



**Organizational, Management and Control Model pursuant to Legislative
Decree 231/2001**

Approved by Telespazio S.p.A. Board of Directors
at the meeting of 09/06/2009

CONTENTS**General Section**

1. LEGISLATIVE DECREE n. 231 on 8 JUNE 2001, AS AMENDED	1
1.1. regime of administrative liability of corporate subjects, companies and associations	1
1.2. Sanctions.	6
1.3. Conditions for the Company's exemption from liability.	6
2. CONFINDUSTRIA GUIDELINES	8
3. ADOPTION OF THE ORGANIZATIONAL AND MANAGEMENT MODEL BY TELESPAZIO S.P.A.	10
3.1. Motivations of Telespazio S.p.A. for the adoption of the organizational and management model.	10
3.2. Aims of the Model.	10
3.3. Structure of the Document.	11
3.4. Model Adoption and management in subsidiaries, affiliates and associate structures.	12
3.5. Amendments and additions to the Model.	13
4. THE SURVEILLANCE BODY	13
4.1. Identification of the Surveillance Body.	13
4.2. Functions and powers of the Surveillance Body	15
4.3. Modality and frequency of reports to the Company Boards	16
4.4. Information flows to the Surveillance Body	17
4.4.1. Reports from Company representatives or third parties.	17
4.4.2. Information obligations relative to official deeds	18
5. STAFF TRAINING AND CIRCULATION OF THE MODEL WITHIN THE COMPANY	19
5.1. Staff training	19
5.2. Information for external collaborators and counterparts	20
6. THE SYSTEM OF SANCTIONS	20
6.1. General principles	20
6.2. Sanctions for employees (non-managerial staff)	20

6.3. Measures against managers	21
6.4. Measures against the Directors	22
6.5. Measures against collaborators, consultants and other third subjects	22
7. CONFIRMATION OF THE APPLICATION AND ADEQUACY OF THE MODEL	22
A.1. TYPES OF OFFENCE AGAINST PUBLIC ADMINISTRATIONS (arts. 24 and 25 of the Decree)	25
A.2. THE NOTION OF CIVIL SERVANT AND PERSON RESPONSIBLE FOR A PUBLIC SERVICE (ARTS. 357-358, CRIM. CODE)	28
A.3. AT-RISK AREAS	30
A.4. ADDRESSEES OF THE SPECIFIC SECTION – GENERAL RULES OF CONDUCT AND IMPLEMENTATION OF THE DECISION-MAKING PROCESS IN AT-RISK ACTIVITY AREAS	31
A.5. AREAS OF AT-RISK ACTIVITIES: FUNDAMENTAL ELEMENTS OF THE DECISION-MAKING PROCESS	33
A.5.1 Single at-risk transactions: identification of the internal managers responsible and Evidence Forms	33
A. 5.2 Instructions and verifications of the Surveillance Body ...	34
B.1. TYPES OF CORPORATE OFFENCES AND OF MARKET ABUSE (arts. 25 <i>ter</i> and 25 of the Decree)	38
B.2. OTHER OFFENCES	41
B.3. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES	43
B.4. ADDRESSEES OF THE SPECIAL SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS	45
B.5. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT	46
B.5.1. Financial statements and other corporate information	46
B.5.2 Exercise of the powers of control over corporate management. .	47
B.5.3 Safeguard of the share capital	48
B.5.4. Offering circulars	48
B.5.5 Activities subject to supervision	49

B.5.6 Management of relations with the Auditing Firm	49
B.6. DUTIES OF THE SURVEILLANCE BODY	50
C.1. TYPES OF OFFENCE REGARDING HEALTH AND SAFETY IN THE WORKPLACE (ART. 25 –SEPTIES OF THE DECREE).....	53
C.2. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES.....	54
C.3. ADDRESSEES OF THE SPECIAL SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS	55
C.4. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT.....	55
C.5. THE DUTIES OF THE SURVEILLANCE BODY	63
D.1. TYPES OF OFFENCE REGARDING RECEIVING, MONEY LAUNDERING AND THE USE OF MONEY, ASSETS OR OTHER VALUABLES OF ILLICIT PROVENANCE (ART. 25 OCTIES OF THE DECREE)	66
D.2. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES.....	68
D.3. ADDRESSEES OF THE SPECIFIC SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS	68
D.4. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT.....	69
D.5. THE DUTIES OF THE SURVEILLANCE BODY	70
E.1. TYPES OF COMPUTER CRIMES AND ILLICIT DATA PROCESSING (ART. 24 <i>BIS</i> OF THE DECREE)	72
E.2. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES.....	78
E.3. ADDRESSEES OF THE SPECIFIC SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS	79
E.4. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT.....	81
E.5. THE DUTIES OF THE SURVEILLANCE BODY	86

GENERAL SECTION

1. LEGISLATIVE DECREE N. 231 ON 8 JUNE 2001, AS AMENDED**1.1. REGIME OF ADMINISTRATIVE LIABILITY OF CORPORATE SUBJECTS, COMPANIES AND ASSOCIATIONS**

In implementation of the delegation pursuant to Article 11 of Law n. 300 of 29 September 2000, Lgs. Decree n. 231 was issued on 8 June 2001 (hereinafter: "the Decree") and entered into force on 4 July 2001, by which the Legislator adapted national law to the international agreements, to which Italy had also signed, on the liability of corporate subjects. The said agreements are the Brussels Convention of 26 July 1995 on the Protection of the Financial Interests of the European Community, the Convention signed in Brussels on 26 May 1997 on Corruption Involving European Community Officials or Officials of Member States of the European Union, and the OECD Convention of 17 December 1997 on the Corruption of Foreign Public Officials in International Business Transactions.

The Decree on the "Discipline of Administrative Liability of Corporate Subjects, Companies and Associations, including those without Legal Personality", has introduced into the Italian legal system a regime of administrative liability (in practice, similar to criminal liability) of such Entities (i.e. companies, associations, consortiums, etc., hereinafter: "Entities") for specific offences that are perpetrated in their interest or for the benefit of:

individuals in high positions ("top management") (with representation, administration or direction of the Entity or of another organizational unit who in fact manage and control the Entity); or

- individuals subject to the direction or supervision of one of the persons indicated in the preceding point.

Liability is borne not only the individual who has actually committed the offence, but also by the Entity.

Pursuant to the Decree, therefore, Entities which have an interest in and/or gain an advantage from the offence are also responsible for not having exercised the necessary repression or control. The most serious sanctions applicable to the Entity are certainly those involving disqualification, such as suspension or revocation of authorisations, licences or concessions, the ban on practising business with public administrations, ban on the exercising of business, exclusion from or revocation of loans and subsidies, ban on advertising goods and services. The said liability is also applicable to offences committed abroad, unless they are prosecuted by the State where they have been committed.

The types of offences that currently involve such liability are:

- i. offences committed in transactions with Public Administrations;
- ii. forgery of cash, credit cards and duty stamps, pursuant to Law n. 406/2001, Article 6, which introduced Article 25 *bis* into Lgs. Decree n. 231/2001;
- iii. corporate offences pursuant to Lgs. Decree n. 61/2002, introducing Article 25 *ter*, as amended by Law n. 262/2005, into Lgs. Decree n. 231/2001;
- iv. crimes for the purpose of terrorism or subversion of the democratic system pursuant to Law n. 7/2003, which introduced art. 25-*quater* into Lgs. Decree n. 231/2001;
- v. maiming of female genitals, pursuant to Law n. 7 of 9 January 2006, which introduced art. 25-*quater* 1 into Lgs. Decree n. 231/2001;
- vi. crimes concerning slavery or servitude, trafficking in human beings and the purchase and sale of slaves, sexual exploitation of children and child pornography also through Internet, pursuant to Law n. 228/2003 and Law n. 38/2006, which introduced and amended art. 25-*quinquies* in Lgs. Decree n. 231/2001;
- vii. inside trading and market abuse, pursuant to art. 9 of Law n. 62 of 18 April 18 (Community Law 2004) which in turn adopted the rulings of Directive 2006/6/EC – as provided for in Part V, Section I *bis*, Chapter II, of the consolidated Act of Lgs. Decree n. 58 of 24 February, 1998 – have been recognised by the national Legislator by art. 25-*sexies* of Lgs. Decree n. 231/01;
- viii. Transnational offences of criminal association, money laundering, the traffic of migrants and hindering justice pursuant to Law n. 146 of 2006, which ratifies the United Nations Convention and Protocols against transnational organised crime adopted by the General Assembly on 15 November 2000 and 31 May 2001;
- ix. offences and illicit deeds committed in breach of safety regulations and on hygiene and health in the workplace pursuant to art. 9 of Law 123/07, which amended the law on safety and health in the workplace by the introduction of art. 25 *septies* into Lgs. Decree 231/01. Later, on 30 April 2008, Lgs. Decree n. 81 of 9 April 2008 was published, for the "Implementation of art. 1 of the foresaid Law 123/07 on health and safety in the workplace". This decree re-organises and reforms the laws in force on workers' health and safety by coordinating the same in a single consolidated act;
- x. receiving, money laundering and the use of cash, goods or assets from illicit acts, with the issue of Lgs. Decree 231/07 which adopts Directive 2005/60/EC of the European Parliament on money laundering by the introduction of art. 25 *octies* into Lgs. Decree n. 231/01;

- xi. computer crimes and unlawful data processing, pursuant to Law n. 48 of 18 March 2008, which ratifies the implementation of the Convention of the European Council on computer crimes, signed in Budapest on 23 November 2001 and which entered into force on 1st July 2004 with the introduction of art. 24-*bis* into Lgs. Decree n. 231/01.

Due to the peculiar nature of Telespazio S.p.A., of the offences at present contemplated in the Decree and its successive additions and amendments (which led to the revision of this Model first adopted in 2004), the offences referred to in points i, iii, vi, vii, viii and ix above are those that could affect the Company.

In particular:

Offences against Public Administrations:

- i. the undue receipt of grants, loans or other subsidies from a public body (art. 316 *ter* crim. code),
- ii. fraud to the prejudice of the State or other public body (art. 640, 2 paragraph, n. 1 crim. code),
- iii. aggravated fraud in receiving public funds (art. 640 *bis* crim. code),
- iv. computer fraud to the prejudice of the State or other public body (art. 640 *ter* crim. code),
- v. corruption in the execution of an official act (art. 318 crim. code),
- vi. corruption in the execution of an act conflicting with official duty (art. 319 crim. code),
- vii. corruption in judicial acts (art. 319 *ter* crim. code),
- viii. instigation to corruption (art. 322 crim. code),
- ix. corruption of persons responsible for a public service (art. 320 crim. code)
- x. extortion (art. 317 crim. code),
- xi. embezzlement to the prejudice of the State or other public body (art. 316 *bis* crim. code),
- xii. misappropriation, extortion, corruption and instigation to corruption of members of the institutions of the European Community and officials of European Communities and foreign States (art. 322 *bis* crim. code)

Corporate offences, market abuse and similar offences:

- i. the issue of false corporate information (art. 2621 civil code);
- ii. false corporate information to the prejudice of shareholders or creditors (art. 2622 civil code);
- iii. false in offering circulars (art. 173 *bis* Lgs. Decree n. 58 of 24.02.1998 and successive amendments and additions: "TUF" – *Testo Unico Finanziario* – Consolidated Finance Act);
- iv. false reports or information in communications with the Audit Firm (art. 2624 civil code);
- v. hindered supervision (art. 2625 civil code);
- vi. undue refund of conferment (art. 2626 civil code);
- vii. illegal allocation of profits and reserves (art. 2627 civil code);
- viii. illegal transactions on the stock or shares of the Holding Company (art. 2628 civil code);
- ix. transactions to the prejudice of creditors (art. 2629 civil code);
- x. failure to report conflict of interests (art. 2629 *bis* civil code);
- xi. failure to call the shareholders' meeting (art. 2631 civil code);
- xii. fictitious formation of capital (art. 2632 civil code);
- xiii. undue allocation of corporate assets by liquidators (art. 2633 civil code);
- xiv. unfair influence exercised at the shareholders' meeting (art. 2636 civil code);
- xv. market rigging (art. 2637 civil code);
- xvi. obstructing supervision on the part of the public supervisory authorities (art. 2638 civil code);
- xvii. inside trading (art. 184 TUF);
- xviii. market abuse (art. 185 TUF);

Other Offences:

- i. reduction or maintenance in slavery or servitude, trafficking in human beings, purchase and sale of slaves, sexual exploitation of children and child pornography also via Internet, introduced by Law n. 228/2003 and Law n. 38/2006;
- ii. serious transnational offences committed by an organized group, pursuant to art. 10 of Law n. 146 of 16 March 2006.

Offences committed in breach of safety and accident prevention provisions

- i. manslaughter (arts. 589 crim. code)
- ii. serious bodily harm due to breach of safety and accident prevention provisions (art. 590, clause 3, crim. Code).

Receiving, money laundering and the use of cash, goods or assets from illicit acts:

- i. receiving (art. 648 crim. code);
- ii. money laundering (art. 648 *bis* crim. code)
- iii. use of money, property or other valuables of illegal provenance (art. 648 *ter* crim. code)

Computer crimes and illegal data processing:

computer documents (art. 491 crim. code);

unauthorised access to a computerised or electronic communication system (art. 615 *ter* crim. code);

detention and unauthorised disclosure of access codes to computer or electronic communication systems (art. 615 *quater* crim. code);

circulation of equipment, devices or computer programmes intended to damage or interrupt a computer or electronic communications system (art. 615 *quinquies* crim. code);

unauthorised interception, hindrance or interruption of computer or electronic communications (art. 617 *quater* crim. code);

installation of equipment designed to intercept, hinder or interrupt computer or electronic communications (art. 617 *quinquies* crim. code);

damage to information, data and computer programmes (art. 635 *bis* crim. code);

damage to information, data and computer programmes used by the State or other public body or, in any case, of use to the general public (art. 635 *ter* crim. code);

damage to computer and electronic communication systems (art. 635 *quater* crim. code);

damage to computer and electronic communication systems of public use (art. 635 *quinquies* crim. code).

1.2. SANCTIONS.

The sanctions foreseen for administrative liability are:

- fines;
- disqualification;
- confiscation;
- publication of judicial decisions.

In particular, the main disqualifications, which, however, are not applicable to the corporate offences referred to by Article 25 *ter* of the Decree, concern:

ban on the practice of business;

ban on transactions Public Administrations;

suspension or revocation of authorisations, licences or concessions involved in the perpetration of the offence;

exclusion from subsidized loans, grants, contributions and subsidies and/or the revocation of those already granted;

ban on advertising goods or services.

Fines, applicable in all cases, are determined by means of a "quota" system of points ranging from one hundred to one thousand and from Euro 258.22 to Euro 1,549.37 .

In the case of fines applicable to the offences referred to by art. 25 *ter* of the Decree, the amount of the quota can vary between Euro 516.46 and Euro 3,098.74 (pursuant to the amendment of art. 39, clause 5, of Law n. 262 of 28 December 2005).

The court shall determine the number of quotas according to the seriousness of the facts, the level of the Entity's responsibility and the measures required to eliminate or mitigate the consequences of such facts and to prevent the perpetration of further offences. The amount of the quota is fixed according to the economic situation and the assets of the Entity, in order to ensure the effectiveness of sanctions (Article 11 of Lgs. Decree n. 231/2001).

1.3. CONDITIONS FOR THE COMPANY'S EXEMPTION FROM LIABILITY.

Once the Entity's administrative liability has been established, exemption may be allowed pursuant to Article 6 of the Decree if the said Entity can prove that it had adopted and effectively put into practice, prior to the commission of the facts, the "*organizational, managerial and control models suitable to prevent the type of offence committed*".

According to the same provision, the Company must also institute an internal supervisory organ with the responsibility of supervising the effective functioning of and the effective compliance with the aforesaid models, as well as of updating the same.

Such Organizational, Management and Control Models (hereinafter: "the Models"), pursuant to Article 6, paragraphs 2 and 3, of Lgs. Decree n. 231/2001, must:

- identify the activities relative to which the offences referred to in the Decree may be committed;
- provide for *ad hoc* protocols pursuant to which the Entity's decisions regarding the prevention of crime must be programmed and implemented;
- indicate modalities for the management of the financial resources required to prevent such offences;
- establish the information obligations of the Body responsible for supervising the implementation of and compliance with the Models;
- introduce a disciplinary system suitable to sanction the failure to respect the measures indicated in the Model.

In the case of an offence committed by persons with powers of representation, administration or management of the Entity or any of its departments with financial and functional independence, or by persons who in fact manage and supervise the same, the Entity shall not be liable if it proves that:

- the board of directors had adopted and effectively implemented, prior to the fact, a Model suitable to prevent offences such as that committed;
- the supervision of the implementation of and compliance with the Model, and the updating of the same, was entrusted to department of the Entity endowed with independent powers of initiative and control;
- the persons committed the offence by fraudulently avoiding application of the Model;
- the Surveillance Body adequately performed its duties with regard to the Model.

However, if the offence is committed by persons subject to the management or supervision of one of the above-indicated subjects, the Entity shall be liable if the offence was possible due to failure to comply with the obligations of direction and supervision. Even in the case of such failure, the Entity shall nevertheless be exempt from liability if, prior to

the offence, it adopted and effectively implemented a Model suitable to prevent such an offence.

The Decree also rules that the Models can be adopted, provided they meet the above requirements, on the basis of codes of conduct drawn up by associations representing the sector and which are communicated to the Ministry of Justice which, in concert with the competent Ministries, can submit, within 30 days, observations on the suitability of the Models to prevent the offences.

Lastly, in the case of small Entities, the supervisory obligation can be directly performed by the board of directors.

2. CONFINDUSTRIA GUIDELINES

This Model was developed on the Guidelines issued by *Confindustria* on 7 March 2002, as supplemented on 3 October 2002 by the "Supplementary Appendix on Corporate Offences" (hereinafter: the "Guidelines") and subsequently updated on 24 May 2004 and 31 March 2008.

The development of the Model according to the said guidelines can be summarised as follows:

- identification of *risk areas*, aiming at detecting the Company areas/sectors in which offences are likely to be committed;
- the creation of an supervisory system able to reduce the risks by the adoption of special protocols. It is supported by a co-ordinated series of organizational structures, activities and operating rules which are applied – on the instructions of the top managers - by the Company's managers and employees, and is designed to provide reasonable certainty of the achievement of the purposes of a well-functioning internal supervisory system. The major components of the preventive supervisory system proposed by *Confindustria* are:

code of ethics;

organizational system;

manual and computerised procedures;

powers for authorisations and signatures;

supervisory and management systems;

notices to staff and staff training.

The supervisory system must also be based on the following principles:

- the possibility of verifying and recording every transaction and the suitability of the same;
- separation of duties (no one can independently manage all stages of any process);
- the recording of supervisory activities;
- application of an adequate system of sanctions for breach of the rules and procedures prescribed by the Model;
- the institution of an SB (Surveillance Body), the main characteristics of which are:
 - autonomy and independence,
 - professional skill,
 - continuity of action.
- the obligation borne by the company's departments and particularly by those recognised as more at risk, of reporting to the SB, both on a structured basis (routine reports pursuant to the Model) and in the case of any irregularity or non-compliance emerging from the available information (in the latter case the obligation is extended to all staff without respect for hierarchy);
- the possibility of applying organizational solutions within the group, concentrating in the Surveillance Body the operating resources to be allocated to the supervision also of the companies of the group itself, always providing that:
 - an Surveillance Body is established in every subsidiary;
 - the subsidiaries' SBs can take avail of the Holding Company's SB pursuant to a predefined contractual agreement;
 - the Holding Company's SB staff, in the execution of inspections at the other companies of the group, act as independent professionals who perform their activity in the interests of the subsidiary, directly reporting to this latter's SB, and are subject to the confidentiality obligations that are typical for external consultants.

It remains understood that the decision not to apply some specific aspects of the Guidelines does not affect the validity of a Model. Indeed, the latter is drawn up by taking into account the particular nature of a specific company and can therefore differ from the Guidelines of a general nature.

3. ADOPTION OF THE ORGANIZATIONAL AND MANAGEMENT MODEL BY TELESPAZIO S.P.A.

3.1. MOTIVATIONS OF TELESPAZIO S.P.A. FOR THE ADOPTION OF THE ORGANIZATIONAL AND MANAGEMENT MODEL.

In order to constantly increase correct business conduct and transparency, Telespazio S.p.A. has deemed it consistent with its company policy and the indications of the holding company, *Finmeccanica*, to adopt an organizational and management Model in accordance with the provisions set out in the Decree and the Guidelines issued by *Confindustria*.

The Model, together with the adoption of the Code of Ethics in 2003, is based on the belief that the application of the same – apart from the provisions of the Decree according to which the Model is optional and not obligatory - can represent a suitable tool for increasing the awareness of all the Company's staff and other subjects concerned (customers, suppliers, counterparts, collaborators) and to encourage them to adopt correct and consistent conduct in the execution of their work, such as to prevent the risk of the offences referred to by the Decree.

3.2. AIMS OF THE MODEL.

The Model drawn up by Telespazio S.p.A. is based on a structured and organic system of procedures as well as on supervisory activities which substantially:

- identify the potential risk areas/procedures, i.e. those activities regarding which offence is more likely;
- define an internal system of rules in order to plan the Company's decision making and implementation as regards the risks/offences to be prevented by means of:
 - a Code of Ethics outlining the commitments and ethical responsibilities in the performance of business and Company activities on the part of the employees, directors and collaborators;
 - a system of delegating duties and powers for the execution of Company transactions which ensures a clear and transparent representation of the decision making and implementation process;
- determine a coherent organizational structure which can foster and monitor correct conduct, guaranteeing a clear and organic assignment of duties, applying correct segregation of duties and ensuring that the measures adopted by the organizational structure are actually implemented;
- identify management and auditing processes for financial resources in at-risk activities;

- assign to the SB the duty of supervising the implementation of and compliance with the Model and propose revision.

Therefore the Model aims at:

- improving the system of Corporate Governance;
- preparing a structured and organic system of prevention and supervision aimed at reducing the risk of committing offences connected to the company's business with special focus on reducing the possibility of unlawful conduct;
- fostering awareness in all those operating in the name of and on behalf of Telespazio S.p.A. in at-risk activity areas, of the possibility of being held accountable for administrative tort and for criminal offences in the case of the infringement of the Model, and of being subject to the relevant sanctions applied by both law and the Company;
- informing all those operating in any manner whatsoever in the name of, on behalf of or in the interests of Telespazio S.p.A. that infringement of the Model shall lead to the application of *ad hoc* sanctions or to dismissal;
- emphasising that Telespazio S.p.A. will not tolerate unlawful behaviour of any kind, regardless of purpose, since such conduct (even if the Company may apparently benefit) in any case conflicts with the ethical principles with which Telespazio S.p.A. intends to conform.

3.3. STRUCTURE OF THE DOCUMENT.

This document (Model) consists of a "General Information" section and separate "Specific Information" sections regarding the various types of offence that could represent a risk for Telespazio S.p.A., contemplated in Lgs. Decree n. 231/2001. In the first General Information section, after a description of the principles of the Decree, the essential components of the Model are illustrated, with special reference to the Surveillance Body, staff training and the communication of the Model within the Company, the disciplinary system and the measures that must be adopted in the case of infringement of the rules of the Model. The Specific Section "A" describes specific types of offence contemplated by Articles 24 and 25 of the Decree, i.e. offences against Public Administrations. The Specific Section "B" describes types of offence contemplated by arts. 25 *ter* and 25 *sexies* of the Decree, i.e. the so-called corporate offences of market abuse, and those classified above as "Others". The Specific Section "C" regards the types of offence contemplated by article 25 *septies* of the Decree, i.e. offences and unlawful conduct in breach of the provisions on accident prevention and hygiene and health in the workplace. The Specific Section "D" regards the types of offence contemplated by art. 25 *octies* of the Decree, i.e. receiving, money laundering and the use of cash, goods or gain of illicit provenance. The Specific Section "E" regards

the types of offence contemplated by art. 24 *bis* of the Decree, i.e. computer crimes and unauthorised data processing.

3.4. MODEL ADOPTION AND MANAGEMENT IN SUBSIDIARIES, AFFILIATES AND ASSOCIATE STRUCTURES.

The companies, incorporated under the Italian law, held directly or indirectly by Telespazio S.p.A., shall apply their own Organizational, Management and Control Models which, pursuant to Lgs. Decree n. 231/01, must follow the prescriptions of the Decree.

In this way, the companies shall take as a reference the Model of Telespazio S.p.A. which they shall then adapt by specific amendments in view of the at-risk activity areas specific to each company.

Each subsidiary shall set up its own Surveillance Body whose main duty is to supervise the implementation of the Model according to the procedures contained in the same and the directives of Article 6 of Decree n. 231/01.

The Surveillance Body of each subsidiary shall:

- i. co-ordinate its activity with the SB of Telespazio S.p.A., in order to ensure the adoption of an Organizational, Management and Control Model based on the prescriptions of the Decree, the *Confindustria* Guidelines and the principles of this Model;
- ii. transmit the adopted Organization Management and Control Model and any amendments to the SB of Telespazio S.p.A. .

For the other Italian organisations in which it holds a stake, Telespazio S.p.A. – through its own representative on the Board of Directors or at the Shareholders' Meeting - shall officially emphasise the need to apply the rules of Lgs. Decree n. 231/2001 and shall make all possible effort to meet such need.

With regard to the establishment of new associated structures in Italy, Telespazio S.p.A. shall verify from the onset whether the other Partners have conformed to Lgs. Decree n. 231/2001, also by requiring the Partners to sign a statement to that purpose.

In the case of associated companies abroad, Telespazio S.p.A. requests at least the adoption of the Code of Ethics and informs the governing bodies of the usefulness of adopting suitable preventive procedures in order to protect themselves against possible impact leading to the administrative liability of the company.

In any case, all Telespazio employees and collaborators entrusted to carry out activities on behalf of or in the interests of companies in which Telespazio S.p.A. holds a stake must strictly adhere to the rules of the Code of Ethics and of the Organizational, Management and Control Model adopted by Telespazio S.p.A.

With regard to foreign subsidiaries, the same must assess, according to the applicable local law, the modalities for application of the Guidelines of the *Finmeccanica* Group relative to Lgs. Decree n. 231/01.

3.5. AMENDMENTS AND ADDITIONS TO THE MODEL.

Since this Model is a deed issued by the board of directors (in compliance with the rules of art. 6, clause 1, letter a of the Decree), its adoption, as well as successive amendments and additions, fall under the responsibility and discretion of the Telespazio S.p.A. Board of Directors.

The Telespazio S.p.A. Board of Directors is specifically responsible for supplementing this Model with further Special Sections on any offence which, pursuant to new legislation, may fall within the scope of Lgs. Decree n. 231/01.

4. THE SURVEILLANCE BODY

4.1. IDENTIFICATION OF THE SURVEILLANCE BODY

Pursuant to Lgs. Decree 231/2001, to supervise the effectiveness and observance of the Model, and the updating of the same, must be the responsibility of an internal body of the Company (art. 6, clause 1, letter B of the Decree) other than the Board of Directors.

Telespazio S.p.A. therefore decided, pursuant to resolution of the Board of Directors of 14 April 2003, to initially appoint the Internal Audit department manager as the sole member of the Surveillance Body. Later, on the indications of the Holding Company, on 28 June 2006, the Telespazio Board of Directors appointed a new Surveillance Body with several members. In particular, the Statute and the Regulations of the SB, which discipline its operations, were respectively approved by the Company's Board of Directors on 28 June 2006 and on 5 September 2006.

The Surveillance Body has three members; the Chairman is also a member of the Company's Board of Auditors, and the other two are respectively the Manager pro-tempore of the Internal Audit department and the Manager pro-tempore of the Legal and Corporate Affairs Department. It may be enlarged but by no more than two more members.

The choice depended on the specific nature of the tasks of the SB, the provisions of the Decree and the indications contained in the guidelines issued by Confindustria, and guarantees that the Body has the most opportune requisites of autonomy, independence, professional skill and continuity of action, which the Decree itself requires of the Body.

In particular, also in consideration of the recommendations of the aforesaid guidelines, the requisites are illustrated below:

Autonomy and independence

Because of its autonomy and independence, guaranteed by its collegiate nature, the Surveillance Body can carry out its own role without being directly or indirectly conditioned by the subjects under its supervision. To guarantee its independence, the Surveillance Body reports directly to the Board of Directors, and also reports to the Board of Auditors in the case of any anomaly or irregularity referred to by Lgs. Decree 231/2001, found within the Board of Directors.

Professional skill

The members of the Surveillance Body hold adequate technical-professional skills for the performance of their duties. These characteristics and the Body's independence guarantees the objectivity of its opinion.

Continuity of action

To guarantee effective and constant implementation and respect for the Model, the Surveillance Body has a structure that is constantly dedicated to monitoring Company procedures. For improved and more effective performance of its duties and functions assigned to the same and disciplined by the Statute, the Surveillance Body may take avail, for the execution of its operations, of the Company's Internal Audit Department and of the other departments which may be useful on the various occasions for carrying out its activities.

The Body may also take avail of external advisors, of proven professional skill, whenever necessary for the performance of its verification and monitoring activities or to update the Model, always in respect of the Company's internal procedures for assigning consultancy mandates.

The Statute of the Surveillance Body establishes and regulates – among other things - the modalities by which the information and documents requested by the Body, in order to guarantee effective action on the Company organisation, must be transmitted.

The Body may also delegate specific tasks to one or more of its components, its collegiate responsibility always holding firm.

4.2. FUNCTIONS AND POWERS OF THE SURVEILLANCE BODY

The activity of the Telespazio S.p.A. Surveillance Body consists, in particular, in:

monitoring the application of the Model with regard to the various types of offence contemplated by the Decree;

checking on the effectiveness of the Model and its capacity to prevent the offences referred to by the Decree;

identifying and proposing to the Board of Directors revisions and amendments to the said Model, in the case of new legal provisions or changed Company conditions;

constantly monitoring the Company's system of procedures for the prevention and management of the risks of offence, pursuant to Lgs. Decree 231/2001 and the application of the Corporate Governance system and of making any necessary amendments to the same.

Therefore, on a practical level, the following tasks are assigned to the Telespazio S.p.A. Surveillance Body:

- activation of the control procedures, taking into account that the operating management in any case continues to hold responsibility for monitoring activities, also those relative to at-risk areas, and that this task is an indispensable part of the Company's business process;
- periodic verification of the map of the areas subject to the risk of offence, in order to adapt the same to changes in Company activities or structure. For this purpose, the Management and those responsible for supervising the individual departments must report to the SB any situations that could expose the Company to the risk of offence. All communications must be in writing (also via e-mail or fax) and anonymity will be respected;
- periodic verification targeted at certain transactions or specific deeds, carried out within the sphere of the at-risk activities as defined in the single Specific Sections of the Model;
- the promotion of suitable initiatives to circulate the Model, and preparation of the internal organisational documentation necessary for the functioning of the Model, containing instructions, clarifications or updated information;
- the collection, processing and filing of information (including the reports referred to in paragraph 4.4 below) concerning the Model, and the revision of the information list which must be obligatorily transmitted to the SB (see paragraph 4.4 below);
- internal inquiries into presumed infringements of the prescriptions of the Model which are reported to the SB or which come to light during the supervisory activity of the SB;

- verification to ensure that the elements foreseen in the various Specific Sections of the Model for the various types of offence (adoption of standard clauses, execution of procedures, etc.) are in any case adequate and respond to the needs for the observance of the prescriptions of the Decree, proposing revision of the said elements should they be found inadequate;
- working in coordination with the Internal Audit Department and the other Company departments in monitoring the at-risk activities; The SB is informed, by the Management and the Company departments, of every activity carried out concerning situations that could expose the Company to the risk of the offences contemplated in Lgs. Decree 231/01; the SB also has free access to all relevant Company documentation, including data classified as sensitive pursuant to the Privacy Code, processing of which is subject to the general authorisation of the Data Protection Commissioner (Official Journal 190/04) or by specific authorisation;
- to check that the documentation requested pursuant to the various Specific Sections of the Model for the various types of offence is available, regularly revised and effectively implemented. The most important activities or transactions contemplated in the Specific Sections must be reported to the SB, and the updated information regarding the documentation must be made available to the same, to enable the performance of its control duties.

To perform the above duties, the SB:

has access to Company documents;

is provided with adequate financial and professional resources;

takes avail of the support and cooperation of the various Company departments interested or involved in the control activity.

The statute of the SB, approved by the Telespazio Board of Directors on 28 June 2006, specifically details the duties, functions and powers.

4.3. MODALITY AND FREQUENCY OF REPORTS TO THE COMPANY BOARDS

The Surveillance Body reports periodically to the Board of Directors on the work carried out, particularly as regards correct implementation of the Model and any critical facts that emerge.

The reporting may be carried out informally and on a continuative basis to the Chairman of the Board and the Managing Director also by the single members of the Body.

A formal written report must be sent every six months to the Board of Directors and to the Board of Auditors on the supervisory work carried out and the results.

Within the two months following the closure of every financial period, the Surveillance Body presents to the Board of Directors and the Board of Auditors a general framework report on the work carried out, relations with the Company departments and with the Board of Auditors itself.

In any case, the Surveillance Body must immediately inform the Board of Directors in the case of infringements of the Model or the Code of Ethics, and also if the Model must be revised and in the case of legislative innovations relative to corporate liability.

The SB of Telespazio S.p.A. may, in any case, be convoked at any moment by the aforesaid bodies or may in turn present a request, to report on the effective implementation of the Model or any particular situations.

4.4. INFORMATION FLOWS TO THE SURVEILLANCE BODY

4.4.1. Reports from Company representatives or third parties.

Within the sphere of the Company, the SB must be informed not only of the documentation prescribed by the single Specific Sections of the Model according to the procedures contemplated therein, but also of any other information, of any kind whatsoever, also from third parties, regarding the implementation of the Model in the at-risk areas.

Therefore the following prescriptions hold firm:

- no reports on infringement of the Model or, in any case, on conduct that is not in line with the rules of conduct adopted by the Company, may be refused;
- the SB will examine the reports received and will consider consequent measures according to its own reasonable discretion, if necessary also hearing the author of the report and/or the person responsible for the presumed breach, and will give a written explanation of any refusal to proceed with an internal inquiry;
- the reports, pursuant to the Code of Ethics, the reports must be in writing and may not be anonymous, and must regard every breach or suspected breach of the Model. In order to safeguard the reporting party against reprisal, discrimination or penalisation, the SB guarantees the confidentiality of the identity of the same, except in the case of legal obligations, the protection of the Company's rights or those of persons erroneously accused and/or if the reporting person is not in good faith;

- to facilitate the flow of reports and information towards the SB, dedicated information channels are foreseen (a special e-mail box: ODV@Telespazio.com- Top Fax Call: 06-40999165);
- reports received by the SB must be conserved and kept in a special file to which only the SB staff has access.

4.4.2. Information obligations relative to official deeds

In addition to the reports, including the unofficial reports, referred to in the preceding point, the SB of Telespazio S.p.A. must also be sent all information documents on:

orders and/or reports from the CID or any other authority which indicate inquiries into the offences contemplated by the Decree, even if perpetrated by unknown persons;

requests for legal assistance forwarded by managers and/or employees in the case of police inquiries into offences contemplated by the Decree;

reports drawn up by the managers of other Company departments within the sphere of their supervisory activities, which may bring to light facts, actions, events or omissions that could regard failure to observe the provisions of the Decree;

news relative to the effective implementation, at all Company levels, of the organisational Model, which include evidence of disciplinary procedures carried out and any sanctions applied (including provisions applied to employees) or of the decision to file such procedures with the relative reasons;

the organisational system and the separation of roles.

The organisational system must respect the requisites of:

clarity, formalisation and communication, especially regarding the assignment of responsibility, the definition of the hierarchical chains and the assignment of operational duties;

the separation of roles, i.e. the organisational structure arranged in order to prevent overlapping of responsibilities and the concentration of duties and the consequent avoidance of a high degree of criticality or risk.

To guarantee these requisites, the Company has organisational instruments (staff organisation chart, organisational documents, procedures, etc.) based on general principles of:

- transparency within the Company;
- clear descriptions of the hierarchical chains;
- clear and formal delimitation of roles, with descriptions of the tasks and responsibilities assigned to each department.

Delegation of powers

The system of delegations regards both internal authorisation powers, regarding the Company's decision-making processes relative to operations to be carried out, and powers of representation with the authority to sign deeds and documents destined for external subjects and which are binding on the Company (so-called special or general "power of proxy"). The delegations of powers must fulfil the following requisites: (i) they must be clearly defined and formally assigned by written communications; (ii) they must be coherent with the responsibilities and duties delegated and with the offices held within the organisational structure; (iii) they must specify limits in line with the roles assigned, particularly as regards expenditure and authorisation and/or approval of operations and deeds considered at-risk within the Company environment; (iv) they must be updated in the case of organisational change.

The SB must therefore always be informed of the organisational structure and of the system of delegations of Telespazio S.p.A. and of every modification to the same.

5. STAFF TRAINING AND CIRCULATION OF THE MODEL WITHIN THE COMPANY

5.1. STAFF TRAINING

Telespazio S.p.A. promotes knowledge of the Model, the relevant internal protocols and their revision among all employees, to ensure their acquaintanceship and compliance with the content, and to foster implementation.

The Human Resources and the Organisation and Information Technology departments, together with the SB, also manage staff training with specific focus on the implementation of the Model. Such training is divided according to the following levels:

- Top Management, managers and personnel with the authority to represent the Company: an initial training course, access to the Company intranet with space dedicated to the subject and updated in collaboration with the SB; occasional updates communicated by e-mail;
- Other staff: information given on recruitment for new employees; initial training course by e-learning methods, with IT support, extended whenever necessary to all newly hired personnel; internal information memoranda; access to intranet; updates communicated by e-mail.

5.2. INFORMATION FOR EXTERNAL COLLABORATORS AND COUNTERPARTS

Telespazio S.p.A. promotes awareness and observance of the Model also among its business and financial counterparts, its advisors, collaborators, customers and suppliers.

These are therefore informed of the principles, policies and procedures that Telespazio S.p.A. has adopted on the basis of the Model, as well as the specific wording of the contractual clauses which, pursuant to the said principles, policies and procedures, are adopted by the Company.

6. THE SYSTEM OF SANCTIONS

6.1. GENERAL PRINCIPLES

Pursuant to arts. 6, clause 2, letter e) and 7, clause 4, letter b) of Lgs. Decree 231/2001, the organisational, management and control models which must be adopted and implemented (together with the other conditions foreseen by the said articles 6 and 7) in order to avoid the Company's liability in the case of the offences contemplated by the Decree, can be effectively implemented only if a disciplinary system exists which sanctions infringement of the prescriptions of such Models.

Such a disciplinary system must apply to both employees, external collaborators and third parties who work for or with the Company, and must involve disciplinary sanctions for the former and contractual measures for the latter (e.g. rescission of contract, cancellation from the list of suppliers, etc.)

The sanctions must be applied regardless of any criminal inquiries or charges, since the organisational and procedural models represent binding rules, infringement of which must be sanctioned, in order to observe the dictates of the said Lgs. Decree, independently of the actual perpetration of an offence or of any punishment that may be imposed by law.

6.2. SANCTIONS FOR EMPLOYEES (NON-MANAGERIAL STAFF)

The Telespazio disciplinary system applicable to non-managerial employees is specifically regulated by the National Collective Labour Contract in force and by any connected agreements and deeds.

The sanctions that can be imposed and relative examples of cases of infringement (which are merely examples and therefore do not cover all types of conduct susceptible to disciplinary measures) can be found in the above-mentioned documents.

To this regard, it is emphasised that the Company informs its employees that the Organisational, Management and Control Model is an expression of the employer's authority to issue instructions regarding the performance and discipline of the work (art. 2104 of the civil code) and that consequently

non-respect and/or infringement of the same and of the rules of conduct imposed by the Code of Ethics and/or by Company procedures, represents default of the obligations deriving from the employment contract and disciplinary breach (art. 2106 of the civil code), and as such may involve the application of the sanctions foreseen by the laws in force and by the Collective Labour Agreement.

Therefore, in order to comply with the provisions of Lgs. Decree 231/2001 regarding the adoption of a suitable disciplinary system involving sanctions for the infringement on the part of non-managerial employees of the measures foreseen by the Organisational, Management and Control Models, and/or by the Code of Ethics, the Company implements the already-existing above-mentioned disciplinary system.

In any case, for greater clarity of the system of sanctions, the Company may further enlarge the list of examples of types of conduct which will be sanctioned, informing all employees of the same by the usual foreseen methods, adding certain cases relative to observance of the Model prescribed by Lgs. Decree 231/2001 and of the Code of Ethics.

In charging employees with infringements and in applying the sanctions, the procedures laid down by law, by the National Collective Labour Agreement and by any other agreements in force must be respected.

In the application of disciplinary sanctions, the principle of proportion between the infringement and the sanction must be respected, and any mitigating circumstances must also be taken into account (e.g. actions aimed at eliminating or preventing damaging consequences, the entity of the damage or of the consequences, etc.).

The adequacy of the disciplinary system to the prescriptions of Decree 231/2001 will be constantly monitored by the Surveillance Body, which must be guaranteed an adequate information flow on the types of sanctions applied and the circumstances in which they were applied.

Ascertainment of the aforesaid infringements, possibly reported by the Surveillance Body, the management of the disciplinary procedures and the application of the sanctions remain the responsibility of the Company departments assigned with such duties and to which the relative authority has been delegated.

6.3. MEASURES AGAINST MANAGERS

In the absence of disciplinary system applicable to managers, and in consideration of their relationship of trust with the employer, in the case of breach of the general principles of the organisational, management and control models and of the rules of conduct imposed by the Code of Ethics and/or by Company procedures, the Company will take suitable measures pursuant to law and the National Collective Labour Agreement for Industrial

Managers according to the infringement committed, also taking into account that such infringement represents default of the obligations deriving from the employment contract.

6.4. MEASURES AGAINST THE DIRECTORS

In the case of breach of the laws in force, of the organisational and control models and/or of the Code of Ethics on the part of members of the Company's Board of Directors, the Surveillance Body will inform the entire Board of Directors and the Board of Auditors, which shall take opportune measures pursuant to law, involving the Shareholders' Meeting if necessary.

6.5. MEASURES AGAINST COLLABORATORS, CONSULTANTS AND OTHER THIRD SUBJECTS

Any conduct in breach of the provisions of Lgs. Decree 231/2001 and or the Code of Ethics adopted, in the course of their work with the Company, by collaborators, advisors or other third parties who are not employees but linked to the Company by a contractual relationship, may lead to the application of penalties or, in the case of grave breach, rescission of the contract, the Company always maintaining the faculty of claiming compensation for damages.

For this purpose, especially with regard to outsourced activities, the contracts include specific clauses pursuant to which the contracting parties acknowledge their awareness of the Decree and of the Telespazio S.p.A. Code of Ethics.

The Surveillance Body must assess the suitability of the measures adopted by the Company against collaborators, advisors, third parties and any other subject working for any reason with the Company and shall provide for revision if necessary.

7. CONFIRMATION OF THE APPLICATION AND ADEQUACY OF THE MODEL

The Organisational Model shall be subject to two types of verification:

- monitoring on the effectiveness of the Model (and concrete verification on the compliance with the same) by the institution of a system of periodic statements on the part of all those who are held to observe the same, by which respect for the directives and contents of the Model is confirmed (see the Evidence Form attached to the Specific Section "A").
- The managers of the at-risk areas identified must ensure that the said confirmation form is filled in by their subordinates and transmit the same to the Surveillance Body which will file the forms returned and will also verify the statements by sample checks.
- Verification of procedures: Every year implementation and effectiveness of the Model will be verified by methods established by the SB. In

addition, all reports received during the year and the measures adopted by the SB and the other subjects concerned, events considered as susceptible to risk, and the awareness of personnel of the offences contemplated by the Decree, will be reviewed.

- The result of this review, including annotations of any shortcomings and suggestions for corrective action, will be communicated to the Company's Board of Directors.

SPECIFIC SECTION "A"

Offences against Public Administrations

A.1. TYPES OF OFFENCE AGAINST PUBLIC ADMINISTRATIONS (ARTS. 24 AND 25 OF THE DECREE)

A brief description is given below of the offences contemplated by arts. 24 and 25 of the Decree.

i. Undue receipt of grants to the prejudice of the State (art. 316 *ter* crim. code)

This offence is recognised when grants, funding, subsidised loans or other such subsidies granted or issued by the State or other public bodies or the European Union, is obtained fraudulently by the use or presentation of false documents or by the omission of relevant information.

In such a case, contrary to what is mentioned in the preceding point (art. 316 *bis*, crim. code), the destination of the public funds issued is of no relevance, since the offence is committed when the funds are – unduly – obtained.

This offence, being of a residual nature, only occurs if the behaviour is not recognised as the more serious offence of aggravated fraud to the damage of the State (art. 640 *bis*, crim. Code).

ii. Aggravated fraud to the prejudice of the State or other public body (art. 640, clause 2, n. 1, crim. code)

This offence is recognised when unfair gain is obtained, to the prejudice of the State or other public body or the European Union, inducing certain subject/s into error by artifice or deception.

The offence occurs when, for example, in the preparation of documents or data for participation in public tender procedures, the Public Administration is given untrue information (supported, for example, by counterfeit documentation) in order to be awarded the contract.

iii. Aggravated fraud in receiving public funds (art. 640 *bis*, crim. code)

This offence is recognised if the above-described fraudulent conduct is aimed at obtaining public subsidies, of any kind, from the State, other public bodies, or the European Union.

It can occur in the case of artifice or deception, such as the communication of false information or the presentation of counterfeit documentation, in order to obtain public funding.

iv. Computer fraud to the prejudice of the State or other public body (art. 640 *ter*, crim. code)

This offence is recognised when a computer or electronic communication system is tampered with or when the data contained in the same are manipulated in order to obtain unfair gain to the prejudice of the State or other public body.

In practice, the offence occurs when, for example, a loan has been obtained and unauthorised access is then gained to the computer system of the Public Administration in order to enter a figure greater than that legitimately granted.

v. Corruption (arts. 318-319, crim. code)

This offence is recognised when a civil servant or person responsible for a public service demands to receive or demands a promise of money or some other advantage for him/herself or for others in exchange for omitting to perform, or for delaying the performance of, his/her official duties or to carry out actions contrary to his/her official duties.

This offence also occurs in the case of an undue offer or promise made in connection with actions – conforming with or contrary to official duties – already carried out by the civil servant.

The offence is therefore committed when the civil servant performs his/her duty (e.g. accelerating a procedure which falls within his/her competence) and when he/she carries out an action contrary to his/her duties (e.g. guaranteeing the illicit awarding of a contract).

Such offences differ from extortion in as much as the corrupting and the corrupted parties act in agreement in pursuit of reciprocal gain, while in the case of extortion the private subject is forced to suffer the conduct of the civil servant or the person responsible for the public service.

Pursuant to art. 321 of the criminal code, the punishment foreseen for civil servants and those responsible for a public service is also applied to the private subjects who give or promise the former cash or some other gain.

vi. Corruption in judicial acts (art. 319 *ter* crim. code)

The offence occurs if a certain person offers or promises money or other gain to a civil servant or a person responsible for a public service in order to favour or harm a party to a civil, criminal or administrative lawsuit.

Therefore, this is the offence committed by a Company involved in a court case when it corrupts a civil servant (not necessarily a

magistrate, but also the clerk of the court or any other official) in order to obtain a favourable outcome.

vii. Instigation to corruption (art. 322 crim. code),

The punishment foreseen for this offence is applied to anyone who offers or promises money to a civil servant or a person responsible for a public service in order to induce the said person to perform an action that is contrary to his/her official duties, even if the promise of offer is not accepted. Similarly, the punishment is applied in the case of a civil servant who requests such a promise or offer from a private subject.

viii. Extortion (art. 317 crim. code)

This offence consists in the abuse, on the part of a civil servant or a persons responsible for a public service, of his/her position or power by which he/she forces or induces someone to unduly give or promise money or other gain, for him/herself or others.

The offence in question is one of the risks referred to by Lgs. Decree 231/01: since the offence is committed by an authorised subject, the authorising body shall be liable only if a Company employee or representative, in the interests or to the advantage of the same, aids and abets the civil servant or the person responsible for the public service and, taking advantage of his/her position, demands the performance of undue actions or services.

ix. Embezzlement to the prejudice of the State (art. 316 *bis* crim. code)

This offence is committed by the person who has obtained funding, from the State or another public body or the European Union, destined for the execution of works or activities of public interest and who uses the funding for other purposes.

Since the offence consists in failing to use the funding issued for the foreseen purpose, it can also regard funding obtained in the past which has not been used for the purposes for which it was granted.

To complete the review of the offences contemplated by art. 24 of the Decree (extortion, corruption, instigation to corruption and corruption in judicial acts), it is also pointed out that pursuant to art. 322 *bis* of the criminal code, the said types of conduct are also criminal if they regard foreign civil servants, or those in positions equivalent to those of Italian civil servants, in Community organisms, in other member states of the European Union, in foreign countries or in international public organisations.

A.2. THE NOTION OF CIVIL SERVANT AND PERSON RESPONSIBLE FOR A PUBLIC SERVICE (ARTS. 357-358, CRIM. CODE)

Before analysing the crimes of extortion and corruption, it is necessary to clarify the notion of civil servant and person responsible for a public service, being the active subjects of such offences.

In fact, civil servants and those responsible for a public service are:

1. subjects who carry out a legislative or administrative public duty, such as, for example:
 - members of Parliament and of the Government;
 - regional and provincial councillors;
 - members of the European Parliament and of the European Council;
 - subjects who perform complementary duties (those responsible for the conservation of parliamentary deeds and documents, those responsible for the drafting of reports taken down in shorthand, treasurers, technicians, etc.)
2. subjects who hold a public judicial office, such as, for example:
 - magistrates (ordinary magistrates of the lower courts, of the appeal courts, of the Supreme Court, of the Superior Water Court, the Regional Administrative Courts, the Council of State, the Constitutional Court, military courts, justices of the peace, honorary and aggregate district judges, members of arbitration boards, members of parliamentary inquiry commissions, magistrates of the European Court of Justice, and those of the various international courts, etc.);
 - subjects who perform connected services (constables and officers of the CID, of the financial police and of the Carabinieri, court clerks, secretaries, bailees and bailiffs, witnesses, conciliation board officials, official receivers, clerks responsible for issuing certificates from the offices of the clerks of the courts, expert witnesses appointed by the Public Prosecutor, adjusters for arrangement with creditors, court appointed directors of large companies in a state of insolvency, etc.);
3. subjects who hold a public administrative office, such as, for example:
 - employees of the State, of international and foreign organisations, of territorial bodies (such as functionaries and employees of the State, of the European Union, of supra-national bodies and of territorial bodies, including the Regions, the Provinces, the Municipalities and the Mountain Communities; subjects which perform activities complementary to the institutional services of the State,

such as members of municipal technical offices, members of town planning commissions, administrative managers of building permission amnesty offices, town clerks, those in charge of procedures regarding the public land occupancy, employees of municipal labour agencies, employees of public and municipal companies, subjects responsible for tax collection, the personnel of public health service structures, personnel of ministries and of state bureaus, etc.);

- employees of other national and international public bodies (such as officials and employees of the Chamber of Commerce, of the Bank of Italy, of the Supervisory Authorities, of public welfare institutes, of the National Statistics Institute, of the United Nations Organisation, of the Food and Agriculture Organisation, etc.);
- private licensees of public departments or public services (such as notaries public, private subjects acting as concessionaires or whose activity is, in any case, regulated by the provisions of public law and who carry out activities of public interest or who are entirely or partially controlled by the State, etc.);

Activities consisting in the performance of simple duties of keeping order or merely practical duties (i.e. activities of a prevalently applicative or executive nature, without involving autonomy or decision-making, or which foresee solely the expenditure of physical energy, such as dustmen, grave diggers, etc.), although disciplined by provisions of public law, are not considered public service.

Classification as a civil servant or a person responsible for a public service does not depend on belonging to or being employed by a public body, but on the nature of the work actually performed, i.e. a public function or a public service.

A person who is extraneous to public administration may nevertheless be considered as a civil servant or a person responsible for a public service if he/she practises one of the activities defined as such by arts. 357 and 358 of the crim. code (e.g. employees of banking institutes whose duties are classified as public service, etc.).

Furthermore, art. 322 *bis* extends the classification of the offences of corruption and extortion and other offences against public administrations to also include those involving:

- a member of a commission of the European Community, of the European Parliament, the European Court of Justice and Court of Auditors;
- an official or agent operating with the European Community or a subject who carries out equivalent duties;
- a subject who, within the sphere of other member states of the European Union, carries out duties or activities equivalent to those of a civil servant or a person responsible for a public service;

- a subject who performs duties or activities equivalent to those of a civil servant or a person responsible for a public service in a foreign country not belonging to the European Union, or an international public organisation.

A.3. AT-RISK AREAS

The offences referred to above involve relations with a public administration (understood in the wider sense and also including public administrations of foreign countries).

Therefore, all company areas which, in the performance of their business, have relations with public administrations are considered as at-risk areas. Support areas are Company areas which manage financial type instruments and/or equivalent instruments and where, although not holding relations with public administrations, the said offences could be committed.

Therefore, taking into account the many transactions between Telespazio S.p.A. and public administrations in Italy and abroad, the following areas have been identified as specifically at risk:

Areas at the risk of crime:

Sales and Customer Management;

Marketing and Communications;

Institutional Relations;

Management of Litigation;

Grants for training activities;

The management of relations with financial and tax offices;

Job management;

The management of activities relative to authorisations and licences;

The management of activities regarding grants and subsidies;

Relations with welfare and pension institutes;

The management of testing activities;

The management of import and export activities;

The management of procedures foreseen by the laws on safety in the workplace;

The management of industrial security;

The management of the quality system;

The management of agency contracts.

Support areas:

The management of the IT systems;
Management budgeting and auditing;
Customer accounting;
Supplier accounting;
Finance and the treasury;
Administration and taxation;
The management of the Company's equity;
Goods handling management;
Corporate affairs;
Business courtesy initiatives;
Provisioning;
Personnel selection
Human resources development and training;
Administrative and personnel management

The Company Chairman, the Managing Director and the Director General of Telespazio S.p.A. may propose further areas of at-risk activities to the Company's Board of Directors.

The at-risk areas thus identified have been taken as reference for the definition of the audit procedures to be put into practice for the review of the present internal audit system.

The type and frequency of the audit procedures implemented for the various areas at the risk of crime have been defined taking into consideration the importance of the individual points of contact with the Public Administration.

A.4. ADDRESSEES OF THE SPECIFIC SECTION – GENERAL RULES OF CONDUCT AND IMPLEMENTATION OF THE DECISION-MAKING PROCESS IN AT-RISK ACTIVITY AREAS

This Specific Section regards conduct adopted by Directors, Managers and Employees ("Company Representatives") operating in the at-risk areas, and by external collaborators and counterparts, as already defined in the General Section (hereinafter, referred to as a whole as "the Addressees").

This Specific Section foresees that the Company Representatives directly and the External Collaborators and counterparts pursuant to special contractual clauses, are expressly banned from:

- 1) adopting conduct recognised as any of the above-mentioned offences (arts. 24 and 25 of the Decree);
- 2) adopting conduct which, although not in itself criminal and included in those considered above, could potentially become criminal;
- 3) allowing any conflict of interests to develop in relations with the Public Administration in connection with the aforesaid offences.

Within the sphere of the aforesaid conduct (also sanctioned by the Code of Ethics adopted by Telespazio S.p.A.), it is also forbidden to:

- 1) offer money to civil servants;
- 2) distribute gifts apart from those foreseen by Company practice (as ruled by the Code of Ethics, every form of gift offered or received, beyond normal commercial practice or courtesy, or in any case aimed at acquiring preferential treatment in the performance of any Company activity). It is, in particular, forbidden to give any kind of gift to Italian or foreign civil servants (even in those countries where the giving of gifts is normal practice) or their family members, which could influence their independent judgement or induce them to ensure any kind of advantage for the Company. The gifts allowed must be of modest value or for the promotion of artistic initiatives (e.g. the distribution of books on art). Gifts offered – except those of a modest value – must be documented adequately to allow for the prescribed verification;
- 3) agree on other advantages of any nature whatsoever (promises of employment, etc.) in favour of Public Administration representatives which could lead to the same consequences referred to in point b) above;
- 4) perform activities in favour of a counterpart without adequate justification within the context of the relationship established with such counterpart;
- 5) recognise remuneration for external collaborators which is not adequately justified by the type of work to be carried out and the normal practice in force locally;
- 6) present false statements to national or Community public bodies in order to obtain public grants, contributions or subsidised loans;
- 7) use grants, funding or subsidised loans received from national or Community bodies for purposes other than those for which such funds were destined.

For effective adoption of the above conduct:

- 1) relations with public administrations for the above areas of at-risk activities must be managed separately by the various Company representatives, appointing a specific manager for each operation

- or series of operations (in the case of repeated operations) carried out in the area of at-risk activity;
- 2) association agreements with counterparts must be defined in writing, with all the conditions of such agreements clearly highlighted – especially the economic conditions agreed for joint participation in such agreements – and they must be proposed or verified or approved by at least two subjects belonging to Telespazio S.p.A.;
 - 3) duties outsourced to external collaborators must also be contracted in writing, with indication of the agreement remuneration, and undersigned pursuant to the delegations received;
 - 4) no type of payment may be made in cash or kind;
 - 5) Statements submitted to national and Community public bodies in order to obtain grants, subsidies or loans, must contain only elements of absolute truth and, if such funding is obtained, a specific report must be issued;
 - 6) those in a position of control and supervision in respect of the execution of the aforesaid activities (payment of invoices, destination of grants obtained from the State or Community bodies, etc.) must pay particular attention to the implementation of the procedures and must immediately report any irregularities to the SB.

A.5. AREAS OF AT-RISK ACTIVITIES: FUNDAMENTAL ELEMENTS OF THE DECISION-MAKING PROCESS

A.5.1 SINGLE AT-RISK TRANSACTIONS: IDENTIFICATION OF THE INTERNAL MANAGERS RESPONSIBLE AND EVIDENCE FORMS

Due evidence must be given of the operations carried out in the at-risk areas as listed in paragraph A.3 above.

Therefore, the Chairman, the Managing Director, the Director General and the managers of all the departments which carry out at-risk operations are responsible within the Company for every at-risk operation directly carried out in their own department. The said responsible people:

- are the contact persons for at-risk operations;
- are in particular responsible for relations with public administrations for activities involving the latter.

The said responsible persons must inform the SB of at-risk activities by means of the specific Evidence Form (hereinafter "the Form")

which must be periodically updated (see format attached herewith) and which indicates:

- the Public Administrations involved in the procedures of the operation;
- the statement of the responsible person – on his/her own behalf and on behalf of his/her subordinates delegated to perform activities involving the public administration – declaring that he/she is fully aware of the procedures to be carried out and the obligations to be fulfilled in the execution of the operations and that no offences contemplated in the Decree have been committed;
- the indication of the main initiatives and the main procedures carried out in the execution of the operations.

The SB may impose further controls on such operations, of which written evidence will be given.

A. 5.2 INSTRUCTIONS AND VERIFICATIONS OF THE SURVEILLANCE BODY

The Surveillance Body must:

1) issue and update standard instructions on:

- the standardised and coherent compilation of the Evidence Forms;
- ensure the correct attitude is adopted with regard to at-risk activities and, in general in relations with public administrations.

The relative instructions must be in writing and filed on hardcopy or electronic support;

2) periodically check – with the assistance of the other competent departments – the system of delegations in force, recommending modifications if the power in question and/or qualification does not correspond to the powers of representation conferred on the responsible manager or his/her delegated subordinates;

3) periodically check, with the aid of the other competent departments, the validity of suitable standardised clauses aimed at:

- ensuring observance on the part of external collaborators and counterparts of the provisions of the Decree;
- allowing Telespazio S.p.A. to implement effective control over those who must respect the Model in order to verify respect for the prescriptions contained therein;
- implementation of the sanction mechanisms (such as rescission of contract in the case of counterparts or external collaborators) if infringement of the prescriptions is ascertained;

- 4) informing the management of any additions to the financial management system already present in Telespazio S.p.A., with indication of controls that can bring to light the existence of any non-typical financial flows featuring greater margins of autonomy than normally foreseen.

	<h2>Evidence Form</h2>	Doc n: XXX-SDE-ZZZ Page ___ of ___
---	------------------------	---------------------------------------

Name of responsible manager: _____

Period of reference: _____

Company department: _____

To the Surveillance Body of Telespazio S.p.A.

Whereas:

- Telespazio S.p.A. has prepared its own Organisational, Management and Control Model pursuant to Lgs. Decree 231/01;
- the said Model was approved by the Board of Directors on 23/02/2004 and updated by resolution of 28/02/2006 and of 09/06/2009;
- pursuant to point A.5.a of the Specific Part A ("Offences to the prejudice of Public Administrations") every Responsible Manager must fill in an Evidence Form for activities carried out with a public administration;

I, the undersigned, declare that in the period in question I have performed the following main initiatives/activities involving a public administration:

Meeting / contact date	Public Administration / Public Body	Contact person of the Public Administration / Public Body	Purpose of the meeting / contact	Telespazio contact

The documentation, if any, is available at the competent offices of the Company.

I, the undersigned, declare that I am aware of the content of the Organisation, Management and Control Model of Telespazio S.p.A., and with reference to my relations with the above-indicated public administrations – and those of my own collaborators delegated for the purpose and whose activities have been duly controlled and monitored - there are no anomalies or infringements to the Model to report.

(Signed)

.....

Date:/...../.....

SPECIFIC SECTION "B"

Corporate offences, market abuse and connected offences

Other Offences

B.1. TYPES OF CORPORATE OFFENCES AND OF MARKET ABUSE (ARTS. 25 TER AND 25 OF THE DECREE)

The main offences contemplated by arts. 25 *ter* and 25 *sexies* of the Decree, which could in any case benefit the Company, are briefly described below.

i. False corporate information (arts. 2621 and 2622, civil code)

These are two offences which normally coincide almost completely with each other, and which differ only according to whether the shareholders or creditors are prejudiced. The first (art. 2621, civil code) regards intentional infringement; the second (art. 2622, civil code) is an offence involving damages.

The two types of offence consist in financial statement entries or other corporate communications foreseen by law, addressed to shareholders or the public, of tangible facts which, even if valued by estimation, are false and can mislead the recipients of the information relative to the economic, equity or financial situation of the company or the group to which it belongs, with the purpose of deceiving the shareholders, creditors or the general public; or the omission of information on the said situation which must be communicated by law, for the same purpose.

However:

- the behaviour must be intended to obtain unfair gain for the perpetrator or others; the false or omitted information must be relevant and such as to considerably alter the representation of the economic, equity or financial situation of the company or the group to which it belongs;
- the offence will be exempt from punishment if the false or omitted information cause a variation in the before-tax economic result of the period of no more than 5% or a variation in the shareholders' equity of no more than 1%; in any case, the offence will be exempt from punishment if consequent estimates, considered individually, differ by no more than 10% compared to the correct estimates;
- liability also extends to information regarding assets held by the company or administered by the company on behalf of third parties.

The subjects responsible for the offence are the directors, director generals, auditors and liquidators (an offence requiring the perpetrator to hold a specific office).

ii. Fraud in offering circulars (art. 173 bis, TUF)

This offence is committed when the offering circular, a necessary document for soliciting investment or for application for listing on regulated markets, or the documents which must be published when company shares are offered to the public for sale or for exchange, include false information or conceal data of news in order to mislead the recipients of such documents (clause 1) and is a crime if the intended result is achieved (clause 2).

However:

- the perpetrator must be aware of the falsehood and must have acted with the intention of deceiving the recipients of the document (generic malice);
- the behaviour must be such as to mislead the recipients of the document;
- the behaviour must be intended to obtain unfair gain for the perpetrator or others (specific malice).

The offence will be a common offence if it can be committed by anyone.

The offence will be a crime of an infringement according to whether or not economic damage is caused to the recipients of the document.

iii. Fraud in the Audit Firm's reports or communications (art. 2624, civil code)

This offence consists in false statements or concealing information on the part of those responsible for auditing, concerning the company's economic, equity or financial situation with the intention of obtaining unfair gain for oneself or others.

The sanction is more serious if the behaviour has caused economic damage to the recipients of the communications.

Not only the representatives of the Audit Firm are responsible (offence requiring the perpetrator to hold a specific office), but also the members of the Telespazio S.p.A. Board of Auditors and employees who may be actively involved in the offence. Pursuant to art. 110 of the crim. code, in fact, the directors, members of the Board of Auditors, or other subjects of the Auditing Firm, may also be liable if they have determined or instigated the illegal behaviour of the Auditing Firm.

iv. Prevention of inspection (art. 2625 civil code)

This offence consists in hindering or preventing the control and/or auditing – legally held by shareholders, company boards or auditing firms – by concealing documents or other suitable artifices.

The offence, for which solely the directors bear liability, is more seriously punished if prejudice is caused.

v. Transactions to the prejudice of creditors (art. 2629, civil code)

This offence takes place through the reduction of the share capital, mergers with other companies or spin-offs carried out in breach of the provisions of law, which are prejudicial to creditors ("result" offence).

However, the offence is cancelled if the creditors are reimbursed before judgement.

Liability is borne by the directors.

vi. Unfair influence over the shareholders' meeting (art. 2636, civil code)

This offence occurs when a majority is obtained at the shareholders' meeting by simulated acts or fraud for the purpose of obtaining unfair gain for oneself or others.

The offence can be committed by anyone ("common offence"), therefore also by subjects outside the company.

vii. Market rigging (art. 2637, civil code)

This offence consists in the circulation of false information or through transactions or other artifices which cause a considerable alteration in the price of financial instruments, whether listed or not, and which can increase the confidence of the public or of financial institutes in the stability of the equity.

This is also a common offence which can be committed by anyone.

viii. Obstructing supervision on the part of the public supervisory authorities (art. 2638 civil code)

This offence can be carried out in two different ways, both aimed at preventing supervision on the part of the competent public authorities:

- by informing the supervisory authorities of false facts regarding the economic, equity or financial situation, or by partly or completely concealing facts which should be communicated;
- simply by intentionally hindering the supervision in any way.

In both cases, the offence can be perpetrated by the directors, director generals, auditors and liquidators.

ix. Inside trading (art. 184, TUF)

This offence can be perpetrated in three different ways and by anyone holding privileged information due to their position:

- buying or selling financial instruments or carrying out other transactions, carried out directly or indirectly, on one's own behalf or on behalf of others, on the basis of privileged information;
- communicating privileged information to others, outside one's normal professional practice, duties or office;
- recommending or inducing others, on the basis of the privileged information, to carry out any of the operations mentioned in point 1.

In all cases, the offence can be perpetrated by the directors, director generals, auditors and liquidators and all those who have relations with the company because of their profession and/or office.

x. Market abuse (art. 185 TUF)

This offence can be carried out by anyone by the communication of false information or by carrying out simulated transactions or by other artifices which can cause a considerable alteration in the price of financial instruments.

The offence can be perpetrated by the directors, director generals, auditors and liquidators and all those who have relations with the company because of their profession and/or office.

B.2. OTHER OFFENCES

i. Offences against individual personality

This category of offences includes, in particular, the following crimes:

- reduction or maintenance in slavery or servitude (art. 600, crim. code);
- trafficking in human beings (art. 601 crim. code);
- buying and selling slaves (art. 602 crim. code);
- offences connected with child prostitution and exploitation of the same (art. 600 *bis*, crim. code);
- offences connected with child pornography and exploitation of the same (art. 600 *ter*, crim. code);
- detention of pornographic material produced by the sexual exploitation of minors (art. 600 *quater*, crim. code);
- tourist initiatives aimed at the exploitation of child prostitution (art. 600 *quinqües*, crim. code);
- computer pornography (art. 600 *quater*, I crim. code).ⁱ

Pursuant to art. 25 *quinqües* of Lgs. Decree 231/2001, companies are not only fined but also banned from business practice if their directors or employees (as defined by art. 5 of the same Lgs. Decree 231/2001) commit the crimes contemplated by arts. 600, 600 *bis*, clause 1, 600 *ter*, clauses 1 and 2, in the interest or to the advantage of the company, also if regarding the pornographic material referred to in art. 600 *quater*.ⁱⁱ, 600 *quinqües*, 601, 602, of the criminal code.

ii. Transnational offences

Pursuant to art. 3 of the law ratifying the United Nations Convention against organised transnational crime, a transnational offence is "an offence punished with imprisonment for not less than four years, if an organised criminal group is involved and if:

- it is committed in more than one country; or
- it is committed in one country but a substantial part of the preparation, planning and control takes place in another country; or
- it is committed in one country, but an organised criminal group is implicated which is engaged in criminal activities in more than one country; or
- it is committed in one country but has substantial effects in another country."

ⁱ This new offence was introduced by art. 4 of Law n. 38 of 6 February 2006 and punishes anyone who commits the offences contemplated by arts. 600-*ter* and 600 *quater* consisting in the production and electronic transmission of images of minors of less than eighteen years of age or parts of the same.

ⁱⁱ Wording introduced into art 10 of Law n. 38 of 6 February 2006: "Provisions on the fight against the sexual exploitation of children and child pornography also via Internet".

The offence is aggravated if it has involved the contribution of an organised criminal group engaged in criminal activities in more than one country (the punishment is increased by one third to one half).

With regard to the administrative liability of companies for transnational offences, pursuant to art. 10 of the ratification law, the following provisions are applied:

- for the crimes contemplated by arts. 416 (criminal association) and 416 *bis* (Mafia type association) of the crim. code, arts. 291 *quater* of the Consolidate Act of Pres. Decree to 43 (criminal association for the smuggling of tobaccos processed abroad), and art. 74 *quater* of the Consolidate Act of Pres. Decree 309/1990 (association for illegal trading in drugs and narcotics), the company is fined from 400 to 1,000 units, and may be subject to the ban pursuant to art. 9, clause 2, of Lgs. Decree 231/2001, for not less than one year. If the company or one of its organisational units is regularly used solely or prevalently to allow or facilitate the offences referred to in clause 2, it is permanently banned from business practice pursuant to art. 16, clause 3, of Lgs. Decree 231/2001;
- for offences concerning money laundering (arts. 648 *bis* and 648 *ter*, crim. code), the company is fined from 200 to 800 units, and may also be subject to the ban pursuant to art. 9, clause 2, of Lgs. Decree 231/2001, for not less than two years.
- for offences concerning the traffic of migrants (art. 12, clauses 3, 3 *bis*, 3 *ter* and 4 of Lgs. Decree 286/1998) crim. code), the company is fined from 200 to 1,000 units, and may also be subject to the ban pursuant to art. 9, clause 2, of Lgs. Decree 231/2001, for not less than two years.
- for offences concerning the hindering of justice (arts. 377 *bis* and 378, crim. code) the company is fined up to 500 units.
- All administrative offences contemplated by art. 10 are sanctioned by the provisions of Lgs. Decree 231/2001."

B.3. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES

The areas of activity considered more specifically at risk for Telespazio S.p.A. as regards corporate offences are the following:

- 1) the preparation of the financial statement, the management report, the consolidated financial statement and other corporate communications;
- 2) company transactions that in general regard the equity and which can, in particular, affect the integrity of the share capital;

- 3) the allocation of corporate assets by liquidators of certain companies of the Group;
- 4) periodic information given to the financial markets (road shows);
- 5) the activities subject to supervision by public authorities;
- 6) information and reports to the press and other news organisations.

Taking into account the fact that Telespazio SpA belongs to the Finmeccanica Group, the following activities must also be considered:

- 7) safeguarding Finmeccanica's institutional relations with public supervisory authorities, guaranteeing that the Holding Company's communications regarding the economic, financial and equity situation of the Telespazio group are complete, accurate and prompt;
- 8) the management of relations with the press and other news organisations. The circulation of information that is "price-sensitive" for the Telespazio group could indirectly lead to alteration of Finmeccanica share prices.

With regard to the corporate offences of "False corporate information" (art. 2621) and "False corporate information to the prejudice of shareholders and creditors" (art. 2611), items on the financial statement that can considerably alter the representation of the economic, equity and financial situation of the Company and of the Group, and which are therefore relevant with regard to articles 2621 and 2622, have also been included. The factors considered for the identification of the said items are:

- the tangibility of the financial statement items;
- margins of subjectivity in their estimation.

The items identified are:

- Orders in the process of being fulfilled;
- Provisions for risks;
- Equity investments.

For the "Other offences", apart from the above-listed areas at risk for corporate offences and offences against public administrations, the areas regarding the use of internet, the services rendered as a service provider and the activities which involve contact and permanence abroad must also be considered.

This Specific Section not only refers to the specific rules of conduct relative to the above-indicated areas of risk, but also draws attention to the general rules of conduct foreseen by the Code of Ethics adopted by Telespazio SpA which must be observed by the directors and employees of the Company.

B.4. ADDRESSEES OF THE SPECIAL SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS

This Specific Part "B" is addressed to the Directors, the Auditors, the Director General and the managers and their employees, in hierarchical order, who operate in the at-risk activity areas (hereinafter, "the addressees").

The Addressees are expressly obliged to:

- 1) behave correctly and transparently and to offer full collaboration, in respect of legal provisions and the Company's procedures, in all activities aimed at the preparation of the financial statement and the other corporate communications' in order to give shareholders and third parties accurate and correct information of the economic, equity and financial situation of the Company and the Telespazio group.
- 2) adopt correct and transparent conduct and to offer maximum collaboration, in respect of legal provisions and company procedures, to guarantee protection of the investors' assets;
- 3) strictly comply with all provisions of law which protect the company's equity and share capital, and always act according to the company's internal procedures which are based on the said laws, in order to protect creditors and third parties in general;
- 4) ensure correct functioning of the company and of the company boards, guaranteeing and facilitating every form of supervision over the management of the company, pursuant to law, and the free and correct formation of the will of the shareholders' meeting;
- 5) guarantee that the economic, financial and equity information to be communicated to the public supervisory authorities (e.g. information on subsidiaries) also safeguard Finmeccanica's institutional relations;
- 6) always act correctly and truthfully towards the press and other news organisations;
- 7) comply with the rules that will ensure correct prices of the financial instruments, avoiding conduct which can lead to a considerable alteration of the current market situation;

- 8) comply strictly with the provisions relative to offences against the individual personality, especially as regards sexual exploitation of children and child pornography also via internet.

B.5. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT

The modalities for the implementation of the principles referred to above with regard to the various types of corporate offence are given below.

B.5.1. FINANCIAL STATEMENTS AND OTHER CORPORATE INFORMATION

To prevent the offences referred to in letters a) and b) above, the annual company financial statement, management report, six-monthly report, consolidated financial statement and the choice of the Auditing Firm must be based on specific company procedures.

The said procedures must foresee:

- the listing of the data and information that each company department/body must give, to which other departments/bodies they must be transmitted, the criteria for their preparation and the delivery term;
- the transmission of the data and information to the department responsible (the Chief Financial Officer – CFO) by electronic means so that a trace remains of the various transmissions and the identity of the subjects who enter the data into the system;
- the criteria and modalities for the processing and transmission of the consolidated financial statement data on the part of the companies of the Group included in the consolidation, specifying the responsibilities relative to the various steps of the process and the modalities for reconciliation of infra-group balances;
- the terms within which the draft statement and the auditing firm's report must be transmitted to all members of the Board of Directors, of the Board of Auditors and of the SB, and a suitable registration of such transmission;
- meetings between the Auditing Firm, the Board of Auditors and the SB, before the Board of Directors' meeting which will pass resolution on the financial statement;
- the undersigning, on the part of the managers of the departments involved in the preparation of the draft financial statement or other corporate communications, of a statement testifying to the fact that

the data and information transmitted are true, complete and coherent;

- a communication to the SB of the assessments that have led to the choice of the Auditing Firm;
- systematic and prompt communication to the SB of every other mandate conferred, or intended to be conferred, on the Auditing Company in addition to the certification of the financial statement.

In addition, for the preparation of the communications addressed to shareholders, the general public and, in particular, regarding the preparation of the financial statement, the quarterly reports, the six-monthly report, the procedure below must be followed:

the CFO must issue a statement testifying that:

- the data and information contained in the financial statement and in the above-mentioned accounting documents and all connected documents, are true, correct, accurate and complete, as well as the information elements made available by the Company;
- the statements of the truth, correctness, accuracy and completeness on the part of the CFO of the subsidiaries have been received;
- there are no elements which suggest that the statements and data collected contain incomplete or incorrect elements;
- an adequate audit system exists to ensure reasonable certainty regarding the financial statement data;
- the procedures foreseen by this paragraph have been respected.

Copy of the statement must be transmitted to the Surveillance Body.

B.5.2 EXERCISE OF THE POWERS OF CONTROL OVER CORPORATE MANAGEMENT.

To prevent the offences referred to in letter d), paragraph B.1 above, and in implementation of the rules of conduct given in point iv of paragraph B.4 above, the relative activities must be carried out in compliance with the rules of Corporate Governance and Company procedures.

The said procedures must foresee:

- immediate transmission to the Board of Auditors of all documents relative to the matter on the agenda of Shareholders' Meetings and Board of Directors' Meetings or on which the Board must express an opinion;
- access on the part of the Board of Auditors and of the Auditing Firm to the documents relative to the Company's business for the verifications that the two bodies must perform;

- periodic meetings between the Board of Auditors, the Auditing Firm and the SB to check on observance of Company rules and procedures relative to company provisions on the part of the directors, the management and employees;

B.5.3 SAFEGUARD OF THE SHARE CAPITAL

To prevent the offences referred to in letter v., paragraph B.1 above, all transactions on the Company's share capital, the destination of profit and reserves, for the purchase and sale of equity and company branches, for mergers, spin-offs and unbundling, and all operations, also within the group, which could potentially prejudice the integrity of the share capital, must be carried out according to specific company and group procedures laid down specifically for the specific purpose.

The said procedures must foresee:

- the assignment of decisional and operating responsibility for the aforesaid transactions, and mechanisms for coordination between the various company departments involved;
- the communication of information on the part of the Company Management and discussion of the aforesaid operations in meetings between the Board of Auditors, the Auditing Firm and the SB;
- explicit approval from the Telespazio SpA Board of Directors.

B.5.4. OFFERING CIRCULARS

To prevent the offences referred to in letter ii., paragraph B.1 above, offering circulars must be prepared, or jointly prepared, on the basis of specific company procedures.

The said procedures must foresee:

- verification whenever possible to ensure that the data and information are correct;
- if the data and/or information given in the circular are from sources external to the Company, the acquisition of a statement of truth on the part of the external subjects;
- the identification of a person responsible for each step of the drafting – or joint drafting – of the offering circular;
- Immediate transmission of information to the SB by the subject responsible for the operation, for each initiative involving the drafting, or joint drafting of offering circulars, and publication of the same.

Before the works for the drafting of the circular are started, a suitable training programme must be drawn up for all subjects involved in the activity in question, aimed at informing them of the relative laws in force, and of the cases representing the offences of fraud in offering circulars; in addition, adequate support and technical information must be provided for the execution of the competent activity.

B.5.5 ACTIVITIES SUBJECT TO SUPERVISION

To safeguard Finmeccanica's institutional relations with the supervisory bodies, the Holding Company's communications on the economic, equity or financial situation of the Telespazio group must be transmitted according to procedures that assign specific responsibilities, especially in the case of:

- periodic reports pursuant to law and regulations;
- the transmission of requested data and documents;

The procedures must be based on the following principles:

- quality and promptness of the communications;
- reliability of the communications, which must be supported by a reliable computerised system and by effective internal monitoring;
- adequate formalisation of the procedures in question;

during inspections, with the requested documentation being made fully available immediately, and with full collaboration in the performance of the inspection.

All communications and information transmitted to Finmeccanica for the above supervisory activities must also be kept available for the SB for its periodic internal inspections.

B.5.6 MANAGEMENT OF RELATIONS WITH THE AUDITING FIRM

The following directives must be followed in the management of the said relations:

- the personnel within the CFO's department responsible for the transmission of the documentation to the Auditing Firm must be identified;
- the responsible person of the Auditing Firm must have the possibility of contacting the SB for joint verification of situations that present critical aspects regarding the offences considered; also the SB may need to contact the Auditing Firm for the same reason;

- the Auditing Firm or any other companies belonging to the same group may not be assigned advisory duties;
- prior authorisation must be given by the Board of Directors for conferring mandate on the Auditing Firm for any work whatsoever, including auditing of the accounts, except for the mandate conferred pursuant to art. 155 of Lgs. Decree 58/1998;
- the SB must be informed in advance of every mandate proposal referred to in the preceding point;
- independent work contracts or employment contracts may not be stipulated with employees of the company which carries out the obligatory accounting audit for 36 months following:
 - expiry of the contract between Telespazio SpA and the said Auditing Firm, or:
 - termination of the contractual agreement between the employee and the Auditing Firm.

B.6. DUTIES OF THE SURVEILLANCE BODY

The Surveillance Body is responsible for the following duties:

- 1) with regard to the financial statement and other corporate information, since the Telespazio SpA financial statement is certified by an auditing firm, the duties of the SB are limited to:
 - monitoring the effectiveness of the internal procedures and rules of corporate governance in order to prevent the offences of false corporate information;
 - examination of any reports received from the control organs or from any employee and organisation of the verifications deemed necessary;
 - verification of the effective independence of the auditing firm.
- 2) with regard to the other at-risk activities:
 - periodic verification of respect for the internal procedures and rules of corporate governance;
 - periodic verification of communications to the Holding Company of facts regarding the economic, equity or financial situation subject to supervision;
 - monitoring the effectiveness of the verifications aimed at preventing offences;
 - examination of any reports received from the control organs or from any employee and organisation of the verifications deemed necessary.

The SB must report the results of its supervisory and control activities regarding corporate offences every six months to the Board of Auditors.

SPECIFIC SECTION "C"

Offences regarding safety and health in the workplace

C.1. TYPES OF OFFENCE REGARDING HEALTH AND SAFETY IN THE WORKPLACE (ART. 25 –SEPTIES OF THE DECREE)

A brief description is given below of the main offences contemplated by art. 25 *septies* of the Decree.

i. Manslaughter (art. 589 crim. code)

This crime occurs when a person is killed unintentionally subsequent to breach of the provisions for the prevention of accidents in the workplace.

ii. Unintended grievous bodily harm (art. 590, clause 3, crim. code)

This crime occurs when a person unintentionally causes another serious physical harm subsequent to breach of the provisions for the prevention of accidents in the workplace.

The crime, with regard only to events involving breach of the provisions on the prevention of accidents in the workplace or relative to hygiene in the workplace or events resulting in occupational disease, is prosecuted by the Public Prosecutor.

Pursuant to art. 583 of the crim. code grievous bodily harm is:

- serious:
 - if it results in an illness that threatens the victim's life, or an illness or disability which prevents the victim from performing his/her normal activities for a period of more than forty days;
 - if the event produces permanent deficiency in a sense or an organ;
- very serious if the event results in:
 - an illness which is certainly or probably incurable;
 - the loss of a sense;
 - the loss of a limb or a mutilation which renders the limb unserviceable, or the loss of an organ or of the capacity to procreate, or a permanent and serious speech difficulty;
 - facial deformation or disfigurement.

C.2. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES

The analyses carried out have revealed that for the offences contemplated by art. 25 *septies* of the Decree, the at-risk areas, which represent the phases of the safety management system, are those listed below:

- 1) **Planning:** the activities of planning and organisation of roles and of activities linked to health protection, safety and hygiene in the workplace, aimed at establishing objectives coherent with the Company's policy and to establish the processes necessary to reach the objectives and to define and assign resources.
- 2) **Implementation and functioning:** activities aimed at defining organisational structures and responsibilities, training modalities, consultation and communications, document management system modalities, control of documents and data, operational control modalities, and management of emergencies. In particular:
 - system of departmental delegation regarding health, safety and hygiene in the workplace;
 - identification, assessment and management of risks regarding health, safety and hygiene in the workplace;
 - information activities regarding health, safety and hygiene in the workplace;
 - training activities regarding health, safety and hygiene in the workplace;
 - relations with suppliers with regard to activities linked to health, safety and hygiene in the workplace;
 - management of Company assets with regard to activities linked to health, safety and hygiene in the workplace.
- 3) **Auditing and corrective action:** activities aimed at the implementation of modalities for measuring and monitoring performance, the recording and monitoring of accidents, incidents, non-conformities, corrective and preventive action, modalities for the management of the recordings, modalities for the execution of periodic audits.
- 4) **Directors' review:** activities for the periodic review on the part of the top management in order to assess whether the system for the management of health and safety is completely implemented and if it is adequate to achieve the Company's policies and objectives.

The at-risk areas thus identified have been taken as reference for the definition of the audit procedures to be put into practice for the review of the present internal audit system.

The Company has organised its corporate structure for health and safety in the workplace on the basis of the figures indicated below:

- the employer;
- the employer's delegates;
- the prevention and protection service manager;
- the prevention and protection service;
- the Company doctor;
- the workers' safety representative,
- the emergency operators.

C.3. ADDRESSEES OF THE SPECIAL SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS

This Specific Section regards conduct adopted by Directors, Managers and Employees ("Company Representatives") operating in the at-risk areas, and by external collaborators and counterparts, as already defined in the General Section (hereinafter, referred to as a whole as "the Addressees"). This Specific Section foresees that the Company Representatives directly and the External Collaborators and counterparts pursuant to specific contractual clauses, are expressly banned from:

- 1) adopting, collaborating towards or causing conduct which, considered individually or collectively, directly or indirectly represent the offences indicated above (art. 25 *septies* of Lgs. Decree 231/2001);
- 2) breach the principles and Company procedures prescribed in this Specific Section.

C.4. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT

The system of control adopted by the Company foresees, for the at-risk area identified, a series of control protocols, described below:

- 1) For **planning the system for the management of health and safety in the workplace**, the following control protocols have been established:

- ***Policies and Objectives*** This protocol illustrates the policy which defines the orientation and general objectives regarding health and safety which the company intends to reach; the document:
 - is formally approved by the top management of the Company;
 - contains at least the commitment to comply with the applicable laws in force on health and safety and with the other agreed requisites;
 - is adequately circulated among employees and all parties concerned (individuals or groups concerned, involved or influenced by the health and safety in the workplace of a specific organisation);
 - is periodically reviewed to ensure that the objectives are suitable to mitigate the risks present in the organisation and appropriate (e.g. to comply with new regulations and laws).

 - ***Annual and long-term planning*** This is an Investment Plan relative to health and safety in the workplace, approved by the delegated company organs:
 - which clearly indicates expiry dates, responsibilities and the availability of the necessary resources for implementation (financial, human, logistics and equipment);
 - which is adequately circulated within the organisation to ensure that all personnel have sufficient comprehension of the same.

 - ***Legal and other prescriptions*** A set of Company rules define criteria and modalities to be adopted to provide for:
 - revision to comply with the relevant legislation and all other applicable prescriptions on health and safety;
 - identification of where such prescriptions must be applied (company departments) and the modalities for circulation of the same.
- 2) For the **implementation and functioning of the system for the management of health and safety in the workplace**, the following control protocols have been established:
- ***Provisions and documentation of the system*** A set of company rules discipline roles and responsibilities for the management of the documentation relative to the system for the management of health and safety (e.g. Manuals, Procedures, Work instructions), coherent with the Company's policy and guidelines. In particular, the said set of provisions also include modalities for the management, filing and conservation of the documentation produced (e.g. filing/registration modalities to guarantee an adequate level of traceability/verification).

- **Organisation and responsibilities – of the employer**
Organisational provisions identify the employer, taking into account the organisational structure of the Company and of the sector of productive activity.
- **Organisation and responsibilities – PPSM/PPSO/the Company Doctor/WSM/Emergency operators**
Organisational provisions discipline the appointment of the Prevention and Protection Service Manager (PPSM), the Prevention and Protection Service Operators (PPSO), the Company Doctor, the Workers' Safety Manager (WSM) and the Emergency Operators, which:
 - define the specific requisites in compliance with the relative laws;
 - foresee the traceability of checks carried out on the holding of the specific requisites foreseen by the relative legal provisions;
 - foresee assessment of personnel to understand the capacities and availability as regards time in order to cover such specific roles;
 - foresee the traceability of the formal acceptance of the office.
- **Organisation and Responsibilities – safety on temporary or mobile worksites²⁰**. When foreseen by the laws in force²¹, these company provisions:
 - discipline the modalities for identifying and assigning the position of Coordinator for matters of health and safety for the planning of works and Coordinator for matters of health and safety during the execution of the work, taking into account the professional requisites foreseen by law;
 - foresee the traceability of the assessment of the requisites and acceptance of the office on the part of the Coordinators.
- **System of departmental delegations**
This is a system of departmental delegations based on the following principles developed by case law:
 - effectiveness-existence and simultaneous decisional and financial autonomy of the delegate²²;
 - adequate technical-professional skill and experience on the part of the delegate²³;

²⁰ Any place where building or civil engineering works are carried out, the list of which is given in annex X to Lgs. Decree 81/2008.

²¹ The employer and contracting party for a work contract as specified by art. 89, letter b) of Lgs. Decree 81/2008.

²² An official system of delegations relative to health and safety and a set of company rules which guarantee verification of traceability and of the permanence of the delegations, which clearly indicates whether the delegation or sub-delegation is effective for matters of health and safety and which foresees traceability of the criteria on the basis of which coherence between delegated offices and decisional and expenditure powers is determined.

- supervision of the delegate's activity, non-acquiescence and diligence²⁴;
 - certainty, specificity and awareness²⁵.
- ***Risk detection and assessment – Roles and responsibilities***
 This company procedure indicates roles, responsibilities and modalities for the execution, approval and updating of the global and documented assessment of all risks present in the Company. The procedure must, in particular:
- indicate roles, authority, requisites of skill and training needs for the personnel responsible for detecting and controlling danger and risks;
 - identify the subjects responsible for verification, approval and updating of the contents of the Risk Assessment Document (RAD);
 - indicate modalities and criteria and the specific terms or periods for review of the danger and risk detection and assessment processes;
 - foresee, when necessary, the traceability of the involvement of the Company Doctor in the process of danger and risk detection and assessment;
 - foresee assessment of the various types of sources of risk: ordinary or generic hazards, ergonomic hazards, specific hazards, process and organisational hazards and the identification of similar areas in terms of danger within the Company;
 - foresee indication of the duties of the workers' representatives;
 - foresee the survey and characterisation of the chemical agents and equipment and machinery present;
 - foresee explicit definition of the assessment criteria adopted for the various risk categories, pursuant to the laws and prescriptions in force.
- ***The Risk Assessment Document (RAD)*** This document, drawn up pursuant to the provisions defined, reports risk assessment and contains at least:

²³ A company provision which defines the procedures for checking whether the delegate continues to hold the technical-professional requisites, and a plan for periodic refresher courses and for the technical-professional development of the delegate, and a system of periodic assessments of his/her technical-professional skills.

²⁴ An official continuous/periodic information flow between the delegating body and the delegate and on the relative official supervision.

²⁵ An official system of delegation on health and safety in which the operating scope is clearly indicated and company provisions which foresee the traceability of the acceptance of the delegations.

- the assessment procedure, with specification of the criteria adopted;
 - indication of the prevention and protection measures and the personal protection devices, consequent to the assessment;
 - the programme of the measures deemed opportune to guarantee improvement of safety levels over time.
- **Operational control – assignment of tasks and duties** This Company provision indicates the criteria and modalities defined for entrusting tasks and duties to the workers on the part of the Employer. The provision must, in particular:
- define the criteria for the assignment of tasks to the worker on the basis of his/her capacity and condition, and considering his/her health and safety and the results of the medical examinations performed;
 - define the organisational measures for the participation of the Company Doctor and of the PPSM in the definition of the workers' roles and responsibilities;
 - foresee the traceability of the assessment activities carried out for this purpose (e.g. definition of the specific check lists such as lists of critical tasks and/or processes with impact on health and safety).
- **Operational control – Personal protection devices (PPD)** A company provision provides for the management, distribution and maintenance in an efficient state of the Personal Protection Devices. The provision must, in particular:
- define modalities for verification of the necessary requisites such as the strength, suitability and duration in good condition and efficiency of the PPD;
 - foresee the traceability of the activities of delivery and verification of the functionality of the PPD (e.g. specific check lists such as lists of the PPD to be delivered, shared with the Prevention and Protection Service Manager).
- **Emergency management** A company provision provides for the management of emergencies in order to mitigate the effects on the health of the population and on the external environment. The provision must, in particular:
- indicate the measures for controlling the risk situation in the case of an emergency;
 - indicate the modalities for the evacuation of the workplace or the danger zone in which there is serious and immediate danger;
 - indicate the modalities for the intervention of the workers appointed to implement the fire-fighting and evacuation

- measures in the case of serious and immediate danger, and the first aid measures;
- indicate the modalities to avoid risks for the health of the population or deterioration of the external environment;
 - indicate the modalities and timing/frequency of emergency drills.
- **Management of the fire risk** A Company provision defines the measures necessary for the prevention of fires. The provision must, in particular:
- provide for the monitoring of the activities to be carried out for the application and renewal of the PPD;
 - indicate the modalities for informing workers of the conduct to be adopted in the case of fire;
 - indicate the modalities for keeping and updating the fire record.
- **Consultation and communications**
- A calendar is drawn up of the periodic meetings of all subjects responsible for verification of the situation for management of matters regarding health and safety and for the adequate communication of the results of the meeting within the organisation.
 - A company provision disciplines the communication of the information on health and safety. The provision specifically disciplines:
 - the information to be periodically communicated by the employer to the employees;
 - the information to be communicated to the Company Doctor, when necessary, regarding the processes and risks involved in production.
- **Training, sensitisation and skills** A company provision disciplines training. The provision must, in particular:
- define the modalities for providing training for every worker on: company risks, prevention and protection measures, specific risks and safety rules, characteristics of the hazardous substances (safety forms and rules of good practice), emergency procedures, the names and the roles of the PPSM and of the Company Doctor, and instructions for the use of work equipment, when applicable, and for the use of the PPD;
 - define the criteria for providing training for every worker (e.g. hiring, transfer or change of duties, the introduction of new equipment, technologies or hazardous substances);
 - for subjects involved in the management of health and safety matters, indicate the sphere, contents and modalities of training with regard to the role undertaken within the organisational

- structure (Workers' Safety Representatives, Protection and Prevention Operators, Emergency and First Aid teams);
- define the timing for providing workers with training on the basis of the modalities and criteria defined (definition of an annual training plan).
- ***Relations with suppliers and contractors – information and coordination*** A company provision defines:
- modalities and contents of the information which must be given to external companies regarding all the provisions and prescriptions that a work contractor must know and undertake to respect and ensure his/her employees respect;
 - roles, responsibilities and modalities for the processing of the Risk Assessment Document which indicates the measures to be adopted in order to eliminate risks due to interference between workers if several companies are involved in the execution of a job.
- ***Relations with suppliers and contractors – qualification*** A company provision defines modalities for the qualification of suppliers. The provision must, in particular, contain:
- the results of the verification of the technical-professional requisites pursuant to art. 90, clause 9, of Lgs. Decree 81/08;
 - specifications of what may be supplied, together with purchasing specifications and the best technologies available, with regard to the protection of health and safety.
- ***Relations with suppliers and contractors – contractual clauses*** Standard contractual clauses specify the safety costs in purveyance contracts, work contracts and sub-contracts.
- ***Asset management*** Company provisions specify the maintenance/inspection activities of company assets in order to always guarantee the integrity and adequacy of the same. The provisions, in particular, foresee:
- periodic verification of the adequacy and integrity of the assets and conformity to the applicable legal requisites;
 - the planning, execution and verification of the inspection and maintenance activities carried out by suitable, qualified personnel.
- 3) For **auditing and corrective action**, the following control protocols have been established:
- ***Measuring and monitoring performance - accidents*** A company provision indicates:

- roles, responsibilities and modalities for detecting, recording, and internal investigation of accidents;
 - roles, responsibilities and modalities for the traceability and investigation of incidents/accidents which occur²⁶ and for near incidents/accidents²⁷;
 - the modalities by which the operators concerned must inform the employer and the protection and prevention service manager of the accidents/incidents which occur.
- ***Measuring and monitoring performance – other data (other than accidents and incidents)*** Company provisions define roles, responsibilities and recording and monitoring modalities (also through the use of indicators) for:
- data regarding health monitoring;
 - data regarding the safety of plant (lifting gear and lifts, electrical systems, equipment under pressure, underground tanks, laser appliances, machines);
 - data regarding hazardous substances and preparations used in the company (safety forms).
- ***Measuring and monitoring performance – lawsuits/disputes*** Company provisions define roles, responsibilities and modalities for monitoring disputes and lawsuits pending regarding accidents in the workplace, in order to identify areas where there is greater risk of accident.
- ***Auditing*** A company provision disciplines roles, responsibilities and operating modalities for the auditing and periodic verification of the efficiency and effectiveness of the safety management system. The provision, in particular, defines:
- the timing for the programming of the activities (official Audit Plan);
 - the skills required of the personnel involved in audit activities, in consideration of the auditor's independence and the activity which must be audited;
 - the modalities for recording audits;
 - the modalities for identifying and applying corrective action if there is a relevant deviation from what is prescribed by the system for the management of health and safety in the company or other applicable prescriptions;
 - the modalities for verification of the implementation and effectiveness of the aforesaid corrective action;

²⁶ Events which result in harm (in the case of physical harm to a person, the term "accident" is used).

²⁷ Incidents which involve a high potential of risk, but which have not produced any damage, or only marginal damage.

- the modalities for informing the Company's top management of the audit results.
 - **Reporting.** A company provision disciplines roles, responsibilities and modalities for reporting to the Surveillance Body and the Top Management.
- 4) For **the Directors' review**, the following control protocols have been established:
- **Execution of the review process** A company provision defines roles, responsibilities and operating modalities for the execution of the review carried out by the company top management regarding the effectiveness and efficiency of the system for the management of health and safety in the company. The provision foresees the traceability of the performance of the following activities:
 - the analysis of any deviation between the results obtained the programmed targets;
 - the analysis of the Audit results;
 - the analysis of the results of the monitoring of the performance of the system for the management of health and safety (accidents, other data);
 - the state of progress of any improvement actions defined in the previous review;
 - indication of the improvement targets for the next period and the need for any modifications to elements of the system for the management of health and safety in the company.

C.5. THE DUTIES OF THE SURVEILLANCE BODY

The Surveillance Body's duties are the following:

- 1) to monitor the internal procedures for the prevention of offences relative to health and safety.

This task must be carried out also taking into account the following information flows:

- communication by the PPSM of every modification and/or revision of the Risk Assessment Document;
- minutes of the periodic risk prevention and protection meetings (art. 35 of Lgs. Decree 81/2008), by the PPSM;

- every revision linked to changes in the responsibilities conferred pursuant to Lgs. Decree 81/2008, communicated by the Human Resources, Organisation and Information Technology department;
 - any reports from the control organs or any employee concerning shortcomings or inadequacies of workplaces or equipment, or of the PPD made available by the company, and any other situation of danger linked to health and safety in the workplace;
- 2) To periodically verify, with the assistance of the other competent departments, any standard contractual clauses regarding safety costs in purveyance contracts, work contracts and sub-contracts;
- 3) six-monthly interviews with the PPSM on the activities of competence and on the aspects linked, in general, to planning accident prevention provisions and on the protection of hygiene and safety at work.

SPECIFIC SECTION "D"

**Receiving, money laundering and the use of cash, goods or other
gain from illicit acts**

D.1. TYPES OF OFFENCE REGARDING RECEIVING, MONEY LAUNDERING AND THE USE OF MONEY, ASSETS OR OTHER VALUABLES OF ILLICIT PROVENANCE (ART. 25 OCTIES OF THE DECREE)

Art. 63, clause 3, Lgs. Decree 231 of 27 November 2007 has introduced into the category of offences regarding administrative liability pursuant to Lgs. Decree 231 of 2001, art. 25 *octies* pursuant to which a company can be fined and barred from practice for the offences of receiving, money laundering and the use of money, assets or other gain of illicit provenance (offences contemplated by arts. 648, 648-*bis* and 648-*ter* of the criminal code).

Art. 64, clause 1, letter f), of the same provision has also abrogated clauses 5 and 6 of art. 10 of Law 146/2006, against transnational organised crime, pursuant to which the company bore liability and was sanctioned pursuant to Lgs. Decree 231/2001 for the offences of money laundering and the use of money, assets or other gain of illicit provenance (arts. 648-*bis* and 648-*ter*, crim. code), if featuring elements of transnationality, according to the definition given in art. 3 of the said law 146/2006.

Consequently, pursuant to art. 25 *octies* of Lgs. Decree 231/2001, the company can now be punished for offences of receiving, money laundering and the use of illicit capital even if carried out in a strictly national sphere, always providing the company itself derives an interest or an advantage. A brief description is given below of the main offences contemplated by art. 25 *octies* of the Decree.

i. Receiving (art. 648 crim. code)

Pursuant to art. 648, crim. code, "apart from the cases of aiding and abetting, anyone who buys, receives or conceals, or who is in any case involved in buying, receiving or concealing, money or other assets resulting from any crime" can be prosecuted.

Buying must be understood as the effect of a negotiating activity, in exchange for cash or without payment, by which the agent obtains possession of the asset.

Receiving indicates any form by which possession of the asset resulting from crime is obtained, even if only temporary or merely as a favour.

Concealment refers to hiding the asset resulting from a crime after receiving it.

Receiving can also involve the purchase, the receiving or the concealment of the asset. Such conduct is recognised in every activity

of mediation, not understood in the sense of the civil code (as specified by case law), between the perpetrator of the main offence and the third party buyer.

The last clause of art. 648, crim. code, extends the offence to also include the case in which "the perpetrator of the crime, from which the money or assets result, cannot be charged or punished since he/she cannot be prosecuted for the said crime".

The purpose of charging the subject who receives the asset is to prevent the perpetration of the harm to the economic interests which began with the perpetration of the main crime. A further purpose for the charge is to avoid the perpetration of the main crime, as a consequence of the limits imposed on the circulation of gain resulting from such crime.

ii. Money laundering (art. 648 *bis* crim. code)

This offence is recognised when someone "except for the cases of aiding and abetting, substitutes or transfers cash, assets or other gain resulting from crimes of malicious intent: or carries out other operations on such gain in order to hinder the identification of the criminal provenance". The crime in question also exists even when the perpetrator of the crime from which the gain results cannot be charged or punished since he/she cannot be prosecuted for the said crime". However, the offence requires a criminal act to have been committed first, although the money launderer may not have had any part in the same.

The punishment is greater when the offence is committed within the sphere of professional practice, and it is lesser if the money or other gain results from a crime for which the punishment is imprisonment of no more than five years.

The provision is applicable even when the perpetrator of the crime from which the gain results cannot be charged or punished since he/she cannot be prosecuted for the said crime". Any obstacles imposed to prevent the identification of the said assets after they have been substituted or transferred have a relevant effect.

iii. Use of money, property or other gain of illegal provenance (art. 648 *ter* crim. code)

This offence is committed by "anyone, except for cases of aiding and abetting and the cases foreseen by arts. 648 crim. code (receiving) and 648-*bis* crim. code (money laundering), who uses cash or assets or other gain resulting from crime in economic or financial activities".

Also in this case, the use of the assets within the sphere of a professional activity is an aggravating circumstance and the last clause

of art. 648 is extended to such subjects, although punishment is decreased if the amount involved is particularly modest.

The specific use of the term "use", with a wider meaning than "invest" which supposes use aimed at particular objectives, expresses the meaning of "use in any manner". However, the use of the term "activity" to indicate the investment sector (economic or financial activities) allows for the exclusion of the occasional or sporadic use of money or other assets.

The specific nature of the offence, compared to that of money laundering, lies in the attempt to prevent the illicit provenance of the money, assets of other gain to be traced, pursued by the use of the said resources in economic or financial activities.

The legislator's intention is to punish such mediation activities which, unlike money laundering, do not immediately substitute the gain resulting from crime, but which in any case contribute to the "laundering" of illicit capital.

D.2. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES

The analyses carried out have revealed that for the offences contemplated by art. 25 *octies* of the Decree, the at-risk area is Administration, Finance and Control, with reference to the "*Management of financial transactions*".

D.3. ADDRESSEES OF THE SPECIFIC SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS

The following rules of conduct, of a general nature, apply to both the Addressees of the Model who, for any reason whatsoever, are involved in the areas at risk as regards the offences of receiving, money laundering and the use of money, assets or other gain of illicit provenance.

In general, such subjects are required:

- 1) to guarantee that every operation or transaction is correctly and promptly registered in the company's accounting system according to the criteria indicated by law and on the basis of the applicable accounting standards; every operation or transaction must be authorised, verifiable, legitimate, coherent and congruent;
- 2) to make payments in the interests of the Company only if there is adequate supporting documentation.

It is forbidden to receive or accept, in any way and under any circumstances, the promise of payment in cash, or to risk being implicated in events linked to the recycling of money deriving from illicit or criminal activities.

D.4. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT

The system of control adopted by the Company foresees, for the at-risk area of Administration, Finance and Control and with reference to the management of financial transactions, a series of control protocols, described below:

- 1) **Regulation:** the process in question must be regulated by specific documentation on internal organisation which disciplines the management of financial flows. Within the sphere of the said process, the roles and responsibilities of the subjects appointed to manage the various steps must be defined, as well as the protocols for prevention which these latter must apply. In particular, the process must be described distinguishing between the incoming and outgoing financial flows. Furthermore, the following preventive protocols must be foreseen:
 - checks carried out when entering/modifying the identity data of suppliers/customers in the system, aimed at ensuring complete correspondence between the name of the supplier/customer and the name of the holder of the account to/from which the payment must be made/accepted;
 - payment/collection is allowed only to/from subjects present in the identity database;
 - payments may not be made to/received from accounts identified by a code;
 - it is forbidden to use cash or other financial instruments to bearer for any collection, payment or transfer transaction, or any other use of funds, and transfers to or from current or savings accounts held anonymously or in a fictitious name are also forbidden;
 - it is forbidden to use credit institutes without physical head offices (managed entirely through electronic means and internet);
 - the ceilings and limits defined for payments must be respected.
- 2) **Traceability:** All steps of the financial flows must be documented and traceable.
- 3) **Separation of tasks:** the process must be carried out in accordance with the principle of the separation of tasks between the departments involved in approval, execution and control.

- 4) ***Powers of proxy and delegations:*** the process must prescribe that the activities must be carried out pursuant to the provisions of the Company's Articles of Association, its internal system of powers of proxy for the assignment of the power to represent and sign on behalf of the Company, and the system of internal delegations for the performance of the activities of competence.

D.5. THE DUTIES OF THE SURVEILLANCE BODY

The SURVEILLANCE BODY must:

- 1) periodically verify, with the assistance of the other competent departments:
 - the powers of proxy in force, recommending modifications if the power for management and/or the qualification of the delegate does not correspond to the conferred power of signature;
 - the ceilings foreseen for payments;
- 2) monitor the effectiveness of the internal procedures for the prevention of the offences of receiving, money laundering and the use of assets, money or other gain of illicit provenance, in particular as regards full coincidence between the subject receiving/ordering the payments and the counterparts effectively involved in the transactions, the registered head office of the counterpart (e.g. tax havens), and the credit institutes used (e.g. head offices of banks involved in the transactions and institutes which do not have physical head quarters anywhere).

These tasks shall be carried out also taking into account any reports from the control organs or from any employee.

SPECIFIC SECTION "E"

Computer crimes and illegal data processing

E.1. TYPES OF COMPUTER CRIMES AND ILLICIT DATA PROCESSING (ART. 24 *BIS* OF THE DECREE)

Law n. 48 of 18 March 2008 on the "Ratification and execution of the European Council Convention on computer crime, signed in Budapest on 23 November 2001, and adaptation provisions of the entire discipline" has further extended the range of offences for which the company can bear liability. Art. 7 of the said provision has introduced art. 24 *bis*, "Computer crime and illicit data processing", into Lgs. Decree 231/2001.

A brief description of the main offences contemplated by art. 24 *bis* of the Decree is given below.

i. Electronic documents (art. 491 *bis* crim. code)

"In the case of any fraud contemplated by this article regarding a public or private electronic document with probative force, the provisions of the article concerning respectively public deeds and private contracts are applied."

The above provision makes fraud by the use of electronic documents a criminal offence; a list of such offences is given below:

- Tangible fraud committed by a civil servant in public deeds (art. 476, crim. code)

This is the offence committed by a civil servant who, in the performance of his/her duties, creates a completely or partially false deed or alters a true deed.

- Tangible fraud committed by a civil servant in certificates or administrative authorisations (art. 477, crim. code)

This is the offence committed by a civil servant who, in the performance of his/her duties, forges or alters certificates or administrative authorisations, or who causes them to appear valid by counterfeit or alteration.

- Tangible fraud committed by a civil servant in authenticated copies of public or private deeds and in certifications of the content of deeds (art. 478, crim. code)

This is the offence committed by a civil servant who, in the performance of his/her duties, supposing that a public or private deed exists, issues a simulated copy in legal form or issues a copy of a public or private deed which differs from the original.

- **Ideological fraud committed by a civil servant in public deeds (art. 479, crim. code)**

This is the offence committed by a civil servant who, receiving or drafting a deed in the performance of his/her duties, falsely swears that he performed a deed or that the deed was performed in his/her presence, or who swears that he/she has received statements that have not been submitted to him/her, or who omits or alters statements that he/she has received, or who anyway falsely declares facts which are destined to be proven true by the deed.

- **Ideological fraud committed by a civil servant in certificates or administrative authorisations (art. 480, crim. code)**

This is the offence committed by a civil servant who, in the performance of his/her duties, makes false statements, in certificates or authorisations, which are destined to be proven true by the deed.

- **Ideological fraud in certificates committed by a person performing a necessary public service (art. 481, crim. code)**

This crime can be committed by any person who works for the health service or in the legal profession or any other necessary public service, if the person makes a false statement in a certificate, which is destined to be proven true by the deed.

- **Tangible fraud committed by a private individual (art. 482, crim. code)**

This crime is committed by a private person who adopts the behaviour contemplated by arts. 476, 477 and 478.

- **Ideological fraud committed by a private individual in public deeds (art. 483, crim. code)**

This is the offence committed by a person who makes a false statements in a public deed, which is destined to be proven true by the deed.

- **Fraud in registers and notifications (art. 484, crim. code)**

This crime can be committed by anyone who is obliged by law to make registrations subject to the inspection of the police force, or who notifies the police service of his/her own industrial, commercial or professional operations, writing or allowing others to write false indications.

- **Fraud in private deeds (art. 485, crim. code)**

This crime is committed by anyone who, in order to obtain an advantage for him/herself or others or to damage others, completely or

partially creates a false private contract, or who alters a true private contract.

Alterations also include riders falsely added to a true deed after it has been definitively completed.

- **Fraud in a signed blank sheet. Private deed (art. 486 crim. code),**

This is the offence committed by anyone who, in order to obtain an advantage for him/herself or others or to cause damage to others, abuses a signed blank sheet of which he/she has gained possession for a purpose which involves the obligation or the faculty to fill in the blank sheet, writes or makes others write on the sheet a private deed which produces legal effects other than those which he/she was obliged or authorised to write.

A signed blank sheet must be understood as any sheet on which the person undersigning the same has left a blank space destined to be filled in.

- **Fraud in a signed blank sheet. Public deed (art. 487 crim. code),**

This is the offence committed by a civil servant who, abusing a signed blank sheet, of which he/she has gained possession in the course of his/her duties and for a purpose involving the obligation or faculty to fill in the same, writes or makes others write on the sheet a public deed different from that which he/she was obliged or authorised to write.

- **Other frauds in a signed blank sheet. Applicability of the provisions on tangible fraud (art. 488, crim. code)**

This offence is committed in the case of a false statement written on a signed blank sheet other than those indicated by the two preceding articles.

- **Use of a false deed (art. 489 crim. code),**

This offence is committed by anyone who, without being a party to the creation of the fraudulent deed, makes use the same.

In the case of a private deed, the perpetrator of the fact can be punished only if he/she has acted in order to obtain an advantage for him/herself or others or to cause damage to others.

- **Suppression, destruction and concealment of true deeds (art. 490, crim. code).**

This offence is committed by anyone who completely or partially destroys, suppresses or conceals a true public or private deed.

- **Authenticated copies which replace missing originals (art. 493, crim. code)**

The effects of the previous provisions, the term "public deeds" and "private deeds" include the original copies and the authenticated copies of the same, when they legally replace the missing originals.

- Fraud committed by a civil servant responsible for a public service (art. 493, crim. code)

Pursuant to art. 493, crim. code, the provisions of the preceding articles on fraud committed by public officials also apply to civil servants responsible for a public service regarding deeds which they must draw up in the performance of their duties.

ii. Unauthorised access to a computerised or electronic communication system (art. 615 *ter* crim. code)

Art. 615 *ter* punishes a person who gains unauthorised access to a computerised or electronic communication system protected by security measures or remains there against the express or tacit will of the subject with the right to exclude him/her.

Higher sanctions are applied if:

the fact is committed by a civil servant abusing his/her powers or by breach of his/her duties or service, or by a person who, also abusively, practises the profession of private investigator, or by the system operator abusing his/her position;

the perpetrator commits violence on property or persons, or who is clearly armed;

the fact derives from the destruction of or damage to the system or the total or partial interruption of its functioning, or the destruction of or damage to the data, information or programmes contained therein.

The sanction will also be aggravated if the above-described facts regard computer or electronic communications systems of military interest or relative to public order or security or health or civil defence or, in any case, of public interest.

iii. Detention and unauthorised disclosure of access codes to computer or electronic communication systems (art. 615 *quater* crim. code)

Art. 615 *quater* sanctions anyone who, in order to obtain gain for him/herself or others or to cause damage to others, abusively obtains, reproduces, circulates or delivers codes, passwords or other means of access to computer or electronic communication systems protected by security measures, or who in any case gives indications or instructions for the aforesaid purpose.

Heavier sanctions are applied if the fact is committed:

to the prejudice of a computer or electronic communication system used by the state or by another public body or by companies which perform a public service or which provide for a public need;
by a civil servant abusing his/her powers or by breach of his/her duties, or by the system operator abusing his/her position;

Circulation of equipment, devices or computer programmes intended to damage or interrupt a computer or electronic communications system (art. 615 *quinquies* crim. code)

Art. 615 *quinquies* contemplates the phenomenon of the circulation of so-called viruses.

The provision punishes anyone who, in order to illicitly damage a computer or electronic communication system, or the information, data or programmes contained therein or pertinent to the same, to favour the total or partial interruption, or alteration of its functioning, obtains, produces, reproduces, imports, circulates, communicates, delivers or, in any case, makes available to others appliances, devices or compute programmes.

Unauthorised interception, hindrance or interruption of computer or electronic communications (art. 617 *quater* crim. code)

Art. 617 quarter (like art. 617 *quinquies* below) is a provision intending to protect the security and the authenticity of IT and electronic communications.

The provision punishes:

- anyone who fraudulently intercepts, hinders or interrupts communications with a computer or electronic system or communications between several systems;
- anyone who reveals, in any way, to the public all or part of the content of computer or electronic communications intercepted.

Heavier sanctions are applied if the fact is committed:

- to the prejudice of a computer or electronic communication system used by the state or by another public body or by companies which perform a public service or which provide for a public need;
- by a civil servant abusing his/her powers or by breach of his/her duties, or by the system operator abusing his/her position;
- by a person who exercises, also abusively, the profession of private investigator.

vi. Installation of equipment designed to intercept, hinder or interrupt computer or electronic communications (art. 617 *quinquies* crim. code)

Art. 617 *quinquies* punishes the installation, except when allowed by law, of appliances which serve to intercept, hinder or interrupt communications of a computer or electronic communications system or those between several systems.

Heavier sanctions are applied if the fact is committed:

- to the prejudice of a computer or electronic communication system used by the state or by another public body or by companies which perform a public service or which provide for a public need;
- by a civil servant abusing his/her powers or by breach of his/her duties, or by the system operator abusing his/her position;
- by a person who exercises, also abusively, the profession of private investigator.

vii. damage to information, data and computer programmes (art. 635 *bis* crim. code)

This offence is committed by anyone who destroys, deteriorates, cancels, alters or suppresses information, data or computer programmes belonging to others.

Heavier sanctions are applied if the fact is committed with personal violence or threat or by the system operator in abuse of his/her position.

viii. Damage to information, data and computer programmes used by the State or other public body or, in any case, of use to the general public (art. 635 *ter* crim. code)

This offence is committed when an action is aimed at the destruction, deterioration, cancellation, alteration or suppression of information, data or computer programmes used by the State or any public body or a subject connected with the same, or which are, in any case, of public usefulness.

Heavier sanctions are foreseen if the fact derives from the destruction, deterioration, cancellation, alteration or suppression of the information, data or computer programmes.

A heavier sanction is also foreseen if the fact is committed with personal violence or threat or by the system operator in abuse of his/her position.

ix. Damage to computer and electronic communication systems (art. 635 *quater* crim. code)

Art. 635 *quater* punishes anyone who, by the behaviour referred to in the aforesaid article 635 *bis*, or through the introduction or transmission of

data, information or programmes, destroys, damages or make entirely or partially unserviceable the computer and electronic communications systems of others, or who seriously hinders functioning.

A heavier sanction is foreseen if the fact is committed with personal violence or threat or by the system operator in abuse of his/her position.

x. Damage to computer and electronic communication systems of public use (art. 635 *quinquies* crim. code)

This provision foresees sanctions if the fact contemplated by the aforesaid article 635 *quater* is aimed at destroying, damaging, rendering entirely or partially unserviceable, computer or electronic systems of public use or at seriously hindering functioning.

Heavier sanctions are foreseen if the fact results in the destruction of or damage to the computer or electronic communication system of public use, or if the system is rendered completely or partially unserviceable.

A heavier sanction is also foreseen if the fact is committed with personal violence or threat or by the system operator in abuse of his/her position.

xi. Computer fraud on the part of the subject which performs certification services with electronic signature (art. 640 *quinquies* of the crim. code)

Art. 640 *quinquies* punishes the behaviour of a person who issues certificates bearing an electronic signature if he/she, in order to obtain unfair gain for him/herself or others or to cause damage to others, breaches the obligations foreseen by the law for the issue of a recognised certificate.

E.2. MAIN AREAS OF ACTIVITY AT THE RISK OF THE PERPETRATION OF THE OFFENCES

The analyses carried out have indicated, relative to computer crimes and the illicit processing of data, contemplated by art. 35 bis of the Decree, the following risk areas:

Human Resources, Organisation and Information Technology (which also includes the Security Manager)
Engineering lines;
Operations

with reference to the following single activities:

- 1) management of users' profiles and of the authentication process;
- 2) management and protection of the workstation.
- 3) management of access incoming and outgoing external access;
- 4) network management and protection;
- 5) management of system outputs and of memorisation devices (e.g. USB, CD).
- 6) Physical security (including cabling security, network devices etc.).
- 7) Production and/or sale of computer appliances, devices or programmes and of software, hardware, network installation and maintenance services; the purchase, development and maintenance of computer appliances, devices or programmes destined for the market and the supply of services for customers inherent to the management of the same.

E.3. ADDRESSEES OF THE SPECIFIC SECTION – GENERAL RULES OF CONDUCT IN AT-RISK ACTIVITY AREAS

The following rules of conduct, of a general nature, apply to both the Addressees of the Model who, for any reason whatsoever, are involved in the at-risk areas in respect of computer crimes and unauthorised data processing. In general, such subjects are forbidden:

- 1) to adopt, collaborate towards or instigate conduct which, considered individually or collectively, directly or indirectly represents the offences indicated above (art. 24 *bis* of Lgs. Decree 231/2001);
- 2) to breach the principles and Company procedures prescribed in this Special Section.

Within the sphere of the aforesaid rules, it is specifically forbidden to:

- alter public or private electronic documents which have probative value;
- enter the computer or electronic communications systems of public or private subjects without authorisation;
- enter the company's own computer or electronic communication system to alter and/or cancel data and/or information without authorisation;
- hold and use without authorisation codes, passwords or other means of access to a computer or electronic communication system of public or private competitors, in order to acquire confidential information;
- hold and use without authorisation codes, passwords or other means of access to the company's computer or electronic communication system, in order to acquire confidential information;

- perform provisioning and/or production and/or distribution of hardware and/or software in order to damage a computer or electronic communication system of a public or private subject or the information, data or programmes contained therein, or to favour the total or partial interruption or to alter its functioning;
- fraudulently intercept, prevent or interrupt communications of a computer or electronic communication system of a public or private subjects, in order to acquire confidential information;
- install appliances for the interception, prevention or interruption of communications of public or private subjects;
- modify and/or cancel data, information or programmes of a private or public subject or, in any case, of public usefulness;
- damage the information, data and computer programmes of others;
- destroy, damage or render unserviceable computer or electronic communication systems of public usefulness.

Therefore, the above-indicated subjects must:

- 1) use the information, applications and appliances exclusively in the performance of their work;
- 2) not lend or transfer to third parties any computer appliances;
- 3) Report to the competent departments theft, damage or loss of such instruments; in addition, in the case of the theft or loss of a computer appliance of any type, the person concerned or who has received delivery of such an instrument must report the fact to the police and transmit a copy of the report to the competent department within 24 hours;
- 4) avoid the introduction or conservation in the Company (on hardcopy, electronic support or by the use of the Company's instruments), under any circumstances and for any reason, IT documentation and/or material of a confidential nature and the property of third a party, unless acquired with their express consent.
- 5) Avoid the transfer outside the Company and/or the transmission of files, documents or any other documentation of a reserved nature and the property of the Company itself or of another company of the Group, unless for purposes strictly linked to the performance of their duties and, in any case, only after approval on the part of their immediate superior;
- 6) avoid leaving their own personal CP unattended and/or accessible to others;
- 7) avoid the use of the passwords of other company users, also for access to protected areas, in the name of and on account of the same, unless expressly authorised by the Information System manager;

- 8) avoid the use of software and/or hardware which can intercept, falsify, alter or suppress the content of the communications and/or electronic documents;
- 9) use the internet link for the purpose for which the connection was necessary, and only for the time strictly necessary;
- 10) Respect the procedures and standards foreseen, reporting without delay to the competent departments any anomalous use and/or functioning of the IT resources;
- 11) use only products officially bought by the Company itself, on the Company's hardware;
- 12) refrain from making unauthorised copies of data or software;
- 13) use the electronic instruments available only within the prescribed authorisations;
- 14) comply with every other specific provision regarding access to the systems and the protection of the Company's data and applications;
- 15) strictly comply with the policies for the safeguard of Company security and control of the computerised systems.

E.4. PRINCIPLES FOR THE IMPLEMENTATION OF THE RECOMMENDED CONDUCT

The system of control adopted by the Company foresees, for the at-risk areas identified, a series of control protocols, described below:

- 1) **Security policies** A policy on the security of the computerised system must be signed, which foresees, among other things:
 - the communication modalities, also with third parties;
 - the modalities for the review of the same, either at specific intervals or after significant changes.
- 2) **Organisation of security for internal users** A provision must be adopted and implemented which defines the roles and responsibilities in the management of the access modalities for internal Company users and the obligations of these latter in the use of the computer systems.
- 3) **Organisation of security for external users** A provision must be adopted and implemented which defines the roles and responsibilities in the management of the access modalities for users outside the Company and the obligations of these latter in the use of the computer systems, and also for the management of relations with third parties in the case of access, management, communications, supplies of products/services for data and information processing on the part of the said third parties.

- 4) **Asset classification and control** A provision must be adopted and implemented which defines the roles and responsibilities for the identification and classification of the Company's assets (including data and information).
- 5) **Physical and environmental security** A provision must be adopted and implemented which provides for the adoption of controls to prevent unauthorised access, damage and interference to the rooms where the electronic appliances are housed by protecting the areas and the appliances.
- 6) **Management of communications and operations** A provision must be adopted and implemented which ensures that the IT system operates in a correct and secure manner, by means of policies and procedures. In particular, the provision must ensure:
- correct and secure functioning of the electronic processors;
 - protection of hazardous software;
 - back-up of information and software;
 - protection of information exchange by the use of all types of instruments for communication also with third parties;
 - instruments for the traceability of the operations carried out with the applications, the system and the networks and protection of such information against unauthorised access;
 - organic management of the logs which record users' activities, exceptions and events concerning security;
 - control over changes to the computers and the systems;
 - management of removable devices.
- 7) **Access control** A provision must be adopted and implemented which disciplines access to the information, to information systems, the network, the operating systems and the applications. In particular, the provision must ensure:
- authentication of users by means of an identification code and a password or some other secure authentication system;
 - check lists of the personnel with authorised access to the systems, and of the specific authorisations of the diverse users or categories of users;
 - a procedure for the recording and the cancellation of the records, to grant and revoke access to all information systems and services;
 - review of users' access rights at pre-established intervals of time according to a formal process;

- revocation of access rights in the case of a change in the type of relationship which attributed the access right;
 - access to network services only to users who have been specifically authorised and restrictions on users' ability to link up to the network;
 - segmentation of the network to ensure that connections and information flows do not breach the provisions on access to company applications;
 - closure of inactive sessions after a pre-established period of time;
 - custody of the memorisation devices (e.g. USB keys, CD, external hard disks, etc.) and the adoption of clear screen rules for the computers used.
- 8) **Management of incidents and computer security problems:** A protocol must be adopted and implemented which defines adequate modalities for the management of incidents and of problems relative to computer security. In particular, the protocol must ensure:
- appropriate management channels for the communication of such incidents and problems;
 - periodic analysis of all single and recurrent incidents and detection of the root cause;
 - management of problems which have generated one or more incidents, in pursuit of a final solution;
 - analysis of reports and trends of incidents and problems and identification of preventive action;
 - appropriate management channels for the communication of every weakness or potential weakness in the systems or services observed;
 - analysis of the documentation available on the applications and identification of weaknesses which could generate future problems;
 - the use of informative databases to aid the resolution of incidents;
 - maintenance of the databases containing information on errors known and not yet resolved, the respective workarounds and the final solutions identified or implemented;
 - quantification and monitoring of types, volumes and costs of the incidents linked to IT security.
- 9) **Auditing** A provision must be adopted and implemented which disciplines roles, responsibilities and operating modalities of the periodic auditing of the efficiency and effectiveness of the IT security management system.
- 10) **Human resources and security** A provision must be adopted and implemented which foresees:
- assessment (before hiring or the stipulation of a contract) of the experience of persons destined to perform IT activities, especially as regards the security of the IT systems, and which takes into account

the rulings applicable in this field, the ethical principles and the principles for the classification of the information to which the above-said subjects will have access;

- specific training activities and periodic refresher courses on company IT security procedures, for all employees and, when relevant, also for third parties;
- the obligation to return goods provided for the performance of work activities (e.g. PC, mobile phones, authentication badges and cards, etc.) for employees and third parties on termination of their work agreement and/or contract;
- revocation, for all employees and third parties, of the rights of access to information, systems and applications on termination of their work relationship and/or contract in the case of a change in the duties performed.

11) **Cryptography** A provision must be adopted and implemented which foresees the use and the development of cryptographic controls for the protection of the information and on the management mechanisms for the encoded keys.

12) **Security in the purchase, development and maintenance of the computer systems.** A provision must be implemented which defines:

- the identification of the security requisites in the planning of or modifications to the existing computerised system;
- The management of the risks of error, loss and unauthorised modifications to the information processed by the applications;
- the confidentiality, authenticity and integrity of the information.

The table below sums up the aforesaid control protocols applicable to the single risk areas.

AT-RISK AREAS

CONTROL PROTOCOLS	1. Management of user's profile and of the authentication process	2. Management and protection of the work station	3. Management of access to enter and leave the workplace	4. Management and protection of the networks	5. Management of the outputs of the memorisation system and devices (e.g. USB, CD)	6. Physical safety (including wiring safety, network devices, etc.)	7. Production and/or sale of computer appliances, devices or programmes and of services for the installation and maintenance of hardware, software, networks.
Security policies	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
Organisation of security for internal users	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
Organisation of security for external users	Applicable	Not Applicable	Applicable	Applicable	Applicable	Applicable	Not Applicable
Asset classification and auditing	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
Physical and environmental security	Applicable	Not Applicable	Applicable	Applicable	Applicable	Applicable	Not Applicable
Management of communications and operations	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
Control of access	Applicable	Not Applicable	Applicable	Applicable	Not Applicable	Not Applicable	Not Applicable
Management of incidents and problems of computer security	Applicable	Applicable	Applicable	Applicable	Not Applicable	Applicable	Not Applicable
Auditing	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
Human resources and security	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
Cryptography	Applicable	Applicable	Applicable	Applicable	Applicable	Not Applicable	Not Applicable
Security in the purchase, development and maintenance of information systems	Applicable	Applicable	Applicable	Applicable	Not Applicable	Applicable	Applicable

Key:  Applicable  Not Applicable

E.5. THE DUTIES OF THE SURVEILLANCE BODY

The SURVEILLANCE BODY must monitor the effectiveness of the internal procedures for the prevention of computer crime and illicit data processing.

This task must be carried out also taking into account the following information flows:

- 1) every revision linked to changes in responsibilities or roles at present conferred regarding computer security, communicated by the Human Resources, Organisation and Information Technology department;
- 2) any reports from the control organs or from any employee.