third parties and within the group (operations for selecting, negotiating and posting purchase invoices in accounts)
3. Payment Management (financial expenses against goods and services supply)
4. Customer Data Management (data entry and update on the system in use)
5. Fixed and mobile telephone service contract management in favor of third parties and within the group (front-end and billing system data entry)
6. Revenue receipt management (activity related to non automated collection management)
7. Asset disposal and sale (buyer identification and contract drawing up)
8. Sales channels relationship management (commission management)
9. Revenue Sharing (reverse amount definition to be acknowledged to customers, accounting practice and payment of corresponding invoices)
10. Management of real estate leasing to use as offices and for technological use (identification of the owner of the real estate and contract drawing up)
11. Management of roaming, interconnection and wholesale agreements (identification, contract drawing up and invoice accounting)
12. Relations with the Judiciary (data transmission to magistrates)
13. Management of Libero Portal, I-mode platform and IPTV (management of portal and publication of contents).
14. Human Resources Management (selection, recruiting and administration)
15. Collecting charity funds through SMS (management of sums collected)

H.3 Recipients of the Special Section: general behavioral principles and implementation

This Special Section refers to conduct on the part of directors, senior executives and employees ("Corporate Personnel") and also refers to Outside Contractors and Partners, as already defined in the General Part (here in below all defined as "Recipients").

More specifically, the purpose of this Special Part is to:

- a) Provide a list of general principles and procedures which the Recipients are required to comply with in order for the Model to be correctly applied.
- b) Provide the CO, and the heads of the other corporate functions called on to cooperate with the CO, with the operational tools to carry out required control activities, monitoring and verification.

In carrying out all the operations pertaining to operating activities, in addition to the rules set out in this Model, the Recipients must, generally speaking, know and comply with all the rules and principles contained in the following documents:

- ✓ Group's Code of Ethics;
- ✓ Corporate Governance rules;
- ✓ Suppliers Management procedure;
- ✓ all other documentation relating to the internal control system in use in the Company.

Special Section "H"

This Special Part places an express prohibition on all Recipients, as identified above (restricted to the obligations stated in the specific procedures and in the codes of conduct adopted and the obligations set forth in the specific contractual clauses) from:

- ✓ behaving in such a manner, or collaborating or causing such behavior as – considered either individually or collectively – amounts, directly or indirectly, to one of the offences included in the abovementioned offences;
- ✓ supplying, directly or indirectly, funds benefiting individuals that intend to commit offences mentioned in this Special Part;
- ✓ performing services in favor of Service Companies, Consultants, and Partners that are not adequately justified in the context of the contractual relationship established with them;
- ✓ breaching the corporate principles and procedures provided for in this Special Part.

Furthermore, the company adopts control measures aimed to guarantee the monitoring of commercial and/or financial transactions with subjects who either reside in countries at risk of terrorism or are listed by the Bank of Italy (UIF). These kinds of operations must be notified to and approved by the Compliance Officer.

The following principles, with which the Recipients must comply, may be implemented - when considered appropriate - in specific corporate procedures:

- 1) the amount of all financial transactions must be notified to the beneficiary;
- 2) operations that are considered significant, according to the procedure in force, must be carried out with physical persons and legal entities previously verified, checked and investigated;
- 3) collection of data concerning relationships established with clients, consultants and Partners must be complete and updated in order to correctly and immediately identify the aforesaid parties and to effectively assess their profile;
- 4) agreements with Partners, suppliers and consultants must contain a special clause in which they declare that they have never been implicated in legal actions involving the Criminal Offenses set out in this Special Part, so that WIND may exercise greater caution if a consulting or partnership relationship is established.

H.4 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the Compliance Officer ("Internal Sub-Responsible").

H.5 The control systems

The control systems applicable to the activities selected were defined using as a benchmark the current guidelines from the main trade associations and the best international practices.

Below are the applicable control standards:

Separation of duties: There must be a separation of duties between those who authorise, those

Special Section "H"

who perform, those who enter in accounts and those who control a specific operation so that no one person will be in charge of managing an entire process alone.

Rules of conduct:

All operations must be formalised, highlighting the appropriate points of control. The operations must be regulated by a defined procedure and temporary events must at least comply with the principle of being verifiable.

Powers of authorization and signature:

The delegation and proxy system for the company's external activities must correspond to the organization and management responsibilities assigned, and include a precise threshold for approval of expenses.

Traceability:

Every operation, transaction or action must be verifiable, documented, consistent and congruous so that it is possible to make checks at any time in order to endorse the motivation and the characteristics of the same.

Notification of anomalies:

A system of management control must be in place able to identify any critical issues emerging

Training and communication:

There must be put in place an employee training plan together with internal communication about the contents of the decree and the Model.

H.6 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through *adjustment proposals* to company functions able to actually implement them within the corporate structure, or by means of a *follow-up* to check that the solutions proposed have been implemented and actually work).

Special Section "I" Computer Crimes

I.1 Computer Crimes typology

Knowledge of the structure and execution modalities of the crimes, the commission of which by persons qualified ex Article 5 of Legislative Decree No. 231/2001, connected with the regime of responsibility pertaining to the company, is functional to prevention of those crimes and thus to the entire control system foreseen by that Decree. To this end a brief description of the crimes of which at Article 24-b of Legislative Decree No. 231/2001 (Computer Crimes and Illicit Data Processing) is provided below.

Fraud in IT documents (Article 491-b of the Italian Penal Code)

This crime extends the penal indictability of the crimes indicated at Book II, Title VII, Section III of the Italian Penal Code, that is the hypotheses of falsehood, material or ideological, committed in public deeds, certificates, permits, private agreements or private deeds by a representative of the Public Administration of a private individual, where the same refer to an "IT document with probatory effect", that is an IT document complete with at least a simple digital signature. "IT document" indicates the electronic representation of legally significant deeds, facts or data (Article 1, c.1, letter p, Law No. 82/2005).

Illicit access to an IT or telecommunications system (Article 615-3rd)

This disposition punishes the conduct of those who abusively penetrate, that is avoiding any form, albeit minimal, of barrier against access, an IT or telecommunications system protected by security measures, that is they remain therein against the will of those with the right to exclude them.

Illicit detention and diffusion of access codes for IT or telecommunications system (Article 615-4th)

This disposition punishes the conduct of those who illicitly procure, reproduce, divulge, communication or consign codes, key words or other means suitable to provide access to an IT or telecommunications system protected by security measures or who, in any manner, provides indications or instructions in this sense, in order to procure a profit for themselves or others or to damage another party.

Diffusion of equipment, devices or IT programmes intended to damage or interrupt an IT or telecommunications system (Article 615-5th)

This norm punishes the conduct of those who, to illegally damage an IT or telecommunications system, or indeed the information, data or programmes hosted thereon or pertaining thereto, or indeed to favour the interruption or alteration of the function thereof, procures, produces, imports, divulges, communicates, delivers or in any manner makes available to others equipment, devices or IT programmes.

Illegal interception, impediment or interruption of IT or telecommunications communications (Article 617-4th)

This norm punishes the conduct of those who, fraudulently, intercept communications about an IT or telecommunications system or between the several systems, impedes or interrupts the same or reveals, by any public information medium, wholly or partially, the content of the said communications.

Installation of devices intended to intercept, impede or IT or telecommunications communications (Article 617-5th)

This norm punishes the conduct of those who, except as legally permitted, installs devices intended to intercept, impede or interrupt communications relative to an IT or telecommunications system, or between such systems.

Damaging IT information, data and programmes (Article 635-bis)

This norm punishes the conduct of those who destroy, deteriorate, delete, alter or suppress someone else's IT information, data or programmes, except where this act may constitute a more serious crime.

Damaging IT information, data and programmes used by the State or other public authority, or, in any manner of use to the public (Article 635-3rd)

This norm punishes the conduct of those who act to directly destroy, deteriorate, delete, alter or suppress IT information, data or programmes used by the state or another public authority or pertaining thereto, or, in any case, of public utility, except where this act may constitute a more serious crime.

Damaging IT or telecommunications systems (Article 635-4th)

This norm punishes the conduct of those who, with the conduct of which at Article 635-b, that is by the introduction or transmission of data, information or programmes, destroys, damages, renders unserviceable, wholly or partially someone else's IT or telecommunications systems or seriously impedes their function, except where this act may constitute a more serious crime.

Damaging IT or telecommunications systems of public utility (Article 635-5th)

This norm punishes the conduct described at Article 635-4th, where intended to destroy, damage, render unserviceable, wholly or partially IT or telecommunications system of public utility seriously impede their function.

IT fraud by an actor providing digital signature certification services (Article 640- 5th)

This norm punishes those who provide digital signature certification services when these, in order to procure illicit profit for themselves or others or to cause damages to others, breaches the obligations established by law for the release of a qualified certificate.

This latter crime cannot be applied given that Wind does not provide digital signature certification services.

I.2 Risk Areas

In the light of the legislative innovation illustrated and considering the activities undertaken by the company, the business activities listed below may be considered sensitive with respect to the crimes of which at Article 25-8th, of Legislative Decree No. 231/2001:

1. Management of access, accounts and profiles. This is an articulated series of activities undertaken to regulate the typology of access to the data, systems and applications considered critical or sensitive to impede access by unauthorised persons.
2. Telecommunications network management. Activities connected with the management/operation and maintenance of telecommunications networks and the implementation of security measures to guarantee the confidentiality of information, as well as monitoring events on the network to identify anomalous access and/or usage and to define corrective action rapidly.
3. Hardware systems management. This is a series of activities addressing the identification, implementation, maintenance and monitoring the hardware components used by the Company.
4. Software systems management. The activities connected with the identification, development, maintenance and monitoring of the software systems used by the Company.
5. Management of physical access to the sites which host IT infrastructures. A series of articulated activities addresses the definition of physical security measures implemented to impeded unauthorised access to the physical sites which host IT infrastructures.
6. Digital format documentation management and security. The management of cryptography techniques applied to IT documentation and definition of the methodologies, archiving timing and conservation of digital format documents.

I.3 Recipients of the Special Section: general behavioral principles and implementation

This Special Section refers to conduct on the part of directors, senior executives and employees ("Corporate Personnel") and also refers to Outside Contractors and Partners, as already defined in the General Part (herein below all defined as "Recipients").

More specifically, the purpose of this Special Section is to:

- c) Provide a list of general principles and procedures which the Recipients are required to comply with in order for the Model to be correctly applied.

Special Section "I"

- d) Provide the CO, and the heads of the other corporate functions called on to cooperate with the CO, with the operational tools to carry out required control activities, monitoring and verification.

In carrying out all the operations pertaining to operating activities, in addition to the rules set out in this Model, the Recipients must, generally speaking, know and comply with all the rules and principles contained in the following documents:

- ✓ Group's Code of Ethics;
- ✓ Corporate Governance rules;
- ✓ procedures of usage of IT resources
- ✓ all other documentation relating to the internal control system in use in the Company.

The present special section expressly prohibits the above Recipients from the following (limited to the obligations included in the special procedures and in the codes of conduct adopted and to the obligations included in specific contract clauses):

- ✓ putting in place, cooperating with or being responsible for behaviour which – considered individually or collectively – includes the specific crime forming part of those considered above (Art. 25-quater of leg. dec. 231/2001);
- ✓ supplying, directly or indirectly, finance for subjects that intend to commit crimes contained in the present special section.
- ✓ providing services to consultants, partners, and suppliers which cannot be sufficiently justified within the context of the contractual relationship, or in relation to the type of task to complete.
- ✓ violating the principles and the company procedures detailed in the present special section.

I.4 Activity areas at risk: appointing the Internal Responsible

For the identified risk area the C.E.O. or a delegated senior executive, by the C.E.O. appoints an internal resource (the Internal Responsible).

The Internal Responsible:

- ✓ becomes the person in charge and has responsibility with regard to risk activities;
- ✓ within the framework of risk areas within his or her remit, he or she is responsible for ensuring compliance with the reference principals outlined in the Model and is responsible for correct implementation of the control system;
- ✓ he or she works closely with the CO, undertaking all such activities as are required in order to perform supervisory functions;
- ✓ he or she promptly notifies the CO of any conduct detected which is not consistent with the rules of conduct adopted in accordance with the principles contained in the Model.

All Internal Responsible can delegate the operational activities to the people in charge whom he or she designates, notifying the CO ("Internal Sub-Responsible").

I.5 Control Protocols

The system of controls implemented by the Company on the basis of the indication provided by international standards such as ISO 27001 and international "best practices" in matters of crimes committed by the Company foresees both protocols of a general nature and specific protocols for each of the activities listed above.

I.5.1 General Protocol

The following are the general protocols across all risk areas, with direct or indirect impact on the correct execution of the activities linked with the processes in those areas and, consequently, with the potential for criminal action:

1. the information security policy must be prepared, formally approved, periodically updated and communicated to all company personnel; the policies and procedures relative to information security must be aligned with the orientation indicated in the policy, must be periodically updated and communicated to all users;
2. back up management must be disciplined by a procedure which defines the back-up activities for every telecommunications network, the frequency of the activity, the modalities, the number of copies, the data

- conservation period;
3. the Company must possess Business Continuity Plan and a Disaster Recovery Plan, in order to guarantee IT systems and critical process continuity in case of disaster; the solutions identified must be updated and tested periodically;
 4. the generation and protection of activity logs on the systems, at least in the context of activities related to sensitive data must be disciplined by appropriate formal procedures;
 5. the detection and resolution of logical security incidents must be regulated by suitable procedures which define the incident classification criteria and escalation levels on the basis of the anomaly typology reported, and whether there must be notification of the same to interested parties and whether reporting activities are required on the results obtained.

I.5.2 Specific Protocols

The following are the control procedures specific to single risk areas, representing peculiar aspects of the processes present in the said areas:

1. Access, account and profile management

1. The system authentication requisites for access to data and to applications must be individual and univocal;
2. the procedure which defines the rules for creating access passwords for the network, for applications, for the company information property and for critical and/or sensitive systems (for example: minimum password length, complexity rules, expiry, etc.) must be formalised and notified to all users for selection and use of the key word;
3. the assignment of remote access to the systems by third parties such as consultants and suppliers must be regulated by the execution of the activities defined in a formal procedure;
4. any accesses effected by users to applications must be subject to verification and, with reference to the ambit of sensitive data, the applications must trace of changes to the data effected by users, and controls must be apply to detect mass variations to company databases;
5. account and access profile management must foresee the use of a formal system of authorisation and registration of the attribution, modification and deletion of system access profiles; procedures must be formalised for the assignment and use of special privileges (system administrator, super user, etc.);
6. Periodic checks must be conducted on user profiles to validate the level of responsibility of individuals assigned privileges; the results must be registered in an opportune manner.

2. Telecommunications network management

1. The telecommunication network management procedure must foresees the definition of responsibilities, implementation of security checks to guarantee the confidentiality of the data within the network and of data transiting public networks, the adoption of network segregations mechanisms and of network traffic monitoring instruments, implementation of network security event tracing mechanisms;
2. telecommunications network implementation and maintenance, the definition of periodic verification of network function/operation and of the anomalies encountered, the execution of periodic vulnerability assessment and ethical hacking must be defined in formal procedures, in order to identify all the responsibilities of the actors involved and the operative modalities.

3. Hardware Systems management

1. Hardware systems management must foresee the compilation and maintenance of an up to date inventory of the hardware in use at the Company and regulate responsibilities the operative modalities in the case of hardware implementation and/or maintenance in a formal procedure.

4. Software system management

1. Software systems management must include the compilation and maintenance of an up to date inventory of the software in use at the Company, the use of formally authorised, certified use of software and the execution on the principal systems of periodic verification of the software installed and of the mass memory of the systems used;
2. the change management process intended as software maintenance and/or new implementation must be defined by formal procedures for verification and testing of new software released both by internal personnel and by outsourcing suppliers.

5 Management of physical access to site hosting IT infrastructures

1. Physical security management for the sites hosting infrastructures must include, in an appropriate formal procedure, the vigilance modes, the reporting process for violations/illicit penetration of technical premises or breach of security measures, the counter-measures to be applied;
2. physical access to reserved premises hosting IT infrastructures must be guaranteed to be by use of access codes, token authenticators, PINs, badges, biometric values; there must be periodic control of the correspondence of the authorisations assigned with the role of the user authorised.

6. Digital format documentation management and security

1. the use of specific cryptography techniques for the protection and/or transmission of information must be regulated by a formal procedure which defines the operative modalities and the responsibilities of the actors involved in the management process;
2. a key management system must be implemented to support the cryptographic techniques for the generation, distribution, revocation and archiving of those keys;
3. controls to protect the keys against potential modification, destruction and/or unauthorised use must be predisposed and opportunely documented;
4. procedures to regulate the management of digital signature usage in documents must be formalised, disciplining responsibilities, authorisation levels, certification system adoption rules, and archiving and destruction modes for the same.
5. the IT document archiving, production and maintenance procedure must be predisposed and divulged to all actors involved in the process of IT document management.

All documentation referring to each activity above must be periodically updated and adequately archived and conserved in order to guarantee the traceability of the phases followed in the ambit of the activities covered. Access to archived documents is permitted to personnel only as authorised by company operative procedures, to the internal auditors, auditors and the CO.

The prescriptions indicated are not an exemption from compliance with the behavioural indications of which at the Ethical Code.

I.6 Instructions and verification of the CO

The tasks and activities to be performed by the CO for complying with the Model, on the basis of indications contained in articles 6 & 7 of legislative decree No. 231/2001, are the following:

- ✓ monitoring the effectiveness of the model, by comparing actual conduct against the model established.
- ✓ examining the adequacy of the model, in other words its real and not the hypothetical ability to generally prevent undesirable behaviours .
- ✓ analysing the long term endurance of the stability and functionality of the model:
- ✓ making provisions for the necessary upgrades in a dynamic conception of the model, assuming that the analysis conducted makes corrections and additions necessary (through adjustment proposals to company functions able to actually implement them within the corporate structure, or by means of a follow-up to check that the solutions proposed have been implemented and actually work).