ZTE ITALIA SERVIZI S.R.L.

Organisation, management and control model

Pursuant to Legislative Decree no. 231 dated 8 June 2001

Approved by the Board of Directors of 21st March 2018

CONTENTS

DEFINITIONS

Sensitive Activities	Corporate activities in the realm of which there is the risk of committing offences as set out in the decree or relevant for the management of financial resources
CCNL	National Collective Employment Contract
Code of Ethics	Group *Code of conduct* adopted by the company and additional documents thereto
Employees	Subjects who have a contract of subordinate or semi-subordinate employment with the company, and also workers administered and seconded to the company
Leg. Decree 231/2001 or Decree	Legislative Decree no. 231 dated 8 June 2001
Confindustria Guidelines	Confindustria document (approved on 7 March 2002 and updated to March 2014) for the preparation of Organisation, Management and Control Models as set out in Legislative Decree 231/2001
Model	Organisation, management and control model adopted by the company pursuant to Legislative Decree 231/2001
Supervisory Body or SB	Body provided for in article 6 of Legislative Decree 231/2001, entrusted with the task of

	supervising the function and observance of the Model and it being updated
PA	Public Administration, for which the following are jointly intended: - Public bodies created by a deed of State to meet State organisational and functional needs, such as municipalities and provinces, reclamation and irrigation consortia, chambers of commerce, ENAC, INPS, INAIL and IPSEMA; - Public Officials: subjects who carry out a public legal, judicial or administrative function and who can form or show the PA's wishes, via exercising their authoritative or certifying power, such as members of state and local administrations, supranational administrations (e.g. The European Union), the police, financial police, chambers of commerce, building commissions, judges, judicial officers, ancillary administrative bodies for justice (e.g. Bankruptcy receivers), directors and employees of public bodies, private subjects invested with powers that allow them to form or manifest the Public Administration's wishes; - subjects appointed for a public service: subjects who, for any reason, provide a public service, to be intended as an activity governed

	in the same ways as a public function, but has no typical powers of the latter, with the exclusion of carrying out simple tasks of public order or providing purely material work. Also a private subject or an employee of a private company can be appointed as a public service official when carrying out activities aimed at the pursuit of a public aim and the protection of a public interest.
Procedures	Procedures, *policies*, organisational provisions, service orders and other provisions and acts from a company that implement the principles of control contained in this document.
ZTE Servizi or Company	ZTE Italia Servizi S.r.l.
ZTE Italia	ZTE Italia S.r.l.

STRUCTURE OF THIS DOCUMENT

This document comprises a General Part and a Special Part

The General Part addresses the following subjects:

- The legislation contained in Legislative Decree 231/2001;
- The company's *governance* system;
- The preparation method for the Model;
- The subjects to whom the Model applies;
- The composition and function of the Supervisory Body;
- The sanction system overseeing violation of the model;
- The diffusion of the model and training of staff.

The Special Part contains rules regarding sensitive activities and states control methods, aimed or suitable for reducing the risk of committing the offences contained in the decree. These control methods are contained in and implemented in the Procedures.

They are an integral part of the Model:

- The document "*Control & risk self assessment* and *Gap analysis ex* Leg. Decree 231/2001", that formalises the results of *Control and Risk self assessment* activities aimed at identifying sensitive activities;
- The Code of Conduct, which defines the principles and rules of conduct for the company;
- The Procedures

These deeds and documents can be found according to the modes foreseen for their diffusion to the company staff.

GENERAL PART

1. The Legislative Decree no. 231 dated 8 June 2001

1.1. Responsibility for offences of bodies

The Legislative Decree no. 231 dated 8 June introduces and governs the administrative responsibility resulting from the offences of collective bodies. This form of responsibility combines aspects of the criminal punishment system and administrative sanctions. Based on the decree, in fact, the body is punished with an administrative fine, as it must answer for an administrative offence, but the sanction system is founded on the criminal process: the authority competent for contesting the offence is the Public Prosecution office and the criminal judge who issues the punishment. Responsibility of bodies for offences therefore has an administrative nature, but is basically a criminal responsibility

The responsibility is also separate and autonomous compared to that of an individual who commits the crime, as it still exists even if the perpetrator of the offence has not been identified, or when the offence has been quashed for a reason other than an amnesty. In all cases, the body's responsibility is added to, and does not substitute, the responsibility of the actual physical perpetrator of the offence.

The decree's field of application is extremely broad and concerns all bodies with legal entity status (including companies), associations also without legal entity status and public economic bodies. The legislation in question is not applicable to the State, local public bodies, non-economic public bodies and bodies that carry out constitutional functions (e.g. political parties and trade unions)

1.2. The categories of the so-called underlying offences

The body can be called upon to answer for the offences - so-called underlying offences - indicated as the source of responsibility in the decree or by a law that entered into force prior to the offence being committed.

On the date on which this document was approved, the underlying offences belong to the following categories:

- offences against the Public Administration (arts. 24 and 25);
- Cyber crimes and the illegal handling of data (art. 24-*bis*);
- Organised crime offences (art 24-*ter*);
- Forged currency, in public credit cards, in duty stamps and in instruments or marks of recognition (art. 25-*bis*);
- crime against industry and commerce (art. 25-*bis*.1);
- Corporate offences, including those of corruption between private persons (art. 25-*ter*);
- Crimes with the purpose of terrorism or subversion of the democratic order (art. 25-*quater*);
- Mutilation of female genital organs (art.25-*quater*.1);
- Crimes against individual personality (art. 25-*quinquies*);
- market abuse offences (art. 25-*sexies*);
- manslaughter or serious or extremely serious injury, committed by violating the laws on health and safety in the workplace (art. 25-*septies*);
- Handling, laundering and use of money, assets or profits of illegal origin, in addition to self-laundering (art. 25-*octies*);
- Crimes relating to the violation of copyright (art. 25-*novies*);
- Inducement not to make declarations or make untruthful declarations to the judicial authorities (art. 25-*decies*);
- Environmental crimes (art. 25-*undecies*);
- Employment of foreign citizens with no permits of stay (art. 25-*duodecies*);
- Racism and Xenophobia offences (Article 25-terdecies);

- Transnational crimes (art. 10, Law no. 146, 16 March 2006)[1].

[1] The amendments to the cases in point of crime provided for by the decree took place with the following legal documents: Decree Law no. 350 dated 25 September 2001, that introduced art. 25-*bis* «Counterfeiting in money, in public credit cards and duty stamps», later expanded and amended in «Counterfeiting in money, public credit cards and duty stamps, and in instruments or signs of recognition» from Law 99, 23 July 2009; Legislative Decree no. 61, 11 April 2002, that introduced art. 25-*ter* «Corporate Crimes»; Law no. 7 dated 14 January 2003, that introduced art. 25-*quater* «Crimes with the aim of terrorism or subversion of democratic order»; Law no. 228 11 August 2003 that introduced art. 25-*quinquies* «Crimes against the individual»; Law no. 62 18 April 2005 that introduced art. 25-*sexies* «Market abuse»; Law no. 7 dated 9 January 2006, that introduced art. 25-*quater*.1 «Mutilation of female genital organs»; Law no. 146 dated 16 March 2006, that provides for the responsibility of bodies for transnational crimes; Law no. 123 3 August 2007, that introduced art. 25-s*epties* «Manslaughter and serious or extremely serious culpable damage, committed with violation of accident prevention and health and safety in the workplace regulations», later amended in «Manslaughter and serious or extremely serious culpable damage, committed with violation of health and safety in the workplace regulations» by the Leg. Decree no. 81 dated 9 April 2008; Leg. Decree no. 231, dated 21 November 2007, that introduced art. 25-*octies* «Fencing, laundering and use of money, asset or profits of illegal origin, », later amended in «Fencing, laundering and use of money, asset or profits of illegal origin, and self-laundering» by Law no. 186 15 December 2014; Law no, 48 18 March 2008, that introduced art. 24-*bis* «Cyber crimes and illegal handling of data»; Law no. 94, 15 July 2009 that introduced art. 24-*ter* «Crimes of organised crime»; Law no. 99 23 July 2009, – already cited – that introduced art. 25-*bis*.1 «Crimes against industry and commerce» and art. 25-*novies* «Crimes regarding the violation of copyright»; Law no. 116 3 August 2009 that introduced art. 25-*novies* (later renumbered art. 25-*decies* by Leg. Decree no. 121 7 July 2011) «Inducement to not make declarations or to make untruthful declarations to the judicial authorities»; Leg Decree 121/2011 – already cited – that introduced art. 25-*undecies* «Environmental Crimes»; Leg. Decree No. 109, 16 July 2012 that introduced art. 25-*duodecies* «Employment of citizens of other countries with no valid resident's permit»; Law no. 190 6 November 2012 that amended arts. 25 and 25-*ter*; Law no 68 22 May 2015, that amended art. 25-*undecies*; Law no. 69 30 May 2015 that amended art. 25-*ter*; Law no. 199 29 October 2016 that amended art. 25-*quinquies*; Leg. Decree 15 March 2017, no. 38, which amended art. 25-*ter*; Law no. 161 of 17 October 2017, which integrated art. 25-duodecies with the insertion of the reference to paragraphs 3, 3-bis, 3-ter and 5 of art. 12 of Legislative Decree no. 286/1998, concerning the conduct of those who "*direct, organize, finance, transport foreigners to the territory of the State or carry out other acts aimed at illegally obtaining their entry into the territory of the State*" or promote their permanence "*in order to obtain an unfair profit from the condition of illegality*"; Law no. 167 of November 20, 2017, which included in the Decree art. 25-terdecies entitled "racism and xenophobia".

The body can also be called upon to answer before an Italian judge for underlying crimes committed overseas in the following conditions:

- The general conditions for proceeding as foreseen by articles 7, 8, 9 and 10 Criminal Code exist to be able to pursue a crime committed overseas in Italy;
- The body has its main site in Italy;
- The state of the place where the crime is committed does not proceed against the body.

1.3. The criteria for charging responsibility to the body; exempting from responsibility

In addition to committing one of the underlying crimes, so that the body can be punished pursuant to Leg. Decree 231/2001 other legislative requisites must be integrated. Such other criteria for the bodies' responsibility must be separated into "objective" and "subjective".

The first objective criterion is integrated by the fact that the offence was committed by a subject connected to the body by a qualified relationship. On this matter, distinction is made between:

- "Subjects in managerial position": i.e., with positions of representation, administration or management of the body, such as directors, general managers, or directors of an autonomous organisational unit and generally those people who manage the body, also by deed, or one of its autonomous organisational units;
- "Subordinates": i.e., all those who are subject to the management and supervision of the subjects in a managerial position. Employees and those subjects belong to this category that, although not a member of staff, have a task to carry out under the management and control of the managers.

Identifying the subjects above does not take into account the contractual level of the relationship they have with the body; in fact, subjects not belonging to the body's staff must also be included whenever they act in the name of, on behalf of or in the interest of the body.

.

Another objective criterion is the fact that the crime must be committed in the interest of or to the advantage of the body; the existence of at least one of the two conditions is sufficient (in this sense, see Criminal Court of Cassation, no. 3615, 20 December 2005):

- The interest exists when the perpetrator of the crime has acted with the intention of favouring the body, regardless of the circumstance whether this objective was actually achieved;
- The advantage exists when the body has gained - or could have gained - positive, economic or other type of result.

With regard to subjective criteria of charging the responsibility to the body, these refer to preventive tools that the body has to prevent the committing of one of the underlying crimes while carrying out company business.

In fact, on the matter of committing a crime by a subject in a managerial position, the decree foresees exemption from responsibility for the body if it can prove that:

- The managers adopted and efficiently implemented organisation, management and control models suitable for preventing crimes of the nature that occurred, prior to the fact being committed;
- The task of supervising the function and observance of models and taking care to update them was entrusted to a body with autonomous powers of initiative and control;
- The managerial subject has committed the crime, fraudulently evading the models;
- Supervision by the afore-stated body was not omitted or insufficient.

In the hypothesis of crimes committed by subordinates, the body can be called upon to answer for them only if committing the crime was possible due to the breach of management or supervision obligations, excluded however if, before the crime was committed, the body set up organisation, management and control models that could prevent crimes of the kind that was committed.

1.4. Indication in the Decree regarding characteristics of the organisation, management and control model

The Decree limits itself to governing some general principles regarding the organisation, management and control model, providing for the following minimum content:

- Identification of body's activities within the realm of which crimes can be committed;
- provision of specific protocols aimed at planning training and implementation of body's decisions, in relation to the crimes to be prevented;
- identification of financial resource management modes that are suitable for preventing the committing of crimes;
- Adoption of a disciplinary system suitable for punishing the non-observance of the measures contained in the model;
- Identification of information flows to the Supervisory Body;
- Provision, for the nature and extent of the organisation and the type of activity carried out, of measures suitable for ensuring carrying out of business in observance of the law and to discover and remove risk situations immediately.

Pursuant to the Law no. 179/2017 ("*Provisions for the protection of whistleblowers who report offences or irregularities which have come to their attention in the context of a public or private employment relationship*"), in order to be compliant with the whistleblowing regulations, a model shall now provide for:

- more than one channels that, while ensuring the confidentiality of the identity of the whistleblower, allow the employees to submit detailed reports of illegal conduct or violations of the 231 Model (one of these channels has to be implemented via informatics tool);
- the prohibition of discriminatory action against the whistleblower (*i.e.* anti-retaliation measures);

- adequate sanctions for those who violate the above-mentioned anti-retaliation measures and for those who – intentionally or negligently – file reports that prove to be unfounded.

The Decree states that the model must undergo periodic checks and updates, both if significant violations of prescriptions emerge and if there are significant changes to the organisation or activities of the body.

1.5. The sanctions

The sanction system provided for in Leg. Decree 231/2001 is divided into four types of sanctions that the body can be subjected to in the event it is convicted pursuant to the decree:

- Pecuniary sanction: is always applied if the judge considers the body responsible and is calculated using a system based on quotas, that are decided by the judge in number and amount; the number of quotas, to be applied between a minimum and maximum that vary depending on the case, depends on the seriousness of the crime, the degree of the body's responsibility, the activity carried out to eliminate or reduce the consequences of the crime or to prevent the committing of other crimes; the total of the single quota is set between a minimum of 258 Euro and a maximum of 1549 Euro, depending on the economic and asset conditions of the body;
- Bans: bans are applied, in addition to pecuniary sanctions, only if expressly provided for the crime that the body is convicted of, and only if at least one of the following conditions exists:
    - The body has obtained considerable profit from the crime, and the crime was committed by a managerial subject, or by a subordinate if committing the crime was made possible by serious shortcomings in organisation;
    - In the event of reiteration of the offences.

  Bans as foreseen in the decree are:
    - Ban from conducting the business;

- Suspension, or revoking of authorisations, permits or licences required to commit the offence
- Ban on contracts with the PA, unless to obtain a public services;
- Exclusion from subsidies, funding, contributions or grants and revocation of any already granted;
- Ban on publicizing goods or services.

Exceptionally applicable with permanent effect, bans are temporary, with a duration of between three months and two years, and regard the specific business of the body that the crime refers to. They can also be applied, on the public prosecutor's request, if serious, evidence of the body's responsibility and specific elements exist that the danger of further committing of offences of the same time as being investigated are considered to be tangible.

- Seizure: on conviction, seizure of the price or profit of the crime or equivalent assets or valuables is always ordered;
- Publication of the conviction: when the body is convicted to a ban, this may also be ordered. It consists of a publication of the sentence, at the body's expense, as an extract or in its entirety, in one or more of the newspapers stated by the judge in the sentence, and by posting in the town hall where the body has its main site.

Administrative sanctions for the body are limited to five years from the date of committing the crime at the base of the administrative offence.

The final conviction of the body is recorded in the national register of administrative offence sanctions.

The Decree also governs the status of the body's responsibility if transformed, merged, spun-off or sold.

In the body is transformed, the responsibility for the crimes committed prior to the date on which transformation takes effect remains. The new body will therefore be the recipient of the sanctions applicable to the original body, for deeds committed before the transformation.

In the event of merger, the body resulting from the merger, also by incorporation, will answer for the crimes that the bodies taking part in the merger are responsible for.

In the event of a spin-off, the responsibility of the spun-off body for the crimes committed prior to the date on which the spin-off takes effect and the beneficiary bodies of the spin-off are jointly obliged to pay any pecuniary sanctions imposed on the spun-off body, in the limit of the net equity transferred to each body, unless it is a body to which the branch of activity involved in the crime is also transferred; bans apply to the body (or bodies) that the branch of business in which the crime was committed has stayed in or joined.

In the event of transfer or awarding of the company in the realm of which the offence has been committed, without prejudice to the right to enforce prior payment by the transferring body, the transferee is jointly responsible with the transferring body for payment of the fine, within the limits of the value of the transferred company and within the limits of the monetary sanctions that are recorded in the mandatory accounting books or due for offences that the transferee was aware of.

2. ZTE Servizi: the company and its *corporate governance* and internal control system

2.1. The Company and the Group

ZTE Servizi is part of a group headed by ZTE Corporation, a global provider of products and services for telecommunications, with more than one hundred branches worldwide.

The company, entirely owned by ZTE Italia, works in the implementation, management and maintenance of transmission plants and networks for telecommunications providers, and the management of research activities required for carrying out the services indicated.

2.2. The *corporate governance system*

The company's *corporate governance* system currently hinges on the Board of Directors, that have the broadest powers for achieving company purpose and for the routine and extraordinary management of the company, except for those deeds that by law and by-laws are the exclusive responsibility of the General Assembly meeting.

The Model and the Procedure are a part of the *corporate governance* system, aimed at making the control system as efficient as possible and preventing the crimes foreseen in the Decree.

The Code of Conduct adopted by the company is essential to the Model, which formalises the ethical principles and values that the company aspires to in carrying out its business.

The Code recognises the legal relevance and mandatory efficacy of the ethical principles and behavioural standards described in it, also with a view to preventing corporate crimes and places observance of current legislation at its very basis.

2.3. The internal control system

The ZTE Servizi internal control system in particular in reference to sensitive activities and consistently with the provisions of the Confindustria Guidelines is based on the following principles:

- clear identification of roles, tasks, and responsibilities of subjects who take part in the realisation of corporate activities (inside or outside the organisation);
- Separation of tasks between those who operatively carry out an operation and those who control it, those who authorise it and those who register it (where applicable);
- Ability to check and document operations ex post: the relevant activities carried out (especially sensitive activities) are suitably formalised, with particular reference to the documents drawn up while being carried out. The documents produced are available on paper or in digital format and are filed by the departments/subjects involved;
- Identification of preventive controls and manual and automatic ex post checks: manual and/or automatic devices are provided for preventing the committing of crimes or to discover

ex post any irregularities that may be in contrast to the model's purpose. These controls are more frequent, detailed and sophisticated in the realm of those sensitive activities characterised by a higher profile of risk of committing crimes.

The following are elements of the internal control system:

- system of ethical principles aimed at preventing the crimes contained in the decree;
- Sufficiently formalised and clear organisational system;
- Authorisation and signatory powers system consistent with organisational and management responsibilities as defined;
- Management control system that can provide rapid reporting of the existence and onset of critical situations;
- Staff communication and training system on parts of the model;
- Disciplinary system suitable for punishing the violation of regulations in the model;
- Operational, manual and digital procedures system, aimed at regulating activities in company areas at risk with suitable control devices;
- Information system for carrying out operational and control activities in the realm of sensitive activities, or to support them.

In reference to the system of ethical principles, the communication and training system and the disciplinary system, please refer to the Code of Conduct and the contents of sections 6 and 7 of this General Part.

The company's organisational system is defined by a company organisational chart and the issue of appointments of departments and organisational orders (service, job descriptions, and internal organisational directives) that provide a clear definition of the departments and responsibilities attributed to each local organisation unit.

The authorisation and decision-making system translates to a detailed system consistent with the distribution of functions and proxies in the company, based on the following principles:

- the proxies match each managerial power with the relative responsibility and a suitable position in the organisational chart, and are updated after any organisational changes;
- Each proxy defines and describes specifically and without misunderstanding the management powers of the person delegated and the subject that the delegated person reports to hierarchically;
- the management powers allocated proxies and their implementation are consistent with company goals;
- The proxy must have spending power in line with the duties appointed;
- Powers of attorney are only conferred to subjects with internal functional delegated power or specific appointment and foreseen the extension of powers of representation and, also spending limits.

The management control system adopted by ZTE Servizi is divided into the various phases of the annual budget preparation, analysis of actual spending and drawing up of forecasts.

The system guarantees that:

- The number of subjects involved, in terms of consistent separation of the functions for drawing up and transmitting information;
- Ability to promptly provide reports on the existence or onset of critical situations via a suitable, rapid information flow and reporting system.

Art. 6, par 2, letter *c)* of the decree states that the model must "*identify management modes for financial resources suitable for preventing the committing of crimes*".

For this purpose, the management of financial resources is defined on the basis of principles based on a reasonable segregation of functions, such as to guarantee that all expenses are requested, made and controlled by independent departments or subjects as far as possible separate, and who do not have other responsibilities that may cause potential conflict of interest.

Art. 6, par. 2, letter b) of the Decree expressly states that the model must "*provide for specific protocols aimed at planning the formation and implementation of the body's decisions in relation to the crimes to be prevented*".

For this purpose, the company has drawn up procedures that provide for governing sensitive activities and therefore guiding and guaranteeing the implementation of control devices foreseen in the model. In particular, the procedures guarantee application of the following principles:

- Clear formalisation of roles, responsibilities, modes and time for realising governed operational and control activities
- Representation and governance of the separation of tasks between the subject taking the decision (decision-making impulse), the subject who authorises its realisation, the subject carrying out the activities and the subject who controls it;
- Traceability and formalisation of each important activity in the process involved in the procedure, in order to retrace activities at a later date and evidence of the principles and control activities applied;
- Suitable filing level for important documents.

To protect company documents and information, suitable security measures for the risk of loss and/or alteration of documents referring to sensitive activities or undesired access to data/documents have been provided for.

To preserve the integrity of data and efficacy of information systems and/or computer applications used to carry out operations or controls in the realm of sensitive activities, or to support them, the presence and operations of the following are guaranteed:

- User profiling system in relation to access to modules or environments;
- Rules for the correct use of systems and company computer equipment (hardware and software);
- Automatic control mechanisms for system access;

- Automatic blocking mechanisms or prevention of access;
- Automatic mechanisms for managing authorising work flows.

3. Method used for drawing up the Model; amendments and updates to the Model

To draw up this document, consistently with the provisions in the decree, with the Confindustria guidelines and the indications given by jurisprudence, the company has proceeded to carry out preventive activity known as *Control and Risk self assessment*.

Control and Risk self assessment were carried out and coordinated by a Project Team comprising external consultants and saw the direct involvement of the company management.

In particular, these activities were divided into the following phases:

- Acquisition and analysis of important documentation for company/group governance and internal control system (e.g. Organisational charts, codes of conduct, structure of proxies and powers of attorney, internal procedures and reports);
- Preliminary identification of sensitive activities in the various organisational structures involved, with particular reference to the ones most involved by the Leg. Decree 231/2001, also considering the identification of potential new risks-crimes;
- Identification of *key officers* to involve in the interviews;
- carrying out of interviews aimed at:
    - identification/confirmation of sensitive activities, operational modes used to carry them out and subjects involved;
    - Identification of potential risks of committing underlying crimes that can be traced to each sensitive activity;
    - Analysis and evaluation of control devices/systems that reduce the risks above and identification of possible areas for improvement;

- Sharing of information that emerges with *Management* and formalisation of information in a summary *report* ("*Control & risk self assessment* and *Gap analysis ex* Leg. Decree 231/2001") that is an integral part of this document.

This activity will identify suitable devices to use in the control system in order to make it suitable for reducing the risk of committing crimes, as well as the actual implementation of devices as above in the control system by individual key officers involved each time.

The company has adopted this version of its organisation, management and control model by resolution of the Board of Directors of ()

The model must always be amended or added to promptly, by resolution of the Board of Directors, in the event that:

- Significant changes occur in the legislation of reference (e.g. introduction of new underlying crimes in the decree), and in the company organisation or activities;
- Violations or evasion of instructions contained therein have been found, that have proven the inefficacy for the purpose of preventing crimes.

Amendments to the procedures are made by the managers of the departments involved.

4. Recipients of the Model and governance of relations with third parties

The Model applies:

- To Company Directors;
- To company Employees;
- To those who operate on mandate and/or on behalf of the company (e.g. under contract, as consultants, or specific proxy, as defence in court); these subjects are bound to observe the model via specific clauses in their contracts.

Also, each contract stipulated by the company with providers of goods or services must also foresee the commitment or a guarantee if the provider is a legal entity that its own directors and employees will undertake to:

- Observe applicable law and not commit crimes;
- Respect the principles of the Code of Conduct and of the Model (which will be introduced to the provider in the ways considered appropriate by the company, e.g. By publication on its own website or through specific communication);
- To fulfil any requests for information by the company's Supervisory Body,

as well as to grant the Company the right to proceed with applying forms of protection (e.g. termination of contract, application of penalties, etc.), wherever a violation of said commitments and guarantees is noted.

5. The Supervisory Body

5.1. Function

In observance of the decree, the company entrusts its Supervisory body with the task of constantly supervising:

- The observance of the model by the subjects it is applied to, as identified above, and the implementation of the instructions from the model for the carrying out of company activities;
- Efficacy of the model in preventing the committing of crimes as per the decree;
- The update of the model.

5.2. Requisites and composition of the Supervisory Body;

Jurisprudence and *best practice* regarding the Leg. Decree 231/2001 have identified the following SB requisites are indispensable:

- Autonomy and independence: the concepts of autonomy and independence have no valid definition in an absolute sense, but must be declined and placed in an operational sense that they will be applied in. Since the Supervisory Body is tasked with verifying compliance, in the company's operations, with the controls applied; the position of the Supervisory Body within the body must ensure its independence from any form of interference and conditioning by any member of the body and, in particular, by top management, especially considering that the function exercised is also expressed in the oversight of the activities of persons in top management positions. Therefore, the Supervisory Body reports only to the Board of Directors when carrying out its functions.

  Furthermore, in order to better guarantee the independence of the Supervisory Body, the Board of Directors provides it with resources, in number and skills proportionate to the assigned tasks, and approves, as part of the company budget process, an adequate allocation of financial resources, proposed by the SB, which the latter may have at its disposal for any need for the proper performance of its tasks (e.g., specialist advice, travel, etc.).

  The autonomy and independence of the individual members of the Supervisory Body must be determined on the basis of the function performed and the tasks assigned to them, identifying from whom and what it must be autonomous and independent in order to carry out these tasks. Consequently, each member must not hold decision-making, operational and management roles that may compromise the autonomy and independence of the entire SB. In any case, the requirements of autonomy and independence presuppose that members are not in a position, even potential, of personal conflict of interest with the Company.

  Also, the members of the Supervisory Body must not:

  - hold operational positions in the Company;
  - be a spouse, relative or similar within the fourth degree of directors of the Company;
  - be in any other situation of actual or potential conflict of interest;

- Professional competence: the Supervisory Body must have technical and professional skills appropriate to the functions it is called upon to perform. Therefore, it is necessary that the Supervisory Body should include persons with adequate professional skills in economic, legal and analysis, risk control and management matters. In particular, the Supervisory Body must have the specialist technical skills necessary to carry out control and consultancy activities.

  In order to ensure the professional skills that are useful or necessary for the activity of the Supervisory Body and to guarantee the professionalism of the Body (as well as, as already mentioned, its autonomy), the Supervisory Body is given a specific spending budget aimed at acquiring additional competences to its own, when necessary, outside the body. The Supervisory Body can thus, including with the help of external professionals, provide itself with competent resources expert, for example, in legal matters, company organisation, accounting, internal controls, finance and safety in the workplace, etc..;

- Continuity of action: the Supervisory Body continuously carries out its activities.

  Continuity of action should not be understood as "incessant operation," since such an interpretation would necessarily impose a Supervisory Body exclusively within the entity, when this circumstance would instead lead to a decrease in the indispensable autonomy that must characterise the SB. Continuity of action means that the SB's activity must not be limited to regular meetings of its members, but must be organised on the basis of an activity plan and the constant conduct of monitoring and analysis of the entity's system of preventive controls.

In compliance with the above-mentioned principles, and taking into account the structure and operations of ZTE Italia, the Supervisory Body of the Company is composed, in collegial form, of two members, not members of the Company's personnel.

5.3. Requisites of eligibility of members of the Supervisory Body

The role of member of the Supervisory Body cannot be entrusted to a person who is:

- suspected or convicted, including with a sentence not yet final or suspended, except for the effects of rehabilitation:
    - For one or more crimes of the ones foreseen by Leg. Decree 231/2001;
    - For any offence committed with criminal intent;
- prohibited, disqualified, foreclosed or convicted, including with a sentence that is not yet final, to a penalty that results in disqualification, even temporary, from public offices or inability to hold a management position;
- submitted or has been subjected to preventive measures pursuant to Legislative Decree no. 159 of 6 September 2011 ("Code of anti-Mafia laws and preventive measures, as well as new provisions on anti-Mafia documentation, pursuant to articles 1 and 2 of Law no. 136 of 13 August 2010");
- Subjected to additional administrative sanctions as set out in art. 187-*quater* of the Legislative Decree no. 58 dated 24 February 1998

5.4. Appointment, revocation, replacement, forfeiture and withdrawal

The Board of Directors appoints the Supervisory Body, justifying the decision concerning the choice of each member, after having verified that the requirements set forth in the preceding paragraphs are met, basing this decision on the curricula as well as on the official and specific statements directly collected from the candidates. In addition, the Board of Directors shall receive a declaration attesting to the absence of the reasons for ineligibility referred to in the previous paragraph from each candidate.

After formal acceptance of the nominees, the appointment is communicated at all company levels, through internal communication.

The Supervisory Body has its own Rules of Procedure, approving their contents and submitting them to the Board of Directors.

The SB remains appointed for three years. Members of the SB can be re-elected on expiration of their mandate.

Withdrawal from office as a member of the SB can only take place through a resolution of the Board of Directors for one of the following reasons:

- loss of requisites as stated above;
- breach of obligations regarding the entrusted role;
- Lack of good faith and diligence in carrying out role;
- non-collaboration with other members of the SB;
- Unjustified absence at two SB meetings;
- breaches of confidentiality obligations or retaliatory or discriminatory acts against those who have reported illegal conduct or a violation of the Model, for reasons directly or indirectly related to the report (including the violation of the anti-retaliatory provisions provided for the whistleblowing legislation);
- performing with malicious intent or gross negligence of reports that prove to be unfounded.

Each member of the SB is under an obligation to inform the Board of Directors, through the Chairman of the SB, of the loss of the requirements referred to in the paragraphs above.

The Board of Directors revokes the appointment of the member of the SB who is no longer eligible and, after adequate motivation, immediately replaces him/her.

Before the expiry of the term of office, any incapacity or impossibility to carry out the task shall constitute a cause of forfeiture of the appointment.

Each member of the SB can withdraw from the assignment at any time, according to the procedures that will be established in the regulations of the Body.

In the event of forfeiture or withdrawal by one of the members of the SB, the Board of Directors shall promptly replace the member that has become ineligible.

5.5. Activities and powers

The Supervisory Body meets at least four times a year and whenever one of the members has asked the Chairman to convene it, justifying the opportunity of calling a meeting. It may also delegate specific functions to the Chairman. Each meeting of the SB is recorded in minutes.

In order to carry out the assigned tasks, the Supervisory Body is vested with all the powers of initiative and control over all company activities and personnel levels and reports solely to the Board of Directors through its Chairman.

The duties and powers of the Supervisory Body and its members cannot be syndicated by any other corporate body or structure, it being understood that the Board of Directors can verify the consistency between the activity actually carried out by the Body and the mandate assigned to it. In addition, the SB, except for prevailing provisions of law, has free access - without the need for any prior consent - to all Company Functions and Bodies, in order to obtain any information or data deemed necessary for the performance of its duties.

The Supervisory Body carries out its functions in coordination with the other control bodies or Functions existing in the Company. In addition, the SB liaises with the company functions involved from time to time in all aspects related to the implementation of the Procedures. The SB may also avail itself of the assistance and support of employees and external consultants, in particular for problems that require the help of specialist skills.

The Supervisory Body organises its activities on the basis of an annual action plan, through which the initiatives to be undertaken are planned in order to assess the effectiveness of the Model as well as its updating. This plan is submitted to the Board of Directors.

The Supervisory Body determines its annual budget and submits it to the Board of Directors for approval.

The Supervisory Body, in overseeing the effective implementation of the Model, is endowed with powers and duties that it exercises in compliance with the law and the individual rights of workers and parties concerned, as set out below:

- carry out, also through other persons (e.g., their own consultants), inspection activities;
- have access to all documentation or information relating to the Company's activities, which may be requested from all the Company's personnel, as well as from the Directors and suppliers of goods and services of the Company;
- report serious and urgent events to the Board of Directors, as well as any events that make it necessary to amend or update the Model;
- propose the adoption of penalties related to the violation of the Model, as per paragraph 6, to the person with disciplinary power;
- coordinate with the HR function to define training programmes relating to Legislative Decree no. 231/2001 and the Model referred to in paragraph 7;
- prepare, every six months, a written report to the Board of Directors, with the following minimum content:
    - a summary of the activities, checks carried out by the SB during the period and their results;
    - any discrepancies between the Procedures and the Model;
    - reports received on possible violations of the Model and results of checks concerning the above reports, as well as on facts that may constitute offences;
    - disciplinary procedures initiated upon proposal of the SB and any penalties applied;
    - general evaluation of the Model and its effective functioning, with possible proposals for additions and improvements;
    - any changes to the regulatory framework;
    - summary of any expenses incurred;

The Board of Directors, the Chairman and the Chief Executive Officer have the right to call a meeting of the Supervisory Board at any time. Similarly, the SB has the right, in turn, to request,

through the Functions or competent persons, the call of the aforesaid corporate bodies for urgent reasons. Meetings with the bodies to which the SB reports must be recorded in minutes and a copy of the minutes must be kept by the SB and the bodies involved from time to time.

5.6. Information flows to the SB and whistleblowing schemes

The SB must promptly obtain, by way of non-exhaustive example, the following information:

- any illicit conduct (or any conduct that appears to be illicit to the whistleblower) which is relevant pursuant to Legislative Decree no. 231/2001, that the whistleblower has become aware of in the performing of their duties, or any violation (or any conduct that appears to be a violation) of the provisions of the Model, or any conduct that is not compliant with the behavioral rules adopted by the Company;
- critical, abnormal or atypical issues found by the Company's Functions in the implementation of the Model;
- measures and/or information from judicial police bodies, or from any other authority, from which it is apparent that investigations are being carried out, even against unknown persons, for crimes referred to in the Decree committed within the scope of the Company's activity;
- internal and external communications regarding any type of offence that may be connected with the offences referred to in the Decree (e.g., disciplinary measures initiated/implemented against employees);
- requests for legal assistance made by employees in the event of judicial proceedings for offences referred to in the Decree;
- news relating to changes in the organisational structure;
- updates to the organisational system and the system of proxies and powers of attorney (including those relating to the system of powers regarding health and safety at work and environmental safety);
- Copy of Board of Directors' meeting minutes.

Such information must be provided to the SB by the Managers of the Company Functions according to their area of competence.As also provided for by Law no. 179 of 30 November 2017, which introduced whistleblowing into the regulations contained in Legislative Decree no. 231/2001, the Company adopts all the measures necessary to ensure that acts of retaliation or discrimination, direct or indirect, against the whistleblower are prohibited for reasons directly or indirectly linked to the report. In particular, the adoption of discriminatory measures against the whistleblower may be reported to the National Labour Inspectorate, for the measures within its competence, as well as by the whistleblower, also by the trade union organization indicated by the same. Furthermore, any retaliatory or discriminatory dismissal of the whistleblower shall be considered null and void. The change of duties pursuant to article 2103 of the Civil Code is also null and void, as well as any other retaliatory or discriminatory measure adopted against the whistleblower. It is the responsibility of the employer, in the event of disputes linked to the imposition of disciplinary sanctions, or to de-scanning, dismissal, transfer, or submission of the whistleblower to another organizational measure having direct or indirect negative effects on working conditions, subsequent to the submission of the report, to demonstrate that these measures are based on reasons unrelated to the report itself. Finally, it should be noted that, in the event of reports or reports made in the manner and within the limits of the law, the pursuit of the interest in the integrity of the entity, as well as the prevention and repression of misappropriation, constitutes just cause for disclosure of information covered by the obligation of secrecy referred to in Articles 326, 622 and 623 Criminal Code and article 2105 of the Civil Code (except where the obligation of professional secrecy applies to a person who has become aware of the news as a result of a professional consultancy or assistance relationship with the body, firm or natural person concerned). When news and documents that are communicated to the body delegated to receive them are subject to corporate, professional or official secrecy, disclosure in a manner that exceeds the purposes for which the offence was eliminated and, in particular, disclosure outside the communication channel specifically set up for that purpose, constitutes a breach of the relative obligation of secrecy.

All recipients of the Model must communicate directly with the Supervisory Body, to report any violations of the Model, through confidential internal mail or through a dedicated e-mail.

In compliance with whistleblowing regulation, the Company has also set up two additional information channels to guarantee the confidentiality of the identity of the whistleblower. The report may then be sent by electronic mail or by traditional mail to the Chairman of the Supervisory Board, to the addresses indicated on the Company's website.

Reports may also be anonymous and must describe in detail the facts and persons reported.

Behaviour aimed exclusively at slowing down the activity of the SB is sanctioned.

In any case, the Company protects whistle-blowers in good faith against any form of retaliation, discrimination or penalisation for reasons connected, directly or indirectly, with the reporting, without prejudice to the right of the assignees to protect themselves if they are found to be responsible for criminal or civil liability related to false statements and without prejudice to legal obligations. In any case, the confidentiality of the identity of the whistle-blower and of the information in any context subsequent to the report itself is guaranteed, without prejudice to legal obligations and the protection of the rights of the Company or of persons accused erroneously or in bad faith. The report is considered to have been made in good faith when it is made on the basis of a reasonable conviction based on facts.

In addition to the reports described above, information must be submitted to the Supervisory Body regarding news concerning disciplinary proceedings and penalties or the measures taken to close such proceedings with their reasons.

The Supervisory Body may submit proposals to the Board of Directors concerning additional types of information that the managers involved in the management of at-risk activities must transmit together with the frequency and methods by which such communications are sent to the Supervisory Board, also through the definition of a specific operating procedure and/or the integration of existing procedures.

Reports received and documentation managed by the SB in general are kept by the SB in a special archive, whether paper or computer, for the entire duration of the Company. The members of the

Board of Directors and persons authorised from time to time by the SB, are allowed access to this archive.

6. Disciplinary System

6.1. General principles

The Decree provides for the introduction of a "disciplinary system to punish non-compliance with the measures set out in the model," both for persons in a top management position and for persons subject to management and supervision by others.

The existence of a system of penalties applicable in the event of non-compliance with the rules of conduct, provisions and internal procedures set out by the Model is in fact indispensable to guarantee the effectiveness of the Model itself.

By virtue of the provisions of the aforementioned Law no. 179/2017 on whistleblowing and with reference to any recipient of the Model, it should be noted that conduct that may be sanctioned must also include the violation, in any way, of the measures to protect the whistleblower, as well as the performing with malicious intent or gross negligence of reports that prove to be unfounded.

The application of sanctions must remain completely independent from the course and outcome of any criminal or administrative proceedings initiated by judicial or administrative authorities in the case in which the behaviour to be punished also applies to integrate an offence pursuant to Decree or a criminal or administrative offence that is relevant pursuant to legislation on the protection of health and safety in the workplace. In fact, the rules set out by the Model are adopted by the Company in full autonomy, regardless of whether any types of conduct may constitute a criminal or administrative offence and whether judicial or administrative authorities intends to prosecute this offence.

The Supervisory Body is responsible for verifying the adequacy of the disciplinary system, constantly monitoring any procedures for imposing penalties on employees, as well as for

intervening against external parties and also reports any infringements of which it becomes aware in the exercise of its own functions.

6.2. Violations of Model

Violations of the Model include:

- behaviours that constitute the types of offence contemplated in the Decree;
- conduct that, though not constituting one of the offences referred to in the Decree, is clearly aimed at committing them;
- conduct that does not comply with the Procedures referred to in the Model and the Code of Conduct;
- conduct that does not comply with the provisions of the Model or referred to in the Model and, in particular, does not comply with the control measures listed in paragraphs 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 and 22 of the Special Section and with the Procedures referred to in the Model itself;
- uncooperative behaviours toward the Supervisory Board, consisting in, by way of example and but not limited to, the refusal to provide the required information or documentation, failure to comply with general and specific directives of the Supervisory Board in order to obtain the information it deems necessary for the performance of its duties and absence without justified reason during inspection visits scheduled by the Supervisory Board and failure to attend training meetings;
- breaches of confidentiality obligations or retaliatory or discriminatory acts against those who have reported illegal conduct or a violation of the Model, for reasons directly or indirectly related to the report (including the violation of the anti-retaliatory provisions provided for the whistleblowing legislation);
- performing with malicious intent or gross negligence of reports that prove to be unfounded.

The seriousness of violations of the Model will be assessed on the basis of the following circumstances:

- presence and degree of intent;
- presence and degree of negligent, reckless behaviour;
- the extent of the danger and/or consequences of the violation for the persons covered by the regulations on the protection of health and safety at work, as well as for the Company;
- predictability of the consequences;
- timing and way in which the violation occurs;
- circumstances in which the violation occurs;
- repeat occurrence consisting in repeated imposition of disciplinary sanctions for violations of the Model, as well as in the repetition of behaviours that are relevant from a disciplinary point of view, assessed both in terms of the single event and overall (though not punished).

6.3. Measures against employees

The violation of the individual rules of conduct of this Model, including the violation, in any way, of the measures to protect the whistleblower, or the malicious or grossly negligent making of reports that prove to be unfounded by employees subject to the national collective labour agreement applied by the Company constitutes a disciplinary offence.

Any violation authorises the SB to require the competent company Function to initiate disciplinary proceedings and the possible imposition of one of the penalties listed below, determined on the basis of the seriousness of the violation committed in the light of the criteria indicated in paragraph 6.2 and of the behaviour carried out before (e.g., any previous violations committed) and after the fact (e. g. notification to the SB of the irregularity) by the perpetrator of the violation.

Disciplinary measures that can be imposed against said employees - in compliance with the procedures laid down in article 7, paragraphs 2 and 3, of Law no. 300 of 30 May 1970 (Workers'

Statute) and any special regulations applicable, as well as applicable national collective labour agreement(s) - are those provided for by the following penalties:

- Verbal warning;
- Written warning;
- Fine of maximum three hours of remuneration;
- Suspension from service and from remuneration for a period of maximum 3 days;
- Disciplinary dismissal with right to notice pursuant to the stated CCNL and dismissal for good reason without notice.

In any case, the penalties applied and/or violations ascertained will always be notified by the competent company function to the Supervisory Board.

In particular, with reference to violations of the Model by employees, it is provided that:

- verbal or written reprimand measures according to the seriousness of the violation shall be taken against an employee who violates the Procedures set forth in the Model or who adopts, when carrying out activities in at-risk activities, conduct in violation of the Model's provisions, unless such conduct results in the application of measures set forth in the Decree;
- a fine is incurred by employees who relapse in any of the violations involving verbal reprimand or written warning referred to in the point above, more than twice within a period of two years, or violate several times internal procedures provided for by this Model on a single occasion or adopt several times behaviours that breach the requirements of Model in the course of the activities of the areas at risk, provided that such conduct does not lead to the application of measures provided for by the Decree;
- suspension from service and remuneration for a period not exceeding three days is incurred by employees who:
    - by violating the procedures provided for by this Model or adopting behaviours that breach the requirements thereof, cause damage to the Company or expose it to an

objective situation of danger, provided that these behaviours are not clearly aimed at committing an offence or result in the application of measures set out in the Decree;

- relapse in a behaviour involving any of the violations that provide for a fine as specified in the paragraph above, more than twice in a period of two years;

- disciplinary dismissal with right of notice in accordance with the applicable national collective labour agreement(s) is incurred by employees who relapse in any of the violations involving suspension referred to in the preceding paragraph point more than twice within a period of two years, after formal written warning; dismissal for just cause without notice shall occur if the employee behaves in a manner which does not conform to the provisions of the Model and is directed solely at committing an offence provided for by the Decree and if employees adopt conduct that blatantly violates the requirements of the Model involving the application by the Company of the measure set out by the Decree or if the employee violates the measures to protect the whistleblower or makes intentional or grossly negligent reports that prove to be unfounded.

Moreover, with reference to the risk of committing offences that violate regulations concerning occupational health and safety provided for by the Circular of the Ministry of Labour No. 15816 of 11 July 2011 concerning the "*Organisational and Management Model as per Article 30 of Legislative Decree No. 81/2008*":

- a measure of written warning is incurred by employees who do not comply with the Model in the case where the violation involves the occurrence of a situation of potential danger for the physical integrity of one or more persons including the author of the violation, and provided that one of the cases provided for in the following paragraphs;

- a fine is incurred by employees who relapse in a behaviour in the case of any violations that involve a written warning as referred to in the point above more than two times in a period of two years or who do not comply with the Model, in the case in which the violation involves the occurrence of an injury to the physical integrity of one or more persons, including the

author of the violation, and provided that one of the cases provided for in the following paragraphs;

- suspension from service and remuneration for a period not exceeding three days is incurred by employees who:
    - do not comply with the Model, in the case in which the violation causes injury qualifiable as "serious" to the physical integrity of one or more persons, including the author of the violation, pursuant to article 583, paragraph 1, of the Criminal Code, and provided that one of the cases provided for in the following paragraph;
    - relapse in conduct involving any of the violations that provide for a fine as specified in the paragraph above, more than twice in a period of two years;
- disciplinary dismissal with the right of notice shall be imposed on employees who commit a repeat conduct in any of the violations involving suspension of service and remuneration, as specified in the preceding point, more than twice in a period of two years; employees who do not comply with the Model shall be dismissed for just cause without notice, if the violation causes an injury, which can be qualified as very serious under article 583, paragraph 2, of the Criminal Code, to the physical integrity or death of one or more persons, including the perpetrator of the infringement.

It is understood that the provisions of the Model cannot be interpreted in such a way as to constitute a derogation from the provisions concerning sanctions for unjustified dismissals set out in Article 18 of Law No. 300/1970 as amended by Law No. 92 of 28 June 2012, and by Legislative Decree No. 23 of 4 March 2015.

6.4. Violation of the Model by executive managers and related measures

With regard to violations of the single rules contained in this Model, including the violation, in any way, of the measures to protect the whistleblower, or the malicious or grossly negligent making of reports that prove to be unfounded committed by Company employees with executive status, these also constitute a disciplinary offence.

Any violation authorises the SB to require the Chairman to impose one of the sanctions listed below, determined on the basis of the seriousness of the violation committed in the light of the criteria indicated in paragraph 6.2 and of the behaviour carried out before (e.g., any previous violations committed) and after the fact (e.g., the communication to the SB of the irregularity) by the perpetrator of the violation.

Disciplinary measures that can be imposed against said executives - in compliance with the procedures laid down in article 7, paragraphs 2 and 3, of Law no. 300 of 30 May 1970 (Workers' Statute) as well as the national collective labour agreement(s) applied and any special regulations applicable - are those provided for by the following penalty system:

- Written reprimand;
- Dismissal for cause with the right to notice;
- Dismissal for cause.

In any case, the penalties applied and/or violations ascertained will always be notified by the competent company function to the Supervisory Board.

In particular, with reference to violations of the Model by executives, it is provided that:

- In the event of a non-serious violation of one or more procedural or behavioural rules provided for in the Model, an executive incurs in a written reprimand consisting in a warning to observe the Model, which constitutes a necessary condition for maintaining a relationship of trust with the Company;
- In the case of a serious breach of one or more procedural or behavioural rules provided for in the Model such as to constitute a significant violation, or in the event of a repeat violation involving a disciplinary written reprimand, the executive will incur a measure of justified dismissal with right to notice;
- In the event that the violation of one or more of the procedural or behavioural requirements of the Model is so serious as to irreparably damage the relationship of trust, not allowing the continuation, even temporarily, of the employment relationship, including the event of

violation of the measures to protect the *whistleblower*, or in the event of the malicious or grossly negligent making of reports that prove to be unfounded, the executive will incur a measure of dismissal for cause.

Also, for company workers who are executive managers, the following are serious violations of the Model's instructions:

- non-observance of the obligation to manage or supervise employees regarding the correct and actual application of the model;
- non-observance of the obligation to manage and supervise other workers who, although not associated with the company by some form of subordinate contract (e.g. Self-employed workers, consultants, collaborators, etc.), are subject to management and supervision of the executive manager pursuant to article 5, par. 1, letter b), Leg. Decree 231/2001, notwithstanding the level of the contract with these workers.

It is understood that the provisions of the Model cannot be interpreted in such a way as to constitute a derogation from the provisions concerning sanctions for unjustified dismissals set out in Article 18 of Law No. 300/1970 as amended by Law No. 92 of 28 June 2012, and by Legislative Decree No. 23 of 4 March 2015.

6.5. Measures against members of the Managerial Body

In the event of violation of the Model, including the violation, in any way, of the measures to protect the whistleblower, or the malicious or grossly negligent making of reports that prove to be unfounded by one or more members of the Company's Executive Body, the SB will inform the entire Board of Directors and the Sole Auditor that they will take the appropriate measures consistent with the seriousness of the violation committed, in light of the criteria set out in paragraph 6.2 and in accordance with the powers provided for by law and/or the Articles of Association (declarations in the minutes of meetings, request to convene or calls of the Shareholders' Meeting with appropriate measures on the agenda against those responsible for the violation, etc.).

Disciplinary measures that can be imposed against one or more members of the Executive Body, subject to a resolution of the Board of Directors to be adopted with the abstention of the person concerned and, where provided for by law and/or the Articles of Association, by resolution of the Shareholders' Meeting, are those provided for by the following penalty system:

- Written warning;
- Temporary suspension from appointment;
- Revocation of appointment.

In particular in reference to violation of the model enacted by one or more members of the company managerial body, it is foreseen that:

- In the event of a non-serious violation of one or more procedural or behavioural rules provided for in the Model, a member of the Executive Body incurs in a written reprimand consisting in a warning to observe the Model, which constitutes a necessary condition for maintaining a relationship of trust with the Company;
- in the event of a serious violation of one or more procedural or behavioural rules provided for in the Model, the member of the Executive Body is temporarily suspended from office;
- In the event of a serious violation of one or more procedural or behavioural rules provided for in the Model such as to irreparably damage the relationship of trust, including the event of violation of the measures to protect the whistleblower, or in the event of the malicious or grossly negligent making of reports that prove to be unfounded, the member of the Executive Body shall be dismissed from office.

In addition to the members of the Executive Body of the Company, a punishable violation of the Model is also a violation of the obligation of direction or supervision of staff concerning the correct and effective application of the requirements of the Model.

6.6. Measures against members of the Supervisory Body (SB) and third parties

For measures against the members of the SB, reference should be made to the rules for their removal from office (paragraph 5.4).

For measures against third parties, reference should be made to the rules governing relations with them (paragraph 4).

7. Communication of Model and training of recipients

The external communication of the Model is carried out through the most appropriate means (e.g., the Company's website).

The HR function is tasked operationally with training relating to the Model and the relevant regulations and for this purpose it coordinates itself with the Supervisory Body.

The Company formalises and implements specific training plans, with the aim of ensuring effective knowledge of the Decree, the Code of Conduct and the Model; the contents of training are differentiated according to whether it is aimed at employees as a whole, employees operating in specific risk areas, Directors, etc.

Participation in training is mandatory and participants' attendance is traced.

The training can also take place through the use of IT tools (e.g., in "e-learning" mode) and is carried out with the support of experts in the reference regulations.

SPECIAL PART

8. Introduction

As already pointed out in paragraph 3 of the General Section, pursuant to the provisions of article 6, paragraph 1, letter a) of the Decree, the Company has identified the at-risk activities (Control and Risk Self Assessment).

The Company has therefore identified and effectively implemented adequate controls in the control system in order to make it suitable for reducing the risk of commission of offences.

They are indicated below:

- At-risk activities with reference to each category of offence identified as relevant for the Company;
- For each At-risk Activity, the controls in place, aimed at or in any case suitable for reducing the risk of committing the alleged offences. These controls are contained in the Procedures and other parts of the internal control system.

9. Relevant underlying crimes for the company

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following crimes as relevant:

- offences against the Public Administration (arts. 24 and 25);
- Cyber crimes and the illegal handling of data (art. 24-*bis*);
- Crimes of organised crime and transnational crimes (art. 24-*ter* and art. 10 of Law no. 146 dated 16 March 2006);
- crime against industry and commerce (art. 25-*bis*.1);
- Corporate crimes, including those of corruption between private subjects (art. 25-ter);

- Crimes against individual personality (art. 25-*quinquies*);
- manslaughter or serious or extremely serious injury, committed by violating the laws on health and safety in the workplace (art. 25-*septies*);
- Handling, laundering and use of money, assets or profits of illegal origin, in addition to self-laundering (art. 25-*octies*);
- Crimes relating to the violation of copyright (art. 25-*novies*);
- Inducement not to make declarations or make untruthful declarations to the judicial authorities (art. 25-*decies*);
- Environmental crimes (art. 25-*undecies*);
- Employment of foreign citizens with no permits of stay (art. 25-*duodecies*);

10. Control devices

In managing all sensitive activities, in addition to the Code of Conduct, the following control devices are also used:

- it is forbidden to behave:
  - In a manner to integrate the cases given of crime as above;
  - In a manner that although it isn't a case of crime as such as specified above, it may potentially become one;
  - In a manner not in line or not compliant with the principles and prescriptions contained in the Model and in the Code of Conduct;
- The sensitive activities must be managed exclusively by the competent company departments;
- Company employees must strictly abide by and observe any limits set in the organisational proxies or proxies awarded by the company;

- Company employees must observe company procedures applicable to sensitive activities, suitably updated and diffused inside the organisation.

11. Crimes against the Public Administration

11.1. Applicable crimes

Consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following crimes against the PA as relevant:

Misappropriation to the damage of the State (art. 316-*bis Criminal Code*)	Consisting in the conduct of whomsoever, outside Public Administration, having obtained grants, subsidies or loans from the State or other public body or from the European Communities intended to favour initiatives aimed at the realization of works or the performance of activities of public interest, do not use them for the aforesaid purposes.
Misappropriation of funds from the state (Article 316-ter of the Criminal Code)	consisting in the conduct of whomsoever, unless the act constitutes the offence set out in article 640-bis of the Criminal Code, through the use or presentation of false statements or documents or documents attesting to untrue things, or through the omission of due information, unduly obtains, for themselves or for others, contributions, loans, subsidised mortgages or other disbursements of the same type, whatever denominated, granted or paid by the State, by other public bodies or by the European Communities.
Fraud against the State or other public entity (Article 640, paragraph 2, point 1, of the Criminal Code)	Consisting in the conduct of whomsoever, by means of trickery or deception, mislead someone into error, procure an unfair profit to the detriment

	of others for themselves or others, if the act is committed to the detriment of the State or another public body or on the pretext of having someone exempted from military service.
Aggravated fraud to obtain public funds (Article 640-bis of the Criminal Code)	consisting in the same conduct referred to in the point above if it is committed to obtain subsidies, loans, subsidized mortgages or other funds of the same kind, however denominated, granted and paid by the State, other public bodies or by the European Communities.
Computer fraud against the State or other public entity (Article 640-ter of the Criminal Code)	consisting in the conduct of whomsoever, by altering in whatever way the functioning of a computer or computer system or intervening without right, by whatever means, on data, information or programmes contained in a computer or computer system or a system relating thereto, procures for himself or others an unlawful profit to the detriment of the State or other public entity
Bribery for the performance of an official act (Article 318 of the Criminal Code)	consisting in the conduct of a public official who, in order to exercise his/her functions or authority, unduly receives, either for himself/herself or for a third party, money or other benefits or the promise of such

Bribery for the performance of an act in breach of official duties (Article 319 of the Criminal Code)	consisting in the conduct of a public official who receives, for himself or a third party, money or other benefits, or accepts a promise of such money or benefits, in order to omit or delay or for having omitted or delayed an official duty, or in order to perform or for having performed an act contrary to his official duties
Bribery in judicial proceedings (Article 319-ter of the Criminal Code)	consisting in acts of corruption if committed in order to favour or damage a party in civil, criminal or administrative proceedings
Undue inducement to give or promise benefits (Article 319 quater of the Criminal Code)	consisting in the conduct of a public official or person in charge of a public service who, by abusing his position or powers, induces anyone to wrongfully give or promise him or a third party money or other benefits, unless it constitutes a more serious offence, as well as in the conduct of whomsoever gives or promises money or other benefits
Bribery of a public service officer (Article 320 of the Criminal Code)	consisting in conduct referred to in Articles 318 and 319 of the Criminal Code, if committed by a person tasked with a public service
Penalties for the corrupter (Article 321 of the Criminal Code)	pursuant to which the punishments laid down in articles 318, paragraph 1, 319, 319-bis, 319-ter and 320 of the Criminal Code in relation to the cases set out in Articles 318 and 319 of the Criminal Code, apply also to whomsoever give or promise

	a public official or person responsible for a public service money or other benefits.
Incitement to bribery (Article 322 of the Criminal Code)	consisting in the conduct of whomsoever offers or promises money or other benefits not due to a public official or a person in charge of a public service for the exercise of his/her functions or powers, or to induce him/her to omit or delay an act of his/her office, or to act contrary to his/her duties, if the offer or promise is not accepted, as well as by in conduct of a public official or a person in charge of a public service who solicits a promise or offer of money or other benefit for the exercise of his/her functions or powers or solicits a promise or the giving of money or other benefits by a private citizen for the purposes set out in Article 319 of the Criminal Code

on the basis of the reference to Article 322-bis made by Article 25, paragraph 4 of Legislative Decree no. 231/2001, the offences referred to in Articles 314, 316, 317 to 320 and 322, third and fourth paragraphs of the Criminal Code apply even if the conduct is directed towards:

- members of the Commission of the European Communities, the European Parliament, the Court of Justice and the Court of Auditors of the European Communities;
- officials and contracted agents within the meaning of the Staff Regulations of officials of the European Communities or the conditions of employment of agents of the European Communities;

- any person seconded to the European Communities by the Member States or by any public or private body, who carries out functions equivalent to those performed by European Community officials or other agents;
- The members and workers to bodies constituted on the basis of the Treaties that the European Communities set up;
- whomsoever, in other EU Member States, perform functions or activities equivalent to those of Italian public officials and persons in charge of a public service;
- judges, prosecutors, deputy prosecutors, officials and agents of the International Criminal Court, persons who are seconded by States Parties to the Treaty establishing the International Criminal Court and who perform functions corresponding to those of officials or agents of the International Criminal Court, and members and agents of entities formed on the basis of the Treaty establishing the International Criminal Court.

The provisions of Articles 319-quater, second paragraph, 321 and 322, first and second paragraphs, shall also apply if the money or other benefit is given, offered or promised to:

- persons mentioned in the first paragraph of the Article;
- persons exercising functions or activities corresponding to those of public officials and of person in charge of a public service in other foreign States or public international bodies, where the fact is committed to obtain an undue advantage in international business transactions or to obtain or maintain an economic and financial business for oneself or others.

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

11.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activities in reference to crimes against the PA:

- management of relations with the Public Administration for the request of permits, licences etc:
- Management of relations with Public Administration during inspections (e.g., health and safety in the workplace, environmental, tax, etc.);
- Litigation management (e.g. civil and labour law);
- Procurement of goods, services and consultancies including managing subcontracts;
- Management of monetary and financial flows - payments;
- Managing outgoing invoices and credit;
- Managing infra-group relations (e.g. sale of goods/services);
- Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.
- Managing expense sheets and relative reimbursements

11.3. Control devices

The current control devices for each sensitive activity are given below:

Managing relations with the Public Administration for the request of permits, authorisations etc

- Relations regarding the sensitive activity in question are normally managed by the CEO; other subjects that hold relations with public subjects (Deployment Manager, Regional Manager, Sub-Regional Manager, Site Permit Specialist) are awarded suitable powers;
- The necessary documents for requests are prepared by the Site Permit Specialist and are submitted to public bodies by consultants who are coordinated and supervised by the Regional Managers;

- Guidelines for the management of relations with public subjects include the principles set out in the Code of Conduct;
- Contacts with Public Administration exponents and results achieved are reported and tracked using emails sent by the Site Permit Specialist to the Regional Managers and then archived;
- The sensitive activity in question is regulated by a procedure that governs the rules of conduct, roles and responsibilities, operational modes, traceability and filing of reports and documents.

Management of relations with Public Administration during inspections (e.g., health and safety in the workplace, environmental, tax, etc.)

- Powers for managing the sensitive activity in question are awarded to the CEO and to the latter's staff for activities carried out in service by ZTE Italia;
- The various subjects involved in the various phases of the process are clearly identified. In particular:
    - in the case of labour law/social security, workplace health and safety and environmental inspections and/or assessments, the involvement of the ZTE Italia HR Manager and the Prevention and Protection Service Manager (RSPP) and any other delegated figures on sites is envisaged;
    - in the event of inspections and/or assessments in administrative/financial matters by the Guardia di Finanza (Italian Tax Police) and Agenzia delle Entrate (Italian Revenue Agency), the involvement of the ZTE Italia Finance Manager is envisaged;
    - these persons are supported by the persons in charge of the departments involved in the inspections, by the CEO and by the ZTE Italia Legal Counsel;

- inspectors may be provided with appropriate facilities (e.g., segregated rooms, network access, hardware, etc.) at the request of the inspectors;
- the persons who participate in checks, inspections or audits inform their hierarchical superior and the SB of any critical issues that have emerged during the execution of the assessments, inspections or audits, and communicate to them:
    - ID of inspectors (name and body belonging to);
    - the date and time of arrival of the inspectors;
    - The duration of the inspection;
    - The subject of the inspection;
    - The result of the inspection;
    - Any report drawn up by the inspection body;
    - the list of any documents handed over;
- The document is kept by the departments involved in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls;
- The sensitive activity in question is regulated by a procedure that governs the rules of conduct, roles and responsibilities, operational modes, traceability and filing of reports and documents.

Management of disputes (e.g. Civil and labour)

- The powers for managing the sensitive activity in question are awarded to the ZTE Italia Legal Counsel, the Chairman of the Board of Directors and the CEO;

- The Chairman of the Board of Directors and the CEO confer mandates on external professionals appointed for the dispute and inform the Supervisory Board about the commencement of the proceedings, the results of various phases of the activity, the conclusion of the proceedings and any critical factor that may occur in *itinere*;
- The various subjects involved in the various phases of the sensitive activity in question are clearly identified. In particular:
    - The ZTE Italia Legal Counsel selects external consultants and manages the disputes with their support, and the ZTE Corporation Legal Team;
    - After the selection by the ZTE Corporation Legal Counsel and Legal Team, the Chairman of the Board of Directors and the CEO of ZTE Servizi award the mandate to the legal consultants;
- Each of the parties involved is responsible for the traceability of the requests for information received during the dispute, as well as for the internal evaluation and authorization process of the documentation submitted during the dispute.

Procurement of goods, services and consultancies including managing subcontracts

- The powers for managing the sensitive activity in question are awarded to the CEO;
- The various subjects involved in the various phases of the sensitive activity in question are clearly identified:
    - in the case of small purchases, it is the function concerned that directly manages needs by submitting a request for offer to three market participants;
    - in other cases, the ZTE Corporation Procurement departments manage the selection of suppliers, consultants and subcontractors and carry out scouting, evaluate offers and negotiate agreements;

- This selection is shared with the Deployment Manager for technical specifications;
- The Outsourcing department takes care of collecting the documents required by the subcontractors (DUVRI - single document on the risk of interference - etc);
- The Prevention and Protection Service Manager (RSPP) supervises the firms appointed on sites for health and safety matters;

- the selection of suppliers is characterised by a systematic evaluation of their integrity requirements;
- remuneration to suppliers is adequately justified in relation to the type of goods/services provided and is in line with existing market conditions or practices;
- the contractual relationships are constantly formalised by means of a written contract drawn up on the basis of a template provided by the Legal Counsel and duly authorized and signed by the CEO;
- the employment contracts provide for a contractual clause/addendum with the commitment to comply with the principles of the Model and the Code of Conduct;
- each supplier is required to sign clauses to adhere to the Group's anti-bribery policy and to the principles of the Code of Conduct, as well as to fill in and sign the ZTE Supplier CSR - Letter of Commitment;
- The consultants are chosen transparently and in a non-discriminating mode, based on requisites of professionalism, independence and competence and are appointed by subjects with suitable powers based on the proxies awarded by the company;
- The appointment of consultant is made in writing with an indication of the fee agreed and the content of the service to be provided;
- Consultancy contracts that provide for “success fees” state clear parameters, that can be documented and verified, for the attribution of said variable component of the fee;

- On completion of the appointment, the consultant must state the services provided in writing.
- The fees for consultants must be suitable justified by the type of service/appointment and are in line with the existing conditions or practices on the market or professional rates currently in force for the category involved;
- The document is kept by the departments involved in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls;
- The sensitive activity in question is governed by the Procedures "*(Transitional) Purchase Bidding Management Regulation for Non-Production Materials (of the Administrative Service Type)*", "*Purchase Bidding System Training Course (Non-Production Materials of the Administrative Service Type)*" and by the procedures regarding *subcontractors*.

Management of monetary and financial flows - payments

- The powers for managing the sensitive activity in question are awarded to the directors;
- Limits to the autonomous use of financial resources are set, by defining spending thresholds, consistent with the management competences and organisational responsibilities;
- The various subjects involved in the various phases of the sensitive activity in question are clearly identified:
    - the ZTE Italia Administration department controls incoming invoices and uploads them into the FOL system (Group *software*) that allocates a protocol number and an ID code for the company;
    - the ZTE Italia Finance Department then carries out a further control and draws up a report with payment deadlines;

- The FOL system provides for various approval steps, that involve the requesting department manager, the ZTE Corporation Accounting and Audit departments and the ZTE Italia Finance Manager;
- ZTE Corporation uploads into the bank to make payments and also carries out banking reconciliations, monitored by the ZTE Italia Finance Manager;

- Except for situations of need or urgency, for which specific compensatory controls are provided, there is no subjective identity between those who commit the company with third parties and those who authorise the payment of sums due based on commitments taken
- Specific reports must be carried out and all the authorisation steps must be recorded on the system;
- The operations that require use of economic or financial resources have a reason expressed and are motivated by the requesting subject, and are documented and recorded in compliance with the principles of professional and accounting correctness;
- Flows in cash are not permitted, except for minimum types of expenses (petty cash) expressly authorised by the managers of the departments involved;
- In reference to banking and financial operations, the company only uses financial and banking intermediaries subjected to transparency and correctness regulations, compliant with European Union law;
- Payments to third parties are made via bank circuits using media that guarantees evidence that the payment beneficiary is actually the third party with a contract with the company;
- The sensitive activity in question is regulated by a procedure that governs activities in the Administration and Finance area, which defines the rules of conduct, the roles and responsibilities, information flows between ZTE Corporation, ZTE Italia and the company, operational modes, traceability and document archiving in reference to

managing financial transactions.

Managing outgoing invoices and credit

- The powers for managing the sensitive activity in question are awarded to the directors;
- The various subjects involved in the various phases of the sensitive activity in question are clearly identified:
    - After carrying out tests, ZTE Servizi obtains the certificate of acceptance of works that is signed by a company representative, empowered with the specific proxies/powers, by the subcontractor and the commissioning client;
    - After accepting the work, the ZTE Italia Finance Manager proceeds with issuing the invoice;
    - The relevant Account Manager, and the ZTE Italia Finance Department manage reminders in the event of delays in incoming payments;
    - ZTE Corporation regularly carries out banking reconciliations;
- The document is kept by the departments involved in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls;
- The sensitive activity in question is regulated by a procedure that defines the rules of conduct, roles and responsibilities, operational modes, traceability and archiving of documents, in particular in reference to the activities aimed at guaranteeing the correct execution of the contract consistently with what is agreed with the commissioning client.

Managing infra-group relations (e.g. sale of goods/services)

- All intercompany relations are formalised in the "*Intercompany Services Framework Agreement*", authorised and signed consistently with the current system of powers;
- The fees foreseen in the intercompany contracts correspond to market criteria;
- *intercompany* transactions are recorded via an ad hoc system managed by the ZTE Corporation Finance department;
- Intercompany reconciliations are systematically carried out;
- Reconciliation reports are systematically archived;
- The sensitive activity in question is regulated by a procedure that governs activities in the Administration and Finance area, which defines the rules of conduct, the roles and responsibilities, information flows between ZTE Corporation, ZTE Italia and the company, operational modes, traceability and document archiving in reference to managing intercompany transactions, in particular with reference to:
    - Preparation, control and authorisation of *intercompany* contracts;
    - management of intercompany invoices and payments;
    - Evaluation and execution of fiscal obligations with reference to the sale of intercompany goods/services (transfer pricing models).

Selection, recruitment and management of staff including administered staff, including management of bonus and reward system

- The powers for managing the sensitive activity in question are awarded to the Chairman of the Board of Directors and the CEO;
- The various subjects involved in the various phases of the process are clearly identified. In particular:

- The department involved makes the request for additional resources or a replacement;
- The ZTE Italia HR Manager draws up the *job description*;
- The interview is managed by the Regional Managers and the technical managers;
- The Chairman of the Board of Directors and the company CEO sign the letter of employment;

➢ insertion process is carried out in the following steps:

- Communication of need for resources by the department involved to the ZTE Italia HR Manager;
- Definition of role (job description), by the ZTE Italia HR Manager;
- First *screening* of CVs by external company that supports the ZTE Italia HR Manager;
- sending of CVs selected by ZTE Italia HR Manager to Regional Manager and Technical Managers;
- evaluation interviews;
- Evaluation sheets filled out after each interview;
- Contract drawn up and selected resource inserted;

➢ Direct and indirect relations between candidate and the PA are checked and evaluated beforehand;

➢ The CVs received from candidates and interview sheets are kept in a paper archive for each subject hired by the ZTE Italia HR Manager;

➢ Candidate evaluations are formalised in specific documents that are then archived by the ZTE Italia HR Manager;

- Hiring contracts have a contractual clause/*addendum* of undertaking to the principles of the Model and the Code of Conduct;
- In reference to remuneration of resources:
    - Pay packets are processed using specific software and with the aid of an external consultant;
    - *payroll* is outsourced;
- The bonus system is drawn up on the basis of objective criteria, depending on the results achieved;
- at the start of the year a goals plan is drawn up with a quarterly review;
- Communications to employees used to show bonuses and rewards are regularly formalised by the ZTE Italia HR Manager;
- The bonus is paid out on payslips
- The document is kept by the departments involved in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls;
- The sensitive activity in question is governed by the Procedures "*Regulation on New Hire Selection and On-boarding*" and "*Regulation on Performance Evaluation*".

Managing expense sheets and relative reimbursements

- Prior authorisation for a transfer is issued in writing by the Line Manager;
- in order to ask for a reimbursement, employees must upload their expense sheets onto the FOL system, stating the type of expense incurred and a description thereof;

- The FOL system automatically produces a page with a bar code that must be printed and handed to the ZTE Italia Administration department, with justification documents attached;
- payment of expense sheets, by the ZTE Italia and ZTE Corporation Finance Department, follows the procedure foreseen, with reference to payment for the sensitive activity of "Managing monetary and financial flows – Payments";
- The sensitive activity in question is governed by the document "*ZTEIT_Regolamento_04 Business trip*".

12. Cyber crimes and the illegal handling of data

12.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following cyber crimes as relevant:

Forging digital documents (art. 491-*bis* Criminal Code)	consisting in cases of falsehoods, whether material or ideological, committed on public deeds, certificates, authorisations by a representative of Public Administration or by a private party, if they concern a "computer document with probative effect," i.e., a computer document with at least a simple electronic signature. “Computer document” means the computer representation of acts, facts or data that are legally relevant (such crime extends the criminal prosecution of offences provided for in Book II, Title VII, Chapter III of the Criminal Code to computer documents with probative effect)
Illegal access to a computer or remote system (art. 615-*ter Criminal Code*)	Consisting in conduct of whomsoever unlawfully introduces oneself, i.e., circumventing any form, even minimal, the barriers to entry into a computer or computer system protected by security measures, or maintains it against the will of those who have the right to exclude it.
Unauthorized possession and circulation of access codes to computer or telecommunications	consisting in the conduct of whomsoever unlawfully obtains, reproduces, spreads, communicates or gives codes, keywords or other suitable means to access to a computer or computer system, protected by security

systems (Article 615-quater of the Criminal Code)	measures, or in any case provides indications or instructions suitable for the purpose of obtaining a profit for oneself or others or of damaging others
Distribution of equipment, devices or programs intended to damage or interrupt a computer or telecommunications system (Article 615-quinquies of the Criminal Code)	consisting in conduct of whomsoever, in order to unlawfully damage a computer or computer system, computer data or programmes contained therein or pertaining thereto, or to contribute to the total or partial interruption or alteration of its functioning, obtains, produces, reproduces, imports, spreads, communicates or in any way puts at the disposal of others computer equipment, devices or IT programmes
Installation of equipment designed to intercept, prevent or interrupt computer or telecommunications communications (article 617-quinquies of the Criminal Code)	consisting in conduct of whomsoever, except for the cases permitted by law, installs equipment capable of intercepting, preventing or interrupting communications relating to a computer or computer system or between multiple systems
Damage to computer information, data or programmes (article 635-bis of the Criminal Code)	consisting in the conduct of whomsoever destroys, deteriorates, deletes, alters or suppresses computer information, data or programmes of others, unless the fact constitutes a more serious offence
Damage to information, data or programs used by the state or other public entity or, in any case, of public benefit (Article 635-ter of the Criminal Code)	consisting in the conduct of whomsoever destroys, deteriorates, deletes, alters or suppresses any computer information, data or programmes used by the State or any other public body, or body anyway having a public utility, provided that the act does not constitute a more serious offence

Damage to computer or telecommunications systems (Article 635-quater of the Criminal code)	consisting in conduct of whomsoever, through any of the conducts under Article 635-bis of the Criminal Code, or through the introduction or transmission of data, information or programmes, destroys, damages or makes unusable, either in whole or in part, the computer or computer systems of others or seriously hampers their functioning, provided that the act does not constitute a more serious offence
Damage to computer or telecommunications systems of public benefit (Article 635-quinquies of the Criminal Code)	consisting in conduct described in the article 635-quater of the Criminal Code, if it is aimed at destroying, damaging, making unusable, in whole or in part, any computer or computer system of public utility or at seriously hampering their functioning.
Computer fraud by the individual providing electronic signature certification services (article 640-quinquies of the Criminal Code)	consisting in conduct of whomsoever provides electronic signature certification services in order to procure unfair profits for oneself or others or to cause other damage, violates obligations provided for by the law for the release of a qualified certificate

For an example of the possible methods of committing offences, reference should be made to the document "Control & risk self assessment and Gap analysis pursuant to Legislative Decree *231/2001*".

12.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activity in reference to cyber crimes:

- Managing information systems.

12.3. Control devices

The current control devices for the sensitive activity in question are given below:

Managing information systems.

- The software used for company management is standard software downloaded from a specific group platform;
- The purchase of licences for said software is by ZTE Corporation;
- The systems are subject to backups with servers in Germany;
- Network security is guaranteed by suitable firewall systems;
- Access to workstations is protected by alphanumerical passwords;
- Implementation, maintenance and monitoring of security devices are managed by ZTE Corporation
- ZTE Corporation manages the ZTE Italia website and relative content;
- traceability of operations carried out and relative communications between users and the ZTE Corporation IT support is guaranteed;
- The sensitive activity in question is governed by the "IT Security Policy", containing instructions for users on the correct use of systems and security regulations to observe.

13. Organised crime and transnational crimes

13.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following organised crimes as relevant:

Crime syndicate (Article 416 of the Criminal Code)	consisting in the conduct of whomsoever promotes, establishes and organises an association of three or more persons in order to commit more than one offence and whomsoever participates in it
Mafia-type association (Article 416-bis of the Criminal Code)	Punishes whomsoever participates in a Mafia-type association including three or more persons, including whomsoever promotes, direct and organise it. Mafia-type association is said to exist when the participants take advantage of the intimidating power of the association and of the resulting conditions of submission and silence to commit criminal offences, to manage or at all events control, either directly or indirectly, economic activities, concessions, authorizations, public contracts and services, or to obtain unlawful profits or advantages for themselves or for others, or with a view to prevent or limit the freedom to vote, or to get votes for themselves or for others on the occasion of an election. An association is said to be of the armed type when the participants have firearms or explosives at their disposal, even if hidden or deposited elsewhere, to achieve the objectives of the said association. The provisions of article 416-bis of the Criminal Code also apply to the Camorra and to

	any other associations, whatever their local titles, even foreign, seeking to achieve objectives that correspond to those of Mafia-type unlawful association by taking advantage of the intimidating power of the association.
Crimes committed using the conditions set forth in article 416-bis of the Criminal Code, i.e., to facilitate the activities of associations as set out in the same article	
Inducement not to make declarations or make untruthful declarations to the judicial authorities (art. 377-Bis Criminal Code);	consisting in the conduct of whomsoever, by violence or threats, or by offering or promising money or other advantage induces a person summoned to give a statement usable in criminal proceedings before the judicial authority, not to give statement, when such a person has the right to remain silent, unless the act constitutes a more serious offence
Abetting (art. 378 Criminal Code)	consisting in conduct of whomsoever, after committing a crime for which the law establishes the death penalty, life imprisonment or imprisonment, and apart from the cases of conspiracy therein, helps individuals to circumvent investigations of authorities, or to evade the search of the authorities

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

13.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activities in reference to organised crime and transnational crimes:

- Procurement of goods, services and consultancies including managing subcontracts;
- Management of monetary and financial flows - payments;
- Managing infra-group relations (e.g. sale of goods/services);
- Managing fiscal matters;
- Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.

13.3. Control devices

The current control devices for each sensitive activity are given below:

Procurement of goods, services and consultancies including managing subcontracts

The control devices are the same as the ones in section 11.3 of the herein Special Part and the corresponding sensitive activity. Also:

- In choosing Suppliers, Contractors, Consultants, the propensity for counterparties with the most ethical, organisational, technical and financial guarantees is ensured (including but not limited to, ethical qualification elements such as the signing of Legality Protocols, the registration in White Lists established at Prefectures, the request or the achievement of legality rating are duly taken into account);
- third parties who refuse to provide or otherwise fail to provide such documentation are not selected as contractual counterparties of ZTE Servizi;

- Periodic monitoring of Suppliers, Contractors, Consultants selected in a re-qualification process is carried out.

Management of monetary and financial flows - payments

Managing infra-group relations (e.g. sale of goods/services)

The control devices are the same as the ones in section 11.3 of the herein Special Part and the corresponding sensitive activities.

Managing fiscal matters

- The powers for managing the sensitive activity in question are awarded to the CEO;
- The various subjects involved in the various phases of the sensitive activity in question are clearly identified. In particular, tax requirements are managed by the ZTE Italia Accounting department, with the support of an external tax consultant: the ZTE Italia Accounting department prepares the draft tax calculation (including VAT calculations), the tax consultant verifies the draft and pays taxes;
- traceability of transactions is guaranteed by the information systems used in company operations, while that of services rendered is attested by the presence and archiving of documents and internal communications;
- The document is kept by the ZTE Italia Accounting department in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls;
- The sensitive activity in question is regulated by a procedure that governs activities in the Administration and Finance area, which defines the rules of conduct, the roles and

responsibilities, information flows with the external taxation consultant, operational modes, traceability and document archiving in reference to managing fiscal obligations.

Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.

The control devices are the same as the ones in section 11.3 of the herein Special Part and the corresponding sensitive activity. Also:

- During selection for recruitment, the criteria of a candidate's reputation are considered;
- Candidates must submit a self-declaration on their criminal record.

With specific reference to the inducement to not make declarations or to make untruthful declarations to the judicial authorities (art. 377 bis, Criminal Code), please refer to section 20.2 of the herein Special part.

14. Crimes against industry and commerce

14.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following crimes against industry and commerce as relevant:

Manufacturing and sale of goods produced encroaching on industrial property rights (Article 517-ter of the Criminal Code)	constituted by the conduct of whomsoever, being able to know of the existence of the industrial property title, manufactures or uses industrially objects or other goods made by usurping an industrial property title or in violation of it, or of whomsoever, in order to make a profit, introduces into the territory of the State, holds for sale, puts on sale with direct offer to consumers or puts into circulation the aforementioned goods.

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

14.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activity in reference to crimes against industry and commerce:

- Execution of service contracts.

14.3. Control devices

The current control devices for the sensitive activity in question are given below:

Execution of service contracts.

- The powers for managing the sensitive activity in question are awarded to the CEO;
- During the test phase as per the sensitive activity in question, the following are present:
    - A representative from the commissioning client;
    - A representative from ZTE Servizi;
    - the *subcontractor* who carried out the work;
- If the test is successful, an acceptance of works certificate is signed;
- the documentation is kept, by the departments concerned, in a specific archive, in such a way as to prevent its subsequent modification, in order to allow the correct traceability of the entire process and to facilitate any subsequent controls;
- The sensitive activity in question is regulated by a procedure that defines the rules of conduct, roles and responsibilities, operational modes, traceability and filing of documents, in particular for the activities aimed at ensuring the correct execution of the contract in compliance with what was agreed with the commissioning client.

15. Corporate crimes, including those of corruption between private subjects

15.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following corporate crimes as relevant:

False corporate communications (art. 2621 Civil Code)	consisting in the conduct of directors, general managers, managers in charge of drawing up the company's accounts, statutory auditors and liquidators, who knowingly present untrue significant material facts in the financial statements, reports, or other corporate disclosures for shareholders or the public, in a way that actually misleads others in cases where the economic, equity or financial position of the company or the group that the company belongs to has to be communicated by law, in order to procure wrongful profit for themselves or others
Impeding control (art. 2625 Civil Code)	consisting in the conduct of directors who, by concealing documents or with other suitable means, prevent or otherwise hinder the performance of control activities legally attributed to shareholders or other corporate bodies
Unlawful return of capital contributions (Article 2626 of the Civil Code)	consisting in conduct of directors who, except for cases of lawful reduction of share capital, return, even under false pretences, contributions to shareholders or release them from the obligation to execute them

Unlawful distribution of earnings and reserves (Article 2627 of the Civil Code)	consisting in the conduct of directors who share out profits or advances on profits that have not actually been earned or that should be allocated to reserves pursuant to the law or distribute reserves, including not comprising profits, that may not be lawfully distributed
Operations that would harm creditors (Article 2629 of the Civil Code)	consisting in the conduct of directors who, in breach of the law for the protection of creditors, carry out reductions of the company's share capital, mergers with other companies or demergers, thus damaging creditors
Fictitious capital formation (Article 2632 of the Civil Code)	consisting in the conduct of directors and contributing shareholders who, also in part, fictitiously form or increase the share capital, by the assignment of shares to an extent that is higher as a whole than the share capital amount, reciprocal subscription of shares or company stock, significant overvaluation of the contributions of assets in kind or receivables or the company assets in the event of transformation
Bribery between private individuals (Article 2635, paragraph 3, of the Civil Code)	consisting in the conduct of whomsoever offers, promises or gives money or other benefits not due to the directors, general managers, managers in charge of drawing up the company's financial reports, auditors and liquidators, to those who, within the company's organisational framework, exercise management functions other than those of the persons indicated, as well as to those who are subject to the management or supervision of said persons, in order for them to

	perform or omit acts in violation of the obligations inherent to their office or the obligations of loyalty
Incitement to bribery between private individuals (Article 2635-bis of the Civil Code)	consisting in the predicate conduct, if the offer or promise of undue money or other benefits is not accepted
Obstructing the operations of public supervisory authorities (Article 2638 of the Civil Code)	consisting in the conduct of directors, general managers, managers responsible for preparing the company's accounting documents, statutory auditors and liquidators of companies or entities and other persons subject to public supervisory authorities by law, or required to meet obligations towards them which, in communications to the aforementioned authorities required by law, in order to hinder the exercise of supervisory functions, expose material facts that do not correspond to the truth, even though they are subject to assessments, on the economic and financial situation of those subject to oversight, or for the same purpose, they conceal by other fraudulent means, in whole or in part, facts which they should have communicated, concerning the same situation, even if the information concerns assets owned or managed by the company on behalf of third parties; or by the fact committed by the directors, general managers, statutory auditors and liquidators of companies, or bodies and other persons subject by law to public supervisory authorities or under obligations towards them, which, in any case, deliberately hinder

their functions, also by omitting communications to the said authorities

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

15.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activities in reference to corporate crimes:

- Managing relations with partners;
- preparation of the financial statements and communications to the Shareholder or the public relating to the economic, equity or financial situation of the Company;
- transactions relating to share capital: management of contributions, corporate assets, profits and reserves, transactions on equity investments and capital;
- Litigation management (e.g. civil and labour law);
- execution of service contracts;
- Procurement of goods, services and consultancies including managing subcontracts;
- Management of monetary and financial flows - payments;
- Managing outgoing invoices and credit;
- Managing infra-group relations (e.g. sale of goods/services);
- Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.
- Managing expense sheets and relative reimbursements

15.3. Control devices

The current control devices for each sensitive activity are given below:

Managing relations with partners;

- Powers for managing the sensitive activity in question are conferred on the CEO, who has support from the ZTE Italia Finance Manager regarding matters of accounting;
- Traceability of activities that can be traced back to the process in question is guaranteed by the documents requested and produced for the partner and from relative reports;
- The transmission of data and information, as well as any communication or evaluation expressed by the Shareholder or sole Auditor, are always documented and archived by the competent department.

Preparation of the financial statements and communications to the Shareholder or the public relating to the economic, equity or financial situation of the Company

- The various subjects involved in the various phases of the sensitive activity in question are clearly identified. In particular:
  - a dedicated ZTE Corporation team creates the verification balance sheet in the ERP system;
  - The ZTE Italia Finance Manager, with support from a consultant, draws up the verification balance sheet again;
  - The consultant deposits the balance sheet;
  - The ZTE Italia HR Manager fills the role of company secretarial office, summons in the name of the Chairman of the Board of Directors and the Shareholders' Assembly and draws up the reports;

- The balance sheet drafts and other accounts documents are made available to the directors in advance of the meeting with the Board of Directors, called to decide on approving the balance sheet;
- The sensitive activity in question is regulated by a procedure that governs activities in the Administration and Finance area, which defines the rules of conduct, the roles and responsibilities, information flows between ZTE Corporation, ZTE Italia and the company, operational modes, traceability and document archiving in reference to managing completion of accounts and drawing up the balance sheet.

Operations regarding share capital: conferring amounts, corporate assets, profits and reserve funds, operations on shareholdings and on capital

- Decisions regarding operations on share capital are made, after decision on the company's ownership formation, during the Board of Directors meeting and Shareholders' Assembly based on the company articles of association and current civil law;
- The document is kept by the departments involved in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls.

Management of disputes (e.g. Civil and labour)

Managing outgoing invoices and credit

Managing expense sheets and relative reimbursements

The control devices are the same as the ones in section 11.3 of the herein Special Part and the corresponding sensitive activities.

Execution of service contracts.

The control devices are the same as the ones in section 14.3 of the herein Special Part and the corresponding sensitive activity.

Procurement of goods, services and consultancies including managing subcontracts **Management of monetary and financial flows - payments** **Managing infra-group relations (e.g. sale of goods/services)** **Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.**
The control devices are the same as the ones in section 11.3 and 13.3 of the herein Special Part and the corresponding sensitive activities.

16. Crimes against the individual

16.1. Applicable crimes

Consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following crimes against the individual as relevant:

Illegal intermediation and exploitation of labour (art. 603-Bis Criminal Code)	For each worker recruited it punishes anyone who: 1) recruited labour with the purpose of sending them to work with other third parties in conditions of exploitation, taking advantage of the workers' state of need; 2) Uses, hires or employs labour, also via afore-mentioned brokers, that subjects workers to conditions of exploitation and takes advantage of their state of need. The existence of one or more of the following conditions is considered to be an indicator of exploitation: 1) the repeated payment of wages in a way that is manifestly different from the national or territorial collective agreements concluded by the most representative trade unions at national level, or in any case disproportionate to the quantity and quality of the work performed; 2) repeated infringement of the legislation on working time, rest periods, weekly rest periods, compulsory leave and holidays;

3) the existence of violations of occupational health and safety rules;

4) subjecting the worker to working conditions, surveillance methods or degrading housing conditions

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

16.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activities in reference to crimes against the individual:

- Procurement of goods, services and consultancies including managing subcontracts;
- Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.

16.3. Control devices

The current control devices for each sensitive activity are given below:

Procurement of goods, services and consultancies including managing subcontracts

The control devices are the same as the ones in section 11.3, 13.3 and 15.3 of the herein Special Part and the corresponding sensitive activity. Also:

- the selection phase of Suppliers and Contractors is based on transparency criteria, paying the utmost attention to information regarding third parties with whom the Company has contractual relations that may even only give rise to the suspicion of the commission of the offence referred to in this Special Section;

- in the case of the signing of contracts and subcontracting contracts, it is verified that the counterpart's legal requisites of regularity are met, through the delivery and/or acquisition of the documentation required by law (e.g. single document for the regularity of contributions - DURC);
- contracts with Suppliers and Contractors include the Contractor's express obligation, as well as any subcontractors, to comply with:
    - national or territorial collective agreements concluded by the most representative trade unions at national level, or collective agreements of any applicable level;
    - legislation on working time, rest periods, weekly rest periods, compulsory leave and holidays;
    - occupational health and safety rules;
- agreements with Suppliers, Contractors and any subcontractors provide for the commitment of such parties to guarantee the existence of the conditions of legality for the stipulation of employment contracts with employees and the right of the Company to request further documentation or to carry out other checks aimed at ascertaining compliance by the Supplier, Contractor and any subcontractor with the regulations indicated in the previous paragraph;
- Correspondence between the names of the workers employed declared by contractors and subcontractors and the workers actually present in the places where they carry out activities on behalf of the Company is verified.

Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.

The control devices are the same as the ones in section 11.3, 13.3 and 15.3 of the herein Special Part and the corresponding sensitive activity. Also:

- If employees are hired or administered staff or seconded staff are used, the HR department checks that labour laws and trade union agreements are respected for the hiring and employment contract in general;
- If staff are hired via an administration agency, the HR department checks that the agency has the authorisation to carry out activities foreseen in the reference legislation;
- The HR department also checks the correct classification of staff in light of relative collective contracts, and based on the badge system and with the aid of specific software, working hours, rest periods and staff holidays;
- The document is kept by the HR department in a specific archive, in such ways as to prevent subsequent amendment, in order to allow correct traceability of the entire process and to aid any further controls.

17. Manslaughter or serious or extremely serious injury, committed by violating the laws on health and safety in the workplace

17.1. Applicable crimes

Considering the structure and activities carried out by the Company, through its control and risk self assessment activities, the Company has identified the crimes of manslaughter and serious or very serious culpable personal injury committed in violation of the regulations on health and safety at work as relevant:

manslaughter or serious or extremely serious injury, committed by violating the laws on health and safety in the workplace (art. 589 Criminal Code);	Punishes whomsoever causes the death of a person by fault with violation of the regulations for the prevention of accidents at work.
Personal injury through negligence (committed by violating the laws on health and safety in the workplace (art. 590 Criminal Code);	Punishes whomsoever culpably causes personal injury to others with violation of the rules for the prevention of accidents at work. In order for the personal injury to be criminally relevant, it must result in illness in the body or mind; the injury is: ➢ serious, if (alternatively) the result is an illness that endangers the life of the injured person, an illness or an inability to carry out ordinary tasks for more than forty days, the permanent weakening of a sense or organ; ➢ Very serious, if (alternatively) the result is an illness that is certainly or probably incurable, the loss of sense, the loss of a limb, a mutilation that renders the limb useless, the loss of the use

of an organ or the ability to procreate, a permanent and serious difficulty of speech, the deformation or scarring of the face.

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

17.2. Sensitive activities; provision by article 30, Legislative Decree no. 81, 9 April 2008

With reference to offences relating to health and safety at work, the Model sets out a different and additional control system from that provided for by accident prevention legislation, and differs from a mere risk assessment.

The Model's objectives are to control the operating system, in order to ensure its continuous verification and effectiveness, and the Model itself is addressed both to persons exposed to the danger of injury and to those who, throughout the corporate structure, are exposed to the risk of committing culpable crimes, so as to allow the latter to adopt predetermined operational and decision-making standards to avoid death and injuries.

The Model therefore constitutes a second-level control system, which regulates the way in which the safety system must be implemented and controlled and is aimed at avoiding accidents (function already performed by the safety management system), as well as that persons with management responsibilities are subject to offences (in point, see Court of Trani-Molfetta, 11 January 2010).

The Model, therefore, regulates activities at risk of offence, other than those at risk of accident (identified by the Risk Assessment Document and regulated by the safety management system). These activities are identified based on the above and on the contents of article 30, Leg. Decree 81/2008, which lists the realms in which the Model must govern legal obligations.

The sensitive activities relating to manslaughter or serious or extremely serious injury, committed by violating the laws on health and safety in the workplace are as follows:

- Identification of the employer and proxies; appointments and attribution of roles and responsibilities;

- Legislative update
- evaluation of risks and preparation of consequent measures;
- Organisational activity, such as emergency, first aid, tenders, periodic meetings;
- Healthcare supervision;
- Information and training
- acquisition of documents and certificates;
- Supervision, control and verification.

17.3. Control devices

The current control devices for each sensitive activity are given below:

Identification of the employer and proxies; appointments and attribution of roles and responsibilities

- The persons referred to in the legislation on health and safety at work are identified and appointed, and they are given the powers - possibly including those of expenditure - necessary to carry out the role;
- The employer has delegated part of his own duties pursuant to article 16 Legislative Decree 81/2008;
- the persons referred to in the previous point possess adequate and effective skills in this field, as well as any technical and professional requirements provided for by law;
- The appointment or, in any case, the attribution of responsibility takes place on a certain date, in writing.

Legislative update

- Compliance with the relevant regulations (laws, technical standards and regulations, etc.) is ensured by means of:
    - regulatory updating, carried out by the Prevention and Protection Service Manager, who indicates the need to comply with applicable regulations;
    - Periodic monitoring of compliance with the applicable legislation.

evaluation of risks and preparation of consequent measures

- The Employer is supported by the Prevention and Protection Service and other actors of the safety management system;
- the risk assessment is contained in a Risk Assessment Document (DVR), specific to all Company premises, drawn up on the basis of a document produced by ZTE Corporation and adapted to Italian legislation;
- the DVR has attachments relating to ZTE Servizi's offices and external activities (commissioning);
- the Rome site of ZTE Italia, where ZTE Servizi is also located, is certified according to the OHSAS 18001 standard;
- the identification of the measures resulting from the risk assessment is carried out on the basis of pre-defined criteria and considers the following aspects:
    - *routine* and *non-routine activities*;
    - activities of all persons having access to the workplace (including external actors);
    - Human conduct;
    - external hazards;
    - hazards associated with operations or created in the surrounding environment;

- infrastructure, equipment and materials at the workplace;
- changes made to processes and/or the management system, including temporary changes, and their impact on operations, processes and activities;
- any applicable legal requirements for risk assessment and implementation of the necessary control measures;
- design of work environments;
- identification of the activities for which provision should be made for the use of personal protective equipment;
- definition of criteria for the selection of personal protective equipment;
- The procedures for delivery of personal protective equipment.

Organisational activities, such as emergencies, first aid, tenders, periodic meetings

- situations that may cause a potential emergency are identified;
- emergency management modes are defined;
- activities to verify the effectiveness of emergency management and emergency simulations are planned and recorded;
- emergency procedures are updated in the event of accidents or negative results of checks or simulations;
- the persons in charge are formally identified;
- emergency and first-aid team personnel are identified, appointed and trained in accordance with the law;
- activities at the Rome site are coordinated with ZTE Italia workers;
- exercises are carried out and recorded;

- Periodic meetings are held to a schedule;
- the technical and professional requirements of contractors are checked (through verification of registration with the Chamber of Commerce and compliance with insurance and social security obligations);
- interference risk assessment is carried out and formalised in the Single Interference Risk Assessment Document (DUVRI);
- The company also draws up the DUVRI prepared by the customer to whom its employees are assigned (commissioning staff);
- in the case of activities carried out on construction sites, the Safety and Coordination Plan (PSC) prepared by the client is sent to ZTE Italia, forwarded to ZTE Servizi and then onto subcontractors by the latter;
- The s*ubcontractors* send the Operational Safety Plans (POS) to ZTE Servizi, which in turn forwards them to ZTE Italia; the latter – together with its own - are sent by ZTE Italia to the commissioning client.

Healthcare supervision

- the Company's Occupational Physician is responsible for verifying the suitability of workers for the tasks to be assigned;
- the Occupational Physician sets out the health surveillance protocol to be submitted to workers and implements health surveillance based on a schedule;
- The documentation on health surveillance is filed with the HR function.

Information and training

- All personnel receive appropriate information about the proper manner of performing their duties, are trained and, in the cases provided for by law, are trained;
- training is provided based on a schedule;
- training is differentiated according to the level and task of the workers, as well as documented and traced;
- The training documentation is archived by the HR function.

acquisition of documents and certificates;

- The certifications are provided to ZTE Servizi by the owners of the properties where the Company has its offices, and are verified based on a schedule.

Supervision, control and verification.

- specific audit activities are planned and conducted based on a specific schedule by the Prevention and Protection Service Manager and the H&S Manager, also with the collaboration of competent corporate persons or external consultants;
- the audits conducted by the H&S Manager are also carried out on the work of the Prevention and Protection Service Manager;
- Audits are also carried out in relation to the work of subcontractors.

18. Handling, laundering and use of money, assets or profits of illegal origin, in addition to self-laundering

18.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via control and risk self assessment, the company had identified the following crimes of handling, laundering and use of money, assets or profits of illegal origin, as well as self-laundering to be relevant:

Handling (art. 648 Criminal Code)	consisting in the conduct of whomsoever, apart from participation in the offence, acquires, receives or conceals money or goods which are the proceeds of a criminal offence, or assists in acquiring, receiving or concealing such money or goods, with a view to gain for himself or another
Laundering (art. 648-*bis Criminal Code*)	consisting in the conduct of whomsoever, apart from participation in the offence, substitutes or transfers money, goods or assets obtained by means of intentional criminal offences, or seeks by any other means to conceal the fact that the said money, goods or assets are the proceeds of such offences
Using money, assets or benefits of illegal origin (Article 648 of the Criminal Code)	consisting in the conduct of whomsoever, apart from participation in the offence and from the cases as per articles 648 and 648bis, uses money, goods or assets obtained by means of a criminal offence for economic or financial activities
Self-Laundering (art. 648-*ter Criminal Code*)	consisting in the conduct of whomsoever, having committed or helped perpetrate a crime committed with criminal intent, uses, replaces, or transfers the

money, assets or other assets derived from the commission of said offence into economic, financial, entrepreneurial or speculative assets in order to actually prevent identification of the criminal origin

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree* 231/2001".

18.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via control and risk self assessment, the company had identified the following sensitive activities of handling, laundering and use of money, assets or profits of illegal origin, as well as self-laundering to be relevant:

- Drawing up of balance sheet and communications to the partner or public regarding economic, assets or financial situation of the company
- Operations regarding share capital: conferring amounts, corporate assets, profits and reserve funds, operations on shareholdings and on capital
- Procurement of goods, services and consultancies including managing subcontracts;
- Management of monetary and financial flows - payments;
- Managing outgoing invoices and credit;
- Managing infra-group relations (e.g. sale of goods/services);
- Managing fiscal matters;
- Managing expense sheets and relative reimbursements

18.3. Control devices

The current control devices for each sensitive activity are given below:

Drawing up of balance sheet and communications to the partner or public regarding economic, assets or financial situation of the company

Operations regarding share capital: conferring amounts, corporate assets, profits and reserve funds, operations on shareholdings and on capital

The control devices are the same as the ones in section 15.3 of the herein Special Part and the corresponding sensitive activities.

Procurement of goods, services and consultancies including managing subcontracts

The control devices are the same as the ones in section 11.3, 13.3, 15.3 and 16.3 of the herein Special Part and the corresponding sensitive activity. Also:

- error indicators are identified to determine any "at-risk" or "suspicious" transactions with counterparties based on:
  - subjective profile of the counterparty (e.g., existence of criminal records, questionable reputation, admissions or statements by the counterparty regarding its involvement in criminal activities);
  - conduct of the counterparty (e.g., ambiguous behaviour, lack of data required for the execution of transactions or reluctance to provide such data);
  - geographical location of the counterparty (e.g., off-shore transactions);
  - economic and financial profile of the transaction (e.g., unusual transactions by type, frequency, timing, amount, and geographical location);
  - Characteristics and purposes of the operation (e.g. use of strawmen, changes to standard contractual terms, purposes of operation).

Management of monetary and financial flows - payments

Managing infra-group relations (e.g. sale of goods/services)

The control devices are the same as the ones in section 11.3, 13.3 and 15.3 of the herein Special Part and the corresponding sensitive activities.

Managing outgoing invoices and credit

Managing expense sheets and relative reimbursements

The control devices are the same as the ones in section 11.3 and 15.3 of the herein Special Part and the corresponding sensitive activities.

Managing fiscal matters

The control devices are the same as the ones in section 13.3 of the herein Special Part and the corresponding sensitive activity. Also:

- All legislative and regulatory provisions, including regulations, governing compliance with fiscal requirements, also with reference to tax consolidation and transfer pricing rules, where applicable, as well as all circulars, instructions and resolutions issued by the competent public authorities (Agenzia delle Entrate, Ministry of Finance, etc.) are complied with;
- the deadlines relating to tax obligations are monitored;
- Relations with consultants involved in the at-risk activity in question are formalised by means of a contract, duly authorised and signed by persons with adequate powers on the basis of the proxies conferred by the Company.

19. Crimes relating to the violation of copyright

19.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following crimes on the matter of violation of copyright as relevant:

Art. 171-*bis*, |Law no. 633, 22 April 1941	consisting in conduct of whomsoever illegally duplicates, for profit, computer programmes or, for the same purpose, imports, distributes, sells, holds for commercial or entrepreneurial purposes or leases programmes contained in media not marked by the Italian Society of Authors and Publishers (SIAE); uses any means intended to permit or facilitate the arbitrary removal or circumvention of software protections; in order to make a profit, reproduces, transfers, distributes, communicates, presents or demonstrates publicly the contents of a database on media without SIAE mark, extracts or reuses the database, distributes, sells or leases a database
Art. 171 ter, Law 633/1941.	consisting in the conduct of whomsoever - among other things - illegally duplicates, reproduces, or distributes literary, dramatic, scientific or didactic, musical or dramatic-musical and multimedia works in the public domain.

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree 231/2001*".

19.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activity on the matter of violation of copyright as relevant:

- Managing information systems.

19.3. Control devices

The current control devices for the sensitive activity in question are given below:

Managing information systems.
The control devices are the same as the ones in section 12.3 of the herein Special Part and the corresponding sensitive activity. Also: ➢ Periodic checks are carried out on the software installed and on mass memories in the systems used, in order to check for the presence of non-licensed software.

20. Inducement not to make declarations or make untruthful declarations to the judicial authorities

20.1. Applicable crimes

The crime of inducement to not make declarations or make untruthful declarations to the judicial authorities is considered potentially applicable to the company:

Inducement not to make declarations or make untruthful declarations to the judicial authorities (art. 377-Bis Criminal Code)	consisting in the conduct of whomsoever, by violence or threats, or by offering or promising money or other advantage induces a person summoned to give a statement usable in criminal proceedings before the

judicial authority, not to give statement, when such a person has the right to remain silent, unless the act constitutes a more serious offence

20.2. Sensitive activities; control devices

The case referred to in article 377-bis of the Criminal Code is not related to specific business activities.

Therefore, with reference thereto, at-risk activities and corresponding controls to be implemented in the Procedures are not identifiable.

The prevention of this type of offence is therefore constituted by the principles contained in the Company's Code of Conduct, with particular reference to the principles relating to relations with judicial authorities.

21. Environmental crimes

21.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following environmental crimes as relevant:

Environmental pollution (art. 452-Bis*bis Criminal Code*)	consisting in conduct of whomsoever, in violation of law, causes a significant and measurable impairment or deterioration: 1) of water, air or extensive or significant portions of soil or subsoil; 2) of an ecosystem, biodiversity, including agricultural, flora or wildlife;
Culpable crimes against the environment (art. 452-*quinquies* Criminal Code)	consisting in conduct of whomsoever commits the crime of environmental pollution and the offence of intentional environmental disaster;
Organized activities for illegal waste trafficking (Article 452-quaterdecies of the Criminal Code)[2]	punishes whomsoever engages in the sale, receipt, transportation, export or import or otherwise abusive management of large quantities of waste through several operations and the establishment of continuous organisational means and activities;
Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006) 152/2006)	consisting in conduct of whomsoever carries out collection, transport, recovery, disposal, trade and

[2] The offence was introduced by Legislative Decree No. 21 of 1 March 2018 and replaces art. 260 of Legislative Decree No. 152/2006, which was abrogated. As specified, in fact, by Article 8 of the Legislative Decree of 1 March 2018, "*from the date of entry into force of this decree, references to the provisions repealed by Article 7, wherever present, shall be considered to refer to the corresponding provisions of the Criminal Code*".

	brokerage of waste without the required authorization, registration or communication;
Illegal waste trafficking (Article 259 of Legislative Decree 152/2006.	Consisting in conduct of whomsoever carries out the illegal trafficking of waste under the law.

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree 231/2001*".

21.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via *control and risk self assessment*, the company has identified the following sensitive activities in reference to environmental crimes:

- Managing environment-related obligations

21.3. Control devices

The current control devices for the sensitive activity in question are given below:

Managing environment-related obligations

- To manage waste, ZTE Servizi uses external suppliers, via ZTE Italia:
  - To dispose of packaging materials, it uses the CONI consortium:
  - To dispose of electronic or electrical equipment (EEE), batteries, pen drives, cell phones, routers, it uses the consortium ECORIT;
- Relations with suppliers are formalised in specific contracts duly signed by subjects with appropriate powers;

- Controls and audits are systematically carried out on the disposal companies that the company uses;
- with reference to dismantling activities, the Company uses subcontractors who undergo a qualification process based on the documentation proving the legal requirements; this documentation is archived;
- Contracts with subcontractors contain clauses in which they undertake to observe environmental legislation.

22. Employment of foreign citizens with no permits of stay

22.1. Applicable crimes

In consideration of the structure and activities carried out by the company, via control and risk self assessment, the company had identified the following crimes of employing citizens of other countries without a regular resident's permit to be relevant:

Employment of foreign citizens with no permits of stay (art. 22-Par.*par. 12-Bis, Leg. Decree no. 286 25 July 1998*);	consisting in conduct of whomsoever, acting as an employer, employs foreign workers who do not have the residence permit referred to in this Article, or whose permit has expired and for which renewal has not been requested within the period required by law, or has been revoked or cancelled, if the workers employed are (either): ➢ More than three in number; ➢ Minors not of a working age; ➢ Subjected to other working conditions of particular exploitation as stated in paragraph three of article 603-*bis* of the Criminal Code, i.e. Subjected to situations of serious danger, in reference to the work to be carried out and the conditions they work in

As an example of the possible ways of committing the crimes, please refer to the document "*Control & risk self assessment and Gap analysis ex Leg. Decree 231/2001*".

22.2. Sensitive Activities

In consideration of the structure and activities carried out by the company, via control and risk self assessment, the company had identified the following sensitive activities of employing citizens of other countries without a regular resident's permit to be relevant:

- Procurement of goods, services and consultancies including managing subcontracts
- Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.

22.3. Control devices

The current control devices for each sensitive activity are given below:

Procurement of goods, services and consultancies including managing subcontracts

The control devices are the same as the ones in section 11.3, 13.3, 15.3, 16.3 and 18.3 of the herein Special Part and the corresponding sensitive activity.

Selection, recruitment and management of staff, including administered staff, including management of bonus and reward system.

The control devices are the same as the ones in section 11.3, 13.3, 15.3 and 16.3 of the herein Special Part and the corresponding sensitive activity. Also:

- in the case of recruitment of third-country nationals already in possession of a residence permit, the existence and validity of the residence permit shall be verified, together with any further documentation needed to perfect their recruitment;
- in the case of recruitment of third-country nationals already in possession of a residence permit, the ZTE Italia HR Manager provides for:
    - the personal request for authorisation (authorisation of recruitment) to be submitted to the competent Prefecture office;
    - giving the authorization, once issued, to the person to be hired, so that s/he can request the competent offices for the issue of entry visa for reasons of employment and therefore, following entry into Italy, the residence permit;

- obtaining the residence permit or the copy of the application for a residence permit submitted to the post office and the receipt thereof and to file this documentation together with the employment contract;
- communications required by law to the Centre for Employment and other competent bodies, ensuring that the information transmitted is truthful, complete and based on appropriate documentation;

➢ The ZTE Italia HR Manager:

- monitors the expiry dates of residence permits and any renewals for third-country workers recruited;
- verifies, during the employment relationship, that the foreign worker has submitted an application for renewal of the residence permit (of which the worker must produce a copy of the receipt issued by the post office at which the application was made), close to the expiry of its validity and in any case not later than sixty days from it;

➢ employees hired by ZTE Servizi are required to undertake to transmit any communication, letter and request from the competent authorities and offices (Police Headquarters, Prefecture, Employment Centre) regarding the validity or expiry of the residence permit to the company;

➢ the at-risk activity in question is covered by the Procedures "Regulation on New Hire Selection and On-boarding" and "Regulation on Performance Evaluation" which govern, among other things, the management of formalities relating to the regularity of stay of non-EU personnel, with particular reference to personnel on secondment from China (with reference to the verification, renewal, application for a residence permit, visa and letters of invitation).