**CHAPTER III**

**MODEL OF CHEMI S.P.A.**

**SPECIAL PART**

## *13. Introduction*

According to Article 6 of the DECREE, the system of in-house controls should include, in relationship with the crimes to be prevented: *i)* specific protocols to plan the development and implementation of the COMPANY's decisions; *ii)* the detection of the management procedures for the financing sources suitable to prevent the commitment of crimes.

The procedures are continuously updated, also upon the proposal or reporting from the BODY..

The BODY verifies that each procedure is in compliance with the principles included in the MODEL.

The BODY proposes the changes and any integrations of the above mentioned prescriptions and implementation procedures.

The BODY contributes to define, along with the involved business functions, the *significant* operations to which the procedures inspired to the MODEL principles apply.

The value and economic extent of an operation related to the Company's activity in the involved compartment, its incidence on decision-making and manufacturing processes, its relevance in relation to the ordinary business activity are markers of *significance* of that operation.

In case of a special emergency or provisionally impossible compliance with the procedures, under the responsibility of the person who carries them out, some derogations to the present Special Part are allowed in the development or performance of decisions. In such a case, the BODY should be immediately informed and a subsequent confirmation by the treating subject is required.

### *14. Detection of risk areas and operations*

Within the scope of the Company's business operating the following *sensitive* activities are detected, basing on crime typology.

### *14. 1. Crimes against Public Administration* (Articles Nos. 24 and 25 of the DECREE)

According to Article 6 of the Decree, within the scope of the *activities* that:

- imply relationships with public officers, persons involved in public service, vigilance and control authorities, inspection bodies, public bodies dispensing contributions and subsidized loans, public institutions and subjects in charge of public service, holders of authorization, granting, qualification, certification or regulatory powers;

- imply the participation in public tenders or negotiations with public institutions concerning the awarding or renewing of works as a license or as a contract, with reference to selection procedures, sub-contract authorization, management of any litigations with the customer, control of the service compliance with the contents of contracts, specifications or disciplinary matters;

- imply the management of public funds, both in the step of acquisition and dispensation of funds, whatever they are called, destined to public purposes, and in the performance of functions in a license regimen, because ruled by public law standards and authority deeds;

the following *risk operations* are detected in the COMPANY, during whose performance or implementation the following crimes can be committed, according to Articles 24 and 25 of the DECREE:

- operations of negotiation, stipulation and performance of contracts or agreements with subjects qualified in public law by *negotiated procedures*;

- operations of negotiation, stipulation and performance of contracts or agreements with subjects qualified in public law by *public evidence procedures*;

- participations in *bids for tenders* or direct negotiation called by public national bodies, EC or foreign bodies or similar institutions carried out within a competitive international context;

- application for and achievement of *qualifications*, whatever they are called, for the practice of a public service or public need;

- generally, management of the relationships with subjects qualified in public law on occasion of the necessary procedures for the acquisition and renewal of *granting/authorizations* and *certifications* and *licenses*, whatever they are called, issued for the COMPANY's ordinary activities;

- activities carried out by the COMPANY as an officer of public service or public need and *relationships with the target recipients of the services*;

- *acquisition* of contributions, grants, financing, insurances and guarantees granted by Italian, EC, or foreign public bodies or subjects and *management* activity of the mentioned items, particularly if they are granted with guarantees for predetermined aims and purposes of use or for investments for manufacturing, environment, research and technological innovation;

- management of the relationships with subjects qualified in public law concerning *real estate rights* and *purchase and management of movables*;

- management activities concerning the relationships with subjects qualified in public law, with Authorities of Vigilance and Control in the fields of tax and accounting, corporate and financial matters, environment, social security, health, hygiene and safety and prevention of industrial accidents and welfare in general, immigration or expatriation of non-EU people, with a particular reference to the control activity carried out by them or

by structures acting on behalf of them, required or ruled by regulatory and legislative standards;

- management of the relationships with P.A. or with the managing authorities authorized to regulate markets and vigilance, also in case of inspections and verifications;
- hiring of staff included in the protected categories or whose hiring is facilitated or imposed as well as relationships with social security or welfare institutions;
- staff hiring operations, when the people to be selected or hired have recently had a direct or indirect relation with the State, Vigilance and Control authorities or P.A. - also foreign - or with European Union organizations, or when these operations are for their own nature in a direct or indirect relation with the mentioned institutions or organizations or when they concern the access to the use of social security cushions and national insurance contributions;
- hiring of outsourced consultants;
- relations with financial administration;
- relations with Public Security authorities;
- commercial promotions and sponsorships of events in which subjects qualified in public law participate;
- management of software owned or generated by subjects qualified in public law or supplied by third parties on behalf of subjects qualified in public law, as well as electronic connections or data transmission in electronic or telecommunications format to the Public Administration or to another Authority.

With a special reference to the business activity of CHEMI S.P.A., the following sensitive areas and operations have been detected:

- supply contracts and free negotiations in both a public and a private area
- direct sale to the chemists
- management and distribution of drug samples
- stipulation and performance of consulting agreements and co-operation with opinion leaders

- gifts, donations and other liberalities
- management of congresses, conventions, seminars and investigator meetings
- management of visits to business laboratories
- management of promotional means
- pre-clinical research activities
- management of clinical studies
- management of non-profit clinical studies
- negotiation of drug price and definition of the pharmacotherapeutic group
- applications for marketing authorization approval
- relations with P.A. concerning pharmacovigilance
- drug traceability
- request and management of public funding
- activities related to drug production
- management of problems concerning environment, health and safety
- management of relations with the privacy protection authority
- management of relations with financial administration
- management of customs duty compliance
- management of litigations
- management of social security and welfare compliance
- management of debt collection
- management of applications for authorizations, licenses and permits
- management of the relations with commercial partners
- scientific information activities
- gadget supply
- sales to wholesalers
- management of corporate affairs compliance
- management of the lists of expenses and representation expenses
- purchase of goods and services
- suppliers accounting
- accounting and balance
- accounting and customers
- treasury
- budget and management control
- staff selection

- staff administration
- staff training and incentives
- management of agents
- management of information systems
- management of storehouses and warehouses
- management of patents and trademarks

***14.2. Computer-related crimes (Article 24-bis of the DECREE)***

According to Article 6 of the DECREE, within the scope of the activities generally involving either the direct or indirect use of information technology systems at CHEMI S.P.A., the following risk operations are detected, during whose performance or implementation the following crimes can be committed, according to Article 24 – *bis* of the DECREE:

- management of user's profile and authentication process;
- management and protection of workstation;
- management of accesses to the outside;
- management of system output and storage devices;
- classification and handling of operations;
- identification of roles and procedures;
- protection of software, contents, web and transmissions;
- monitoring of processing operations;
- access control;
- safety of business continuity;
- policy of technical and legal compliance (copyright);

- web management and protection;
- working-out of general management plan and performance of specific activities of information safety management;
- relation with external parties through information technology systems;
- on-line transactions;
- physical safety (wiring safety, web safety devices);
- management of physical safety of premises, relevant information and equipment;
- classification and use of goods;
- reporting of safety-critical events;
- supply, development;
- maintenance of HW-SW products.

### 14.3. *Coinage offences* (Article 25-*bis* of the DECREE)

According to Article 6 of the DECREE, within the scope of the activities during whose performance some behaviors suitable to endanger the safety and reliability of the money transactions could occur, i.e. counterfeit, money falsification, acquisition or making available on the market of money counterfeited by third parties, the following risk operations are detected at the COMPANY:

- introduction into the Italian State of currency, Italian or foreign money, fiscal stamps;
- possession, management and use of currency, Italian or foreign money, fiscal stamps;
- availability of money funds or values.

**14.4.** ***Crimes against industry and commerce (Article 25-bis.1 of the DECREE)***

Complying with Article 6 of the DECREE, within the scope of the following activities:

- management of manufacturing and distribution process;
- management of the relations with customs officers for import/export operations concerning industrial products ;
- management of the relations with regulatory bodies and with "NAS Carabinieri" and State Police authorities in case of inspections concerning manufacturing process, release of batches on the market or problems about product traceability;
- use of substances or products submitted to specific regulations and management of the relevant compliance, controls and inspections by the vigilance authority;
- management of the relations with public subjects concerning acquisition of authorizations, licenses and grants for the practice of business activities and the running of manufacturing plants;
- management of the paperwork of homologation, certification and declaration of conformity from the relevant Bodies and Institutions, also on occasion of inspection visits;
- management of relations, compliances and communications with the Italian Medicines Agency and other regulatory bodies with reference to authorization and control processes for import and manufacturing of pharmacologically active substances, for the compliance with Good Manufacturing Practice, for product marketing authorizations;
- management of the requirements imposed by Pharmacovigilance system;

- running of national or international commercial development businesses which could imply interlocution flows with authorities or State Police;

- management of patents and trademarks;

- use of sources or information in electronic or telecommunications format or any other original work protected by copyright;

- management of agents and commercial partners

the following risk operations are detected in the COMPANY, during whose performance or implementation the following crimes can be committed, according to Article 25 *bis*.1 of the DECREE:

- manufacturing, use or marketing of products which could infringe industrial property rights or titles;

- direct relations with public officers that could possibly compile forms or impose sanctions as a consequence of the detections carried out;

- production of documentation and regular transmission of due information;

- completion of control log-books and guarantee of regular information flows to the vigilance authorities ;

- direct relations with public officers for the acquisition or the renewal of authorizations, licenses, permits, certifications, and/or grants also on occasion of inspection visits;

- preparation and submission of the documentation required for the acquisition of authorizations, licenses, permits, certifications, and/or grants;

- relations with regulatory bodies for the acquisition of authorizations for the manufacturing and import of pharmacologically active products, for the controls of the compliance with the Good Manufacturing Practice and for product marketing authorizations and for any other compliance with the regulatory activities, in the steps of preparation of the Drug Master File, advancement and conclusion of the authorization procedure for the consequential control activities;

- preparation and submission of the Drug Master Files and of the necessary documentation for the release of the authorizations to the regulatory bodies;

- management of the relations with the relevant regulatory authorities, within the scope of the operations of submission of information flows concerning the compliance with the Pharmacovigilance requirements or on occasion of controls and inspections carried out at the offices of the COMPANY;

- relations with public officers during meetings or institutional or commercial interlocutions or during the development of international plans which could involve interlocution flows with public authorities or administrations;

- direct relations with officials of public institutions in the steps of patent and trademark submission and management of the relevant granting/approval procedures;

- management of any information about the access to computer sources, databases and information technology and telecommunications system;

- management of the activities related to the purchase and use of software, databases or any other copyright-protected product;

- management of the activities related to the use of the company's network and to the access to *internet/intranet*.

**14.5. *Company crimes* (Article 25-*ter* of the DECREE) and *Market abuses* (Article 25-*sexies* of the DECREE)**

According to Article 6 of the DECREE, the following risk operations are detected in the COMPANY, during whose performance or implementation the following crimes can be committed, according to Article 25. *ter* of the DECREE:

- detection, registration and representation of the COMPANY'S activities, and its economic and financial situations, in accounting entries, balance sheets, reports and other Company's internal documents or documents destined to Italian, supranational or foreign Vigilance and Control authorities, to the market or to third parties in general, especially on occasion of extraordinary operations (mergers, splits, …);

- compilation of information documents, information sheets, reports, and releases of information under any form concerning the COMPANY, destined to Vigilance and Control authorities or to investors, journalists, other mass media representatives or the general public, by law or for the COMPANY's decision, also according to Article 114 of T.U.F., as well as formation of any privileged information according to Article 181 of T.U.F.;

- management of general relationships, but also organization of and participation in meetings, in whatever form they are held, with Italian and supranational Vigilance and Control authorities, State Administration officers , or with investors, security analysts, journalists and other mass media representatives;

- communication of information about the COMPANY to third parties and to the market, which have not been communicated to the public yet and intended to be divulged by law or CHEMI S.P.A.'s decision ;

- any operations related to the origin, development and internal or external communication of privileged information according to Article 181 of T.U.F.;

- management of activities established by the law in order to request for the investment or on occasion of the admission of the COMPANY to regulated markets or at the time of public offers of purchase or exchange;

- preparation of the general balance sheet, consolidated balance, reports and other communications established by the law and destined to the partners or to the public and relevant assessment of risk funds;

- relations and connections of whatever nature with the Board of Auditors, auditing companies and partners as well as every kind of co-operation with each of them;

- relations and connections with rating agencies, consultants in extraordinary operations and Italian or foreign financial intermediaries in general;

- documentation, filing and storage of information concerning the operations mentioned under the previous points;

- situations of conflict of interest of Administrators; General Managers, Managers in charge of the compilation of book-keeping documents or in charge of the reports of purchase or sale with third parties

- management of financial resources and guiding and coordinating activities of the accounting procedures in the COMPANY, as well as management of book-keeping and accounting data, of cost centers and submission of each of them to the dedicated function;

- management of the relevant budget of each function and transmission of accounting data;

- activities of the Board of Directors, in particular the ones involving decision-making process about political-financial matters;

- preparation of the General Meetings and management of meetings;

- profit sharing;

- credit securitization ;

- operations, concluded in whatever form, on joint stock capital, COMPANY 's own shares, or shareholdings in Italian and foreign controlling or controlled companies or others;

- purchase, sale or other operations, in whatever form they are concluded , whose purposes are other financial instruments according to Article 180 letters a) and b) of T.U.F. issued by CHEMI S.P.A., controlling, controlled, allied and affiliated companies;

- purchase, sale or other operations, in whatever form they are concluded , whose purposes are unquoted financial instruments or financial instruments for which a request for admission to trading in a regulated market has not been made, and stipulation of non-exchange traded derivatives on Italian and European regulated markets;

- purchase, sale or other operations, in whatever form they are concluded , whose purposes are financial instruments according to Article 180 letters a) and b) of T.U.F., others than the

ones of the previous points, admitted to trading or for which a request for admission to trading has been submitted, in a regulated market of an Italian or other EU country, as well as any other allowed instruments or for which a request for admission to trading has been submitted in a regulated market of a country of the European Union;

- communication of information to third parties or Italian, supranational or foreign Vigilance and Control authorities, concerning the COMPANY whose purposes are unquoted financial instruments or financial instruments for which a request for admission to trading in a regulated market has not been made;

**14.6. *Crimes of terrorism and subversion of democratic order* (Article 25-*quater* of the DECREE)**

According to Article 6 of the DECREE, within the scope of the activities involving the risk to establish relationships with counterparts, customers or subjects that are likely to carry out or facilitate - either directly or indirectly - operations of terrorism or subversion of the constitutional order, the following *risk operations* are detected in the COMPANY, during whose performance or implementation the following crimes can be committed:

- contractual relations with counterparts resident or operating in countries considered to be at risk;

- fulfillment and management of relief and solidarity initiatives, in particular in favor of institutions located or operating in Countries considered to be at risk.

**14.7. *Crimes against individual personality* (Article 25 – *quinquies* of the DECREE) *and employ of citizens of third countries whose stay is irregular* (article 25-*quinquies* and 25-*duodecies* of the DECREE)**

According to Article 6 of the DECREE, within the scope of the activities involving the risk to establish relationships with customers that are likely to carry out or facilitate - either directly or indirectly – initiatives aimed to people's exploitation or child pornography, providing financial sources or money availabilities which result to be instrumental to the pursuit of such illicit activities, the following *risk operations* are detected in the COMPANY, during whose performance or implementation the following crimes can be committed according to Article 25 - *quinquies* or Article 25-*duodecies* of the DECREE:

- contractual relations with counterparts resident or operating in Countries considered to be at risk or with counter-parts – in particular contractors – who employ in Italy citizens of third countries who require the permission to stay;

- management of information technology or telecommunications supports ;

- fulfillment and management of relief and solidarity initiatives, in particular in favor of institutions located or operating in Countries considered to be at risk;

- management of human resources.

**14.8.** ***Organized– also transnational – crimes and money laundering (Article 24 –*** **ter*****, Article 25 –*** **octies** ***of the Decree and Act No. 146 of March16, 2006)***

According to Article 6 of the DECREE with reference to the risk of establishing relationships with individuals or corporate bodies that are likely to pursuit, either directly or indirectly, illicit activities referred to in Article 25-*octies* of the DECREE and Act No. 146/06, the following scopes of activities are detected in the COMPANY, in which the relevant crimes could be carried out:

- investments, funding, intra-group financial operations and management activities concerning general capital flows;

- purchase and sale of business and business branches, establishment of temporary business groups and *joint ventures*;

- assessment, qualification and selection of suppliers of goods and services; assessment of customers and definition of credit limits; as well as management of economical and financial conditions in contracts with customers and suppliers (advances to suppliers, collection and payment terms), reminders of expired debts and debt-collecting activities;

- implementation and management of relief and solidarity initiatives, in particular in favor of institutions located or operating in Countries considered to be at risk;

- gifts to associations, local and governmental bodies (municipalities, universities, etc.) and sponsoring of sport events and associations;

- management of legal and out-of-court litigations and relations with subjects involved in legal proceedings or preventive measures;

- selection and management of non-EU staff and human resources;

- management of information technology and telecommunications supports;

- in general, any activity implying in theory a risk for:

    - carrying out behaviors suitable to integrate, also as a competitor or a facilitator, by means of financial operations, crimes of criminal, also mafia-style, conspiracy that is aimed to tobacco smuggling or traffic in narcotic drugs or psychotropic substances;

    - allowing or facilitating customers or counterparts, either directly or indirectly, in laundering of money, goods or other utilities or using them if they are from an illicit source;

    - possible, also indirect, contacts with criminal organized enterprises;

- carrying out behaviors of obstruction of justice;

- carrying out behaviors suitable to facilitate clandestine immigration phenomena, e.g. business activities involving the admission of non-EU subjects to the territory of a member state.

Within the scope of such activities, the following risk operations are detected in the COMPANY, during whose performance or implementation the following crimes can be committed, according to Act No. 146 of March 16, 2006, and Article 25 - *octies* of the DECREE:

- recourse to splitting techniques of operations or payments;

- operations involving high amounts of money, which are unusual versus those normally carried out by the customer;

- operations frequently carried out by a customer in favor or on behalf of third parties, whenever such relations do not seem justified;

- operations carried out by third parties on behalf or in favor of a customer without plausible justifications;

- request for operations with clearly incorrect or incomplete indications;

- operations with counterparts operating in geographical areas known as *off-shore* centers or as areas of traffic in narcotic drugs or tobacco smuggling, which are not justified by formally legitimate reasons ascribable to the customer's business activity or to other circumstances;

- request for exchange of banknotes with different-denomination banknotes or different currencies;

- operations whose object is the use of electronic money, which – for amount or frequency – do not result to be consistent with the customer's activity or the normal use of the instrument by the customers;

- use of credit letters and other systems of trade financing, howsoever they are called, to transfer money amounts from a country to another, being the relevant transaction not justified by the customer's normal business activity;

- trust registration of goods or financial tools, whenever they have been owned by the commercial partner for a short time and this does not seem in accordance with the customer's financial situation or the business performed.

### 14.9. *Workplace health and safety crimes* (Article 25-*septies of the* DECREE)

Within the scope of all the sectors of activities of the COMPANY and its manufacturing units in which internal employees, outsourced employees or self-employed people are working and to whom the COMPANY entrusts contract and sub-contract works, the analysis of the COMPANY'S business processes has allowed to detect the following sensitive activities with reference to the crimes established in Article 25-*septies* of the DECREE:

- *planning and management of prevention and protection service* of workers' health and safety ;

- *risk detection, assessment and mitigation:* in particular the *risk assessment* activity on a periodical basis in order to: i) detect the dangers and assess the risks concerning workers' workplace health and safety and during the performance of assigned tasks; ii) identify the existing measures of prevention and risk control and for workers' protection; iii) define the implementation plan of any new measures thought to be necessary;

- *organization of business structures* with reference to activities concerning workplace health and safety: in particular, work organization, definition of tasks, functions and responsibilities; analysis, planning and control; participation of internal and trade-union organizations; work

standards and procedures; maintenance and testing; safety equipment, management of emergencies and first-aid; management of health surveillance;

- system of *proxy of functions*;

- activities of *information*, in particular activities of an internal system of information spreading such to pay a necessary, consistent and effective attention to health and safety at each Company's level;

- activities of *training*, in particular implementation and development of training and awareness systematic plans, with the regular participation of all the employees, as well as updating courses for the subjects who carry out particular roles concerning health and safety requirements;

- *relations* with suppliers, designers, manufacturers, installers, subjects involved in procurement, works and supply contracts or relations with suppliers involved in the management of workplace health and safety;

- *management of business assets concerning maintenance and preservation of movables and immovables*;

- activities of systemic and continuous *monitoring* of data and markers representing the main characteristics of the different activities and implementation of any *corrective actions*;

- management of *control mechanisms* (*audits*, inspections, etc.) in order to verify:

- the correct application of applied politics, programs and procedures;
- the clear definition, understanding, sharing and efficiency of organizational responsibilities;
- the compliance of products and industrial activities with law, regulations and internal standards;
- the detection of any deviation and the timely implementation of the relevant corrective actions;
- the detection and control of each cognizable risk situation;
- the granting of continuity of the compliance of plants, goods, and equipment over time;
- control of the impact on staff's health generated by the site industrial activity and proper monitoring and recording of effects.

**14.10.*Crimes of copyright infringement rights (Article 25 -* novies *of the DECREE)***

According to Article 6 of the DECREE, the following *risk operations* are detected in the COMPANY, during whose performance or implementation the following crimes can be committed, referred to in Article 25. - *novies* of the DECREE:

- use of sources and information in electronic or telecommunications format or any other original work protected by copyright;
- management of any information about the access to computer sources, databases and information technology and telecommunications system ;
- management of the activities related to the purchase and use of *information technology*, databases or any other copyright-protected product;

- management of the activities related to the use of the company network and to the access to *internet/intranet*.

- use and divulgation of information materials concerning scientific research or with copyright-protected contents.

**14.11.** ***Environmental crimes (Article 25-undecies of the DECREE)***

According to Article 6 of the DECREE, the following *risk operations* are detected in the COMPANY, during whose performance or implementation the following crimes can be committed, referred to in Article 25 - *undecies* of the DECREE:

- in case of use of substances or products subjected to specific regulations, the management of the relevant compliances with the statutory provisions in force;

- relations with public bodies in case of controls, inspections and concerning the relevant compliances:

- management of products, compilation of control log-books and information flows to the vigilance authorities;

- management of the relations with public subjects concerning the acquisition or renewal of authorizations, licenses, certifications, permits and/or grants for the practice of business activities and the running of manufacturing plants/management of the paperwork of homologation, certification and declaration of conformity from the relevant Bodies and Institutions, also on occasion of inspection visits;

- preparation and submission of the necessary documentation for the issue of authorizations, licenses, permits, certifications and/or grants;

- management of compliances, controls and inspections in case of use of harmful substances, production and disposal of solid or liquid wastes, discharge into waters and atmospheric emission, of provisions of the Decree of Law no. 334/99 and subsequent amendments concerning the risk control of significant accidents and the requirements established for AIA;

- relation with public bodies in case of controls, inspections and concerning the requirements related to waste disposal and environmental management;

- preparation and submission to the relevant bodies of the documentation concerning the compliances about waste disposal, emissions and sewage control and any other environment-related compliance.

## *15. Crime prevention procedures*

### *15.1. General principles*

The following general principles are the base of the procedures which should imperatively be observed by the corporate bodies of CHEMI S.P.A., managers and employees, as well as, under appropriate contractual terms, by Co-operators, Agents, Consultants and other counterparts.

In general, the COMPANY'S organization system should be inspired to the compliance with laws and regulations and to the integrity of corporate assets.

It should be founded on the basic requirements of clear formal and cognizable description and detection of tasks and powers assigned to each individual function, to the different qualifications and professional roles; on the precise description of the reporting lines; on the traceability of each significant decision-making and operative step.

In particular:

- the responsibilities of the management (and the relevant operative procedures) of a business transaction or process should be clearly defined and known within the COMPANY;
- there should be a clear identification and a COMPANY'S specific assignment of powers and limits to the subjects who operate involving the COMPANY and expressing its will;
- powers of organization and endorsement (delegations, authorizations, and relevant spending limits) should be consistent with the assigned organizational responsibilities;

- within each significant business process, the functions should be separated and different subjects should be detected for decision-making, implementation, recording or control of a transaction.

Basically, task separation should be granted through a correct distribution of responsibilities and the expectation of proper authorization levels in order to avoid the overlapping of functions or task allocations concentrating the critical activities on one subject. Moreover, a clear and formalized assignment of powers and responsibilities should be pursued and formalized with a clear definition of the operating limits and consistent with the assigned tasks and the positions occupied within the organizational structure.

In addition:

- the significant documents should be properly formalized and should include the date of the document compilation and control as well as the recognizable signature of the compiler/supervisor; the same documents should be stored in suitable places in order to protect the confidentiality of the included data and to avoid damages, deterioration and loss. The same applies to documents in electronic format;

- any sensitive and/or significant operations should be consistently and congruently documented so that at any time it could be possible to identify the responsibilities of the persons who have operated, assessed, decided, authorized, carried out, recorded and controlled the transaction;

- the controls actually carried out should be precisely documented, so that it could be possible to identify by whom and when they have been carried out, and their outcome;

- periodical summary *reports* should be prepared by the persons responsible for the business processes, summarizing the significant aspects of the activity performed, also through performance indicators which allow to timely detect any anomalies or atypical signs;

- safety mechanisms should be arranged granting a proper protection/physical and logistical access to the Company's goods and data.

*More specifically, in order to anticipate the commitment of CRIMES within the scope of the above mentioned risk areas, activities and operations, the COMPANY develops and adopts procedures that must comply in any case with the following general principles:*

***15.2. Top managers' decisions and conflicts of interest***

The training of administrators and the implementation of their decisions are ruled by the principles and requirements included in the existing legal provisions, in the certificate of incorporation, in the Statute, in the ETHICAL CODE, in the MODEL, in the in-house control system;

the administrators are obliged to timely communicate to the Board of Directors, the Board of Statutory Audits and the BODY - which files and updates – all the information about the appointments filled or the shares that they held – either directly or indirectly – in other Companies or enterprises, as well as their terminations or changes, which for their nature or typology could reasonably let foresee the arising of conflicts of interest according to Article 2391 of the Italian Civil Code;

there is the same obligation of communication mentioned under the previous point by the top managers, who will have to inform the Managing Director and the BODY*;*

there is the same obligation of communication for the members of CHEMI S.P.A. appointed in the corporate bodies of foreign subsidiaries with reference to the existence of ties of consanguinity or affinity with members of the local Public Administration and/or suppliers, customers or third party contractors of the COMPANY itself;

***15.3. Communications with the outside of the COMPANY and relations with Vigilance and Control Public Authorities***

The communications established by the law and regulations to Italian, supranational or foreign Vigilance or Control Authorities or Bodies, to the market or to the partners are timely and correctly submitted, in a truthful and complete way;

complete and immediate cooperation is given to Vigilance and Control Authorities or Bodies, timely and exhaustively supplying the required documentation and information;

the correspondence maintained with the Vigilance Authorities is formally registered; its filing is passed on – according to the subject matter – to the INTERNAL AUDITING or to another concerned function identified;

a specific person is identified - according to the subject matter – responsible for the relations with the Vigilance Authorities, having the task of formalizing in a specific *memorandum* the contents and outcome of the meeting with the Vigilance Authorities after their inspection;

***15.4. Formalization and separation of the steps: traceability of operations***

It should be possible to reconstruct the formation of the deeds and relevant authorization levels, the development of material and recording operations with a stress on their reason and purpose to grant the transparency of the choices taken;

no subjective identity should exist between the subjects who take and implement the decisions, the ones who get accounting evidence of the established operations and the ones having the task of carrying out the controls on those operations in compliance with the law and procedures established by the internal control system;

a person responsible for the operations should be identified (Responsible for the procedure and its implementation); otherwise mentioned in a different and exceptional way, he/she is the responsible for the function concerning the management of the considered transaction;

the person responsible for the procedure can request for information and elucidations to all the functional divisions, operative units, if endowed with autonomy, or to the individual subjects presently or previously involved in that transaction;

the person responsible for the procedure should inform the BODY on a periodical basis about all the significant operations falling within the range of sensitive activities, supplying the necessary information to assess the transaction risks and its critical sides under his/her own responsibility;

the functional division or the organizational unit, whenever information are requested about the concerned subjects, should supply the documentation suitable to answer the question, certifying the source and, when possible, the completeness and truthfulness of such information, or indicating the subjects who could supply that certification;

***15.5. Traceability of operations and information technology system***

The use of technology information systems is established, in order to grant the correct and true ascription of each transaction or of one of its segments to the responsible, the participating subjects and the involved customer, counterpart or bodies;

the system should include the impossibility of changing the recording without evidence;

any access to the company network – both *intranet* and *internet* – to carry out the operations or to document such operations should occur at least by using a double asymmetrical key (*user* ID and personal *password*), to be changed on a periodical basis, or other equally effective measure, which allows the operator to connect to the network within the limit of the procedure step of his/her competence and to leave unchangeable evidence of the intervention carried out and of its author;

***15.6. Document filing and storage***

The documents concerning the activity of CHEMI S.P.A., and in particular the documents or the computer documentation concerning the management of money and values, are filed and stored by the concerned function in such a way that it cannot be possible to allow a subsequent change unless evidence exists;

a specific procedure is established identifying the roles and responsibilities for the transcription, traceability and filing of the business documentation and the statutory books about health and safety;

whenever the document filing and storage service is carried out – on behalf of CHEMI S.P.A. – by an outsourced subject, the service is regulated by a contract according to which, among the other things, the subject serving the COMPANY should comply with specific control procedures suitable to prevent a subsequent document change, unless evidence exists;

the access to already filed documents should always be motivated and allowed only to authorized persons according to internal standards or to a delegated person, to the Board of Statutory Auditors or equivalent body or other bodies of internal control, to the auditing company possibly appointed and to the BODY;

***15.7. Access and use of the information technology system***

Directions for use of the information technology system are established based on a proper confirmation of the *passwords* for the authorization to the access to P.A. information systems possibly owned by some employees pertaining to specific functions or business structures;

information technology tools are arranged so to avoid the access and/or the receipt of materials concerning child pornography and to limit in general the access to internet sites with a crime risk potential;

the scope of a correct and allowed use - that is for the Company's purposes – of the information technology tools available to the employees is clearly established and communicated to all the employees and persons who can access the system;

a personal implementation of software on each employee's *personal computer* should not be possible, save through an intervention of information technology engineers;

### *15.8. Personal data processing*

The access to personal data in possession of CHEMI S.P.A. and their processing should comply with the Decree of Law No.196 of 2003 and following amendments and integrations - also statutory;

the access and treatment of data should be exclusively allowed to authorized persons and confidentiality should be granted when submitting information;

### *15.9. System of proxies and powers of attorney*

Powers of attorney should be consistent with internal proxies;

mechanisms of proxy advertising are established towards external interlocutors;

a procedure is established for the assignment of proxies which, among the other things, will establish:

- the requirements and professional skills that the appointed person should have for the specific area of his proxy;
- the formalization of function proxies with specification of the proxy-related functions;
- the explicit acceptance of the proxy-related functions and following assumption of the relevant obligations from the appointed or sub-appointed person;
- the surveillance of the consistency of proxies and sub-proxies with risk activity areas and on the existence and maintenance of requirements/skills in the appointed person;
- the assessment of technical and professional skills on a periodical basis as well as a verbalization of the controls about that person's suitability;

- the management of expenditure commitments;

proxies are assigned according to the following principles:

- decision-making and financial autonomy of the appointed person;
- adequate technical and professional skills of the appointed person;
- autonomous availability of sources suitable to the task and performance continuity;

the proxy appointed person should have:

- decision-making powers consistent with the formally assigned proxies; a *budget* for the effective compliance with the proxy-related functions with the availability of extra-budget sources in exceptional cases or situations;
- obligation of formalized reporting, with established procedures, about the proxy-related functions, sufficient to grant a vigilance activity without interferences;

***15. 10. Selection of employees, agents, consultants and cooperators***

The choice of EMPLOYEES, CONSULTANTS and COOPERATORS is carried out by and upon indication of the COMPANY' s Function Responsibles in compliance with the general standards formulated by the COMPANY basing on specific professional skills according to the assignment or tasks, equality of treatment, independence, skillfulness and, according to these criteria, the choice should be explained;

the candidates' selection process should include at least two interviews:

- the former is carried out by external consultants or by the Function of Human Resources with the aim of selecting a shortlist of candidates;
- the latter is a technical interview and is carried out by the responsible of the Function interested in the recruitment or by the A.D.;

after the interview, the interviewer will fill-up an interview form summarizing the candidate's features;

the skills claimed by the candidate should be verified by third-party sources; the profile of the typical candidate to be selected should be defined in a written form before starting the interviews;

the hirings should be performed with a regular work contract in compliance with all the current regulations and the collective contractual agreements favoring the inclusion of the worker into the workplace. In particular, the competent functions of the Company should check the possession by the subject with whom the working relationship should be established, of all the pre-requisites required by the law for the stay and performance of the working activity required in the Italian territory. Similar checks should be performed before the conclusion of contracts of consultation, agency, forms of para-subordinate work or of contract, etc.

the procedures should be formalized at the time of recruitment: a documentation set should be prepared, including the information report about the so-called *privacy* and declaration of consent; a recent certificate of judicial record; a recent certificate of pending proceedings; a certificate stating the subject is not submitted to prevention proceedings;

***15.10.bis. Management of scientific consulting***

Top managers of different business areas should be involved, save the assignment of a decision-making role to pharmaceutical sales representatives, or anyway to sales-related functions;

a person responsible for the function requiring the scientific consulting will be identified, with the role of procedure coordinator. The Managing Director will have the control and authorization power on that procedure;

the specific skills resulting from the consultant's curriculum vitae should be closely connected with the task to be carried out and should be consistent with the suggested fees level;

specific rules should exist concerning the determination of consulting charges at a fair market value;

the negotiation should be assessed by a qualified business function, independent of the proposing division;

it is possible to exceed the limits of the list of charges in exceptional cases but with a written explanation and a higher authorization level than the standard one;

a turnover system is established to regulate the limits of maximum cumulative yearly charges paid to the same consultant and a maximum number of tasks, except exceptional and justified reasons;

the fees or the greatest part of the fees should be paid after the complete performance of the consulting services or after a positive assessment about the consulting output. The documentation of the performed service should be available before the payment;

payments to third parties other than the subject who performed the service or in Countries different from the consultant's residence should be prevented;

the consulting agreement should be made in a written form and it should necessarily include: defined topic, development procedures, maximum performance times, payment timetable, consultant's obligations of informing the Company or third parties;

***15.11. Staff training***

Effective procedures are established for the training and consistent updating of employees and cooperators about the rules and protections in force within the COMPANY's structure as a prevention of the crimes mentioned in the DECREE;

the training of all the Function Responsibles is carried out in order that everybody knows the basic notions of balance;

***15.11.bis. Staff training about workers' health and safety***

A document of in-house policy will be distributed among employees establishing the general addresses and purposes of the prevention and protection system aimed to pursuit a proper health and safety protection;

the preparation of a calendar is established, including a timetable of the periodical meetings of the officers involved in the control of health and safety issues;

a procedure is established aimed to rule roles, responsibilities and operative procedures concerning the spreading of periodical information and information in case of immediate and serious danger among workers;

a discipline is established concerning the information report to be supplied to the concerned physician about processes and relevant risks of manufacturing activity;

***15.12. System of wages and bonus***

Any bonus system for employees and cooperators should meet realistic purposes and be consistent with the task and the activity carried out and with the assigned responsibilities and the available operating structure;

no fees or commissions should be established or paid to consultants, cooperators, or subjects qualified in public law in a way non-congruent with the services rendered to the COMPANY and not compliant with the task assigned, to be assessed according to reasonable criteria and according to the market standards and conditions of the reference geographical area or established by the price lists;

direct or indirect organization of travels or periods of stay in foreign locations is assessed and regulated with a special attention and a special consideration to moral principles;

***15.13. Selection of suppliers, commercial counterparts and partner***s

The selection of suppliers of goods or services is made by the concerned function on the base of requirements of proficiency, reliability, cost-saving, equal treatment, transparency in the selection procedure;

the minimum requirements concerning the applicants are always defined, as well as the determination of offer assessment criteria before the reception of the offers;

a procedure about suppliers' qualification and certification is established, which considers the compliance of the supplied goods or services with the purchase specifications and the best available technologies concerning environment, health and safety protection;

the cost-saving principle should never prevail over the reliability criterion;

specific criteria are established about selection, stipulation and implementation of agreements or *joint ventures* with other enterprises to develop investments, with a special reference to economic fairness of joint venture investments;

a special attention is given in assessing any possible trade *partnerships* with companies operating in electronic communication sectors (with reference to the risk of the diffusion of child pornography materials) or tourism sector in risk geographical areas;

### *15.14. Regulation of relations with suppliers, consultants, contractual counterparts and partners*

Contracts with commercial counterparts, consultants and partners include a specific provision, according to which they state that:

- they are aware of the legislation mentioned in the DECREE and of the relevant implications for the COMPANY;
- they will comply with the DECREE;
- in case of companies, they have adopted the organizational **MODEL** established in the DECREE, a similar document or a proper control procedure system;

contracts with commercial counterparts, consultants and *partners* include a specific provision, regulating the consequences of their infringement of the provisions included in the DECREE (e.g. explicit termination provisions, penalties);

the compliance of suppliers with the work regulations in force is verified, paying a special attention to child labor and to the provisions about hygiene, health and safety;

the compliance of the partners with regulations about child and women labor protection, safety health and hygiene conditions; trade union rights or association and representation rights is required and verified;

### *15.15. Management of goods and service supply process*

No identity should exist between the subjects who require the service, the one who authorizes it and the one who pays for the service. Tasks, powers and responsibilities assigned to each person should be clearly formalized;

the precise identification of a function/unit responsible for the definition of specific techniques and offer assessment is carried out;

the appointment of a person responsible for the implementation of the contract ("contract manager") is established, pointing out ing the relevant tasks, powers and responsibilities;

the authorization from a top qualified manager different from the contract manager is established in case of substantial amendments/integrations and/or renewal of that contract;

suppliers and consultants are forbidden to transfer the right to carry out the service established in the contract to third parties or to collect the payment or to pass the payment order to third parties;

***15.16. Management of financial resources***

The limits are established for the autonomous use of financial resources, by fixing quantitative thresholds in compliance with managing skills and organizational responsibilities given to the individual subjects;

the suppliers' payment process should be formalized and based on the principle of *segregation of duties,* by which supplier's census, invoice counting and relevant payment have to be carried out by different subjects;

the purchase management should be centralized;

transactions implying the use of financial or economic resources (acquisition, management, transfer of money and securities) should have an explicit explanation and should be documented and recorded in compliance with the principles of proficiency and proper management/accounting. The decision-making process should be verifiable;

the use of financial resources should be justified by the applicant who will state their fairness;

in case of ordinary operations falling within the established quantitative threshold, the given explanation can be limited to the class or type of the expenses made for that transaction;

the limits mentioned under the previous point could be exceeded only in compliance with the existing authorization procedures and after a proper explanation. However, in case of transactions different from the ordinary ones or exceeding the established quantitative threshold, the explanation should be analytical;

formal and material sources of money and securities should be identifiable;

all the operations of acquisition, management of transfer of money or securities should be documented in each step by the concerned function with the possibility of tracing the physical subjects involved in the different steps;

any subject dealing money or securities of any nature on behalf of the COMPANY should precisely comply with internal procedures concerning detection or reporting of ascertained or suspected

forgeries and comply with the procedures of value control with the utmost care;

any person who ascertains or suspects a forgery or falsification of money or securities should immediately stop the transaction and block the money or securities and promptly inform the person responsible for the procedure and the BODY;

regular payments should be checked with reference to complete matching of recipients/people ordering payments and counterparts actually involved in the transaction;

the Accounting Department should check, at each purchase, the matching between contract/purchase order, invoice and transport document; should verify the actual delivery of the goods or services with the Function who placed the order and should record the transaction;

the employee should obtain the authorization from his/her head for the reimbursement of the expenses incurred in the workplace; such a reimbursement will be credited by bank transfer at the time of payment of salaries;

the type of expenses reimbursable from the COMPANY to the EMPLOYEES should be explicitly regulated;

formal and substantial controls of business flows should be carried out on a periodical basis concerning payment to third parties and payments of intra-group transactions. Such controls should view the registered office of the counterpart company, the credit institutions used (registered office of the banks involved in the transactions and institutions without physical settlement in any country) and any corporate veils and trust structures used for normal and extraordinary transactions;

### *15.17. Economic and financial relationships with the Public Administration or its members*

Contacts with members of P.A. should be specifically justified;

the BODY should be immediately informed in case of illicit or suspected proposals or requests from members of P.A. or subjects qualified in public law;

within the scope of the activities concerning the divulgation of information and promotional materials, professional updating and scientific cooperation, organization of congresses, conventions and scientific meetings, visits to business laboratories, a specific business function should be identified, autonomous and different from the functions of trade and marketing, who should necessarily give an assessment about the scientific contents of activities and transactions;

within the scope of the spread of low cost gadgets, a specific business function should be identified, autonomous and different from the functions of trade and marketing, who should necessarily give an assessment about the close connection of gadgets with the medical and pharmaceutical activity;

within the scope of management of any donations, research funding, scholarships payable from the COMPANY, a specific business function should be detected, autonomous and different from the functions of trade and marketing, who should necessarily give an assessment about the scientific contents of the activities and projects to be financed;

the selection of the beneficiaries of the initiatives mentioned under the previous points should be based on the alternation principle (where specific threshold limits are established) so to allow a wide diffusion of the COMPANY's initiatives through the widest range of operators and to avoid the crystallization of privileged relations and positions: an *ex post* control should be carried out on an annual basis about the actual application of the alternation principle;

### *15.18. Relations with financial intermediaries*

The COMPANY, in order to implement the decisions about the use of financial resources ad in

order to implement the transactions of acquisition, management or transfer of money or securities, should use financial intermediaries and intermediary banks subjected to transparency and fairness regulations in compliance with the European Union standards;

it is mandatory, within the scope of financial transaction management, to use exclusively financial operators equipped with manual and computer supports suitable to prevent either national or international money laundering phenomena;

the use of cash should be prohibited for any collection, payment and fund transfer transactions, direct use or other kind of use of available funds;

acceptance and performance of payment orders from unidentifiable subjects should be prohibited ;

the payment concerning goods or services purchased by the COMPANY should exclusively be made on the bank account headed to the supplier. In general, in no case payments should be made on numbered bank accounts;

the prohibition of making payments on bank accounts of banks belonging to or operating in the so called “tax heaven” countries or in favor of *off shore* companies should be established, except when a proper explanation is given about the specific legitimacy and fairness of those payments;

the payment should perfectly correspond to the amount mentioned in the contract;

the payment concerning goods or services purchased by the COMPANY should not be made in favor of a subject other than the contractual party or in a third country different from the ones of the

contracting parties or from the country of contract implementation, except when a proper explanation is given about the specific legitimacy and fairness of those payments;

***15.19. Knowledge of customers and detection of suspected operations***

A deeper understanding and updating of the counterpart should be carried out in order to assess consistency and compatibility of the required transaction with its economical and financial profile;

customers' commercial and professional credibility and reliability should always be checked, on the basis of some significant markers, i.e.: bankruptcy proceedings, acquirement of commercial information about company, members, administrators of specialized companies, involvement of politically exposed people *ex* Article 1 Technical Enclosure of the Decree of Law 231/07;

detection and immediate reporting should be made to the BODY about transactions thought to be suspected or anomalous for the counterpart, typology, subject matter, frequency or extent;

in case of anomalous profiles of any nature in financial relations with suppliers or customers, the relation is maintained upon explicit authorization by the Managing Director;

transactions should be evidenced and immediately reported if carried out by a subject in the name, on behalf, or in favor of third parties in the absence of family ties or commercial relationships suitable to explain them, that is as the transactions carried out by third parties in favor of counterparts, in the absence of explanatory reasons;

the elements to be considered when assessing a suspected transaction are the following ones:
- amount of the transaction
- modes of performance
- recipient of the transaction
- territorial location

the staff members in direct contact with the customers should report to the Responsible of the Function;

***15.20. Management of cash transactions carried out by customers***

The processing of cheques should be formalized through many control steps;

***15.21. Company's property transfer***

For sale and purchase transactions of companies or company branches, the source of assets transferred to the company or to the company's branch to be purchased should be previously checked, as well as identity, seat, legal status, antimafia certification of the seller;

***15.22. Management of business assets concerning workers' health and safety***

A procedure is prepared regulating the activities and reports of maintenance or inspection of business assets necessary to grant the compliance with the regulations about workplace hygiene and safety;

***15.23. Detection, recording and accounting of the Company's activities in accounting entries, balance sheets, reports and other documents***

In each functional division or concerned organizational unit, suitable measures are established to grant that accounting operations are carried out correctly and in compliance with the principle of truthfulness, completeness and accuracy and that any anomalous situations are promptly reported;

suitable measures are established to grant that the information given to subjects in a higher hierarchical rank by the persons in charge of the function or the concerned organizational unit

of a lower rank is truthful, correct, accurate, timely and documented, also on a computer support;

the responsible function supplying data and information about balance sheet or other corporate communications should sign a statement of truthfulness and completeness of the forwarded information, with precise, analytical and documentable claims;

suitable measures are established to grant that, whenever requests are made by any party about an atypical quantitative change of data vs. the ones already accounted according to the usual procedures, any person aware of them will immediately inform the BODY;

suitable measures are established to grant that, whenever unwarranted requests are made about a change of detection, recording and accounting criteria, any person aware of them will immediately inform the BODY;

suitable measures are established to identify a responsible for the control of the information supplied from the companies operating within the area of consolidation with the aim of drawing-up the consolidated balance sheet. The COMPANY requests to the companies communicating such information to state their truthfulness and completeness;

anybody who forwards the established information to authorities in a higher hierarchical rank should mention the documents or sources from which the forwarded information have been taken and processed, in order to grant their control. Duplicates of the requested documents should be made available;

***15.24. Purchase, sale or other transactions, in whatever form concluded, of unlisted financial instruments or instruments for which no application has been submitted for admission to trading***

***in a regulated market and to the stipulation of derivative contracts not traded on regulated Italian and European markets***

The definition and formalization of a *policy* is established concerning the management of financial investments and relevant risks;

introduction and integration of principles, regulations and procedures concerning market abuses are expected, also making reference to the case series reported by CONSOB and other vigilance and control authorities, even during inspections;

the procedures to carry out transactions on unlisted financial instruments, including also pricing, should be formalized. The performance of transactions should be subjected to the authorization by the Board of Directors;

definition and formalization of principles and operational rules are established concerning transactions on unlisted financial instruments or instruments for which no application has been submitted for admission to trading on a regulated market, differentiating, if necessary, the rules depending on the kind of financial instrument and the reason of the transaction;

the unlisted financial instruments which could be involved in transactions by the COMPANY should be identified, also through controlled companies;

counterparts with whom such transactions can be generally carried out should be identified, along with the limits established for the management of investments and related risks;

the procedures should include the definition of the subjects suitable to decide and carry out the

transactions and to perform activities of vigilance and control on them;

quantitative levels of authorization and approval should be determined;

whenever the trading counterpart is not a financial intermediary submitted to prudential supervision, and does not show fairness and transparency in compliance with EU standards, the function involved in the decision-making process should supply a documented explanation of the transaction and its established price;

derivative contracts are stipulated according to contract models acknowledged by the best international practice (ISDA);

***15.25. Communication of significant information about the COMPANY or GROUP-owned companies concerning unlisted financial instruments or instruments for which no application has been submitted for admission to trading on a regulated market***

Suitable measures are established to grant truthfulness, completeness and accuracy of the information about the COMPANY destined to the market;

suitable measures are established to grant the role separation between the subjects who supply, the ones who approve and the ones who spread information about the COMPANY ;

suitable measures are established to grant that significant information internally transmitted by e-mail are protected against any risks of improper disclosure;

***15.26. Transactions with listed financial instruments***

Financial instruments are defined and described;

a policy is defined and formalized concerning the management of financial investments and relevant risks, the detection of financial instruments which could be involved in transactions by the COMPANY, the relevant quantitative levels of authorization and approval, the counterparts with whom such transactions can be generally carried out and limit thresholds established for the management of investments and relevant risks;

principles and operational rules are defined concerning the performance of transactions on financial instruments, differentiating the rules, when necessary, depending on the type of financial instrument and the purpose of transaction . These procedures should include the definition of the subjects competent to decide the transactions, to carry them out and to exercise activities of control and vigilance on them;

**Commento [c1]:**

procedures are formalized to carry out transactions on financial instruments, including also pricing, whenever the counterparts are GROUP-owned companies and controlling companies, as well as the related parties of the mentioned companies. For this purpose, transactions should be submitted to the authorization by the Board of Directors;

regulations, modes and procedures – also computer based – are established to grant the separation between subjects empowered to act as representatives, also with delegation, in bank transactions and subjects empowered to act as representatives in transactions on financial instruments;

***15.27. Management of privileged information***

Specific procedures are generally adopted for development, implementation, internal and external communication of the COMPANY 's decisions and of events occurring within the COMPANY 's range of action;

the COMPANY 's areas of action are identified, where the privileged information mentioned under the previous point are generally developed, updated, communicated and managed;

suitable measures are established to grant the role separation among the subjects who supply, the ones who approve and the ones who spread information about the COMPANY or other GROUP-owned companies destined to investors, investment analysts, journalists or other mass media representatives;

privileged information or information going to become privileged are identified in the COMPANY (also by the preparation of example lists), as well as criteria suitable to identify the information as privileged or going to become privileged. In particular, whenever the information concern multiple step events or decision-making processes, the definition of privileged information will specify the criteria to assess the time from which the piece of information should be submitted to the procedures of privileged information management (information going to become privileged); in the mentioned definition, communications, instructions, and recommendations of Vigilance and Control Authorities should be considered, also on the basis of suspected transaction lists issued by European Union bodies (e.g. CESR). The definition of identification criteria for privileged information or information going to become privileged should be made by the concerned function and submitted to the BODY 'S approval;

parameters are identified to detect GROUP-owned companies which could be a source of privileged information and to extend the procedure for privileged information management to such companies;

a procedure is established - if necessary - to detect the time when privileged information or information going to become privileged should be disclosed to the public and to identify the subject competent for the disclosure;

confidentiality of either printed or computerized privileged information or information going to become privileged is granted within the COMPANY;

suitable measures are established to prevent and avoid improper and unauthorized disclosure of privileged information or information going to become privileged inside or outside the COMPANY;

suitable measures are established to specifically grant that e-mail internally transmitted significant information is protected against any risks of improper disclosure;

measures are also established to protect, store and update information that – when involving multiple-step procedures – integrate the contents of information themselves;

suitable measures are granted to avoid the selective disclosure of privileged information and information going to become privileged;

subjects that – because of their professional or working activity, i.e. because of their tasks - manage privileged information or information going to become privileged are identified, if necessary; the names of these subjects are entered on an electronic register, with suitable aids to grant their filing and unchangeability except appropriate evidence is given; the entry on the register should be communicated to the concerned subject in order to impose the compliance with the relevant procedures and resulting prohibitions. The same should apply to the subjects allowed to access privileged information or information going to become privileged; moreover, a responsible for the registers including the names of the mentioned subjects is identified, in order to supervise the proper working and to control confidentiality and updating, with the possibility of accessing the register and the contained information;

any– even accidental – access to privileged information is forbidden to persons without proper authorization, as well as the improper spread of information, also within the COMPANY. In particular, documents containing privileged information or information going to become privileged should be filed and stored by the concerned function and the person in charge - in places - also computer files – with a limited access and properly protected. In particular, filing should occur in such a way that it cannot be possible to allow a subsequent change, save appropriate evidence of access to already filed documents is given. The access to these documents will be always grounded and allowed only to authorized persons according to internal standards. Duplicates of documents containing privileged information should be supplied only to authorized persons and any extra duplicates should be destroyed at the end of any meetings;

in case of legitimate disclosure of privileged information to COMPANY 's external subjects (e.g. consultants, auditing companies), contract provisions should be prepared binding the third party to the information confidentiality, possibly establishing the adoption by these subjects of proper measures to protect the received information;

a general prohibition to trade on listed or unlisted financial instruments or derivatives is established for all the subjects who have administrative, control or management functions in the COMPANY and for managers who can normally access privileged information and can take management decisions which could affect the development and future prospects of the COMPANY (the so-called significant persons); possible investment transactions by these subjects can exclusively be carried out through management funds with prohibition of qualitative instructions;

suitable measures are established to prevent that, when the COMPANY transmits the market information contained in the financial statement, in the consolidated balance sheet, in the quarterly or six-month report, further communications are released to the market or to third parties about the mentioned information;

relations with investors, journalists, other mass media representatives or the general audience are exclusively kept by subjects belonging to the concerned functions (at least two, including the function responsible), in compliance with timetable and procedures established by the law, by the market Vigilance Authority and by the internal control system;

the organization and participation in any meetings, in whatever form they are held, with investors, financial analysts, journalists or other mass media representatives, should be made exclusively by the concerned functions and in compliance with the authorization and internal control procedures in force;

suitable measures are established to preventively verify and control the entitlement to participate in the meetings, and the contents to be treated, in whatever form they are held, with investors, journalists or other mass media representatives;

to safeguard truthfulness and completeness of information, suitable measures are established to verify the contents of reports, briefing notes, press releases, informative materials in any form,

destined to Vigilance and Control Authorities or to investors, journalists, other mass media representatives, market or general audience;

***15.28. Protection of industrial properties and copyrights***

Before the marketing of products (either exported or imported, either developed by the COMPANY or obtained on license from third parties) or their manufacturing in Countries that recognize industrial property titles and rights, the existence (or the possibility of infringement) of valid private rights of third parties is controlled (in this case basically, patented inventions, trademarks and non-patented, but secret substantial and identified *know-how*);

the management of the above mentioned controls is centralized in the COMPANY'S Legal Department both for patents and trademarks ;

controls, carried out also with the aid of outsourced qualified consultants and having a written opinion from the Legal Department and possibly from a consultant, should be forwarded to the Managing Director for the ultimate decision;

also the filing of application for patented invention or trademark registration should be preceded by proper controls concerning both the general state of the art and other persons' specific rights existing in the concerned Country/Countries, so as to grant that novelty and invention requirements are met for patented inventions and originality and impossible confusion requirements are met for trademarks;

any appeals or objections in court or administrative headquarters against other people's patents or trademarks are also preceded by proper controls which confirm the total or partial illegality or invalidity of such titles and should be approved by the Managing Director with the favorable opinion of Legal Department;

patent applications are processed by the COMPANY Research Department; trademarks are processed by the relevant trade units or by the licensing sector. The candidate applications and trademarks, having the proper opinion of the Legal Function after performing the controls, are forwarded to the Managing Director for the ultimate decision;

whenever, for urgency reasons, the Managing Director's ultimate decision cannot be preceded by suitable controls, the possibility of filing the patent applications or trademark registrations is subject to appropriate explanation of this derogation shared with Legal Department;

for confidential non-patented know-how received from third parties on the basis of agreements of confidentiality or of other kind, internal communication can be made only according to the *need-to-know* principle, when qualified persons actually involved in the assessment and/or /use of such know-how really need to know it;

the diffusion of scientific publications or of other kind of publications, their abstracts or duplicates can be established by the concerned business function only after control by the Legal Function of the compliance with the copyright regulations in force.

***15.29. Guarantee of nature, quality, compliance of marketed products***

Appropriate control mechanisms are established to avoid that the product delivered to the purchaser does not correspond to the declared or negotiated one for nature, origin, source, quality or quantity;

***15.30. Planning of prevention and protection service concerning workers' health and safety***

A budget, yearly and long term investment plans and specific programs in order to detect and allocate the resources required to achieve health and safety goals are arranged;

***15.31. Structure organization about the activities concerning workers' health and safety***

A prevention and protection plan, the relevant implementation procedures and the relevant monitoring periodical system are established;

roles, responsibilities and procedures of prevention and protection service management are regulated inside the organization;

the mechanisms are defined in compliance with legal regulations concerning:

- assessment and periodical control of qualification and professionalism requirements of the responsible of the prevention and protection service (called RSPP) and of the staff involved in the prevention and protection service (called SPP);
- definition of minimum skills, number, tasks and responsibilities of workers assigned to emergency measures, fire prevention and first aid;
- process of appointment and relevant acceptance by the Competent Physician, pointing out procedures and timing in case of role replacement

***15.32. Risk detection, assessment and mitigation concerning workers' health and safety***

A procedure is defined for the preparation of the Risk Assessment Document (RAS) which establishes, among the other things, the operating procedures of RAS compilation, the responsibilities for the assessment and approval of its contents, the activities of monitoring the implementation and efficacy of actions carried out to protect health and safety in order to re-assess risks and update the same document;

***15.33. Activities of monitoring of workers' health and safety***

A procedure is prepared for a regular and continuous monitoring of data/markers representing the main characteristics of the different activities of the prevention and protection system, establishing, among the other things :

- roles and responsibilities;
- definition and formalization of specific performance markers for the managing activities of Prevention and Protection System, which allow to assess its efficacy and efficiency;

- regulation of monitoring activities;
- analysis and implementation of corrective actions of any system deficiencies ;

the monitoring procedure should establish the traceability of the occurred accidents, missed accidents and potentially dangerous situations, their detection and recording and the investigation about them;

***15.34. Audit activities about workers' health and safety***

Organizational provisions are detected concerning application area, frequency, procedures, skills, roles and responsibilities as well as the requirements for the performance of audit activities and recording and communication of results about concrete and effective application of technical and organizational solutions concerning management and all operational aspects, in compliance with legal provisions and company regulations;

regular controls are established and scheduled about the implementation of the adopted measures destined to neutralize workers' health and safety risk; corrective actions are also established whenever deviations are detected from the provisions stated in the mentioned specific technical and organizational solutions, as well as the control of implementation and efficacy of the mentioned corrective actions;

an organizational provision is established regulating roles, responsibilities and operational procedures of the specific periodical reporting, concerning the Managing Director and the Body, concerning the activities carried out and with the purpose of assessing the system efficacy and suitability;

***15.35. Management of prevention and protection system concerning workers' health and safety***

The procedures are defined concerning the activities of preparation and implementation of the prevention and protection system concerning workers' health and safety, establishing in particular:

- transcription and filing of health control outcomes of the individual workers in Health and Risk Case Report Form;
- management, distribution and maintenance of efficacy of personal protection equipment (PPE);
- operational procedures for the appointment of workers responsible for the implementation of preventive measures, emergency and first aid;
- operational procedures for the management of safety signs;
- operational procedures for workers' access to health and safety risk areas;
- operational procedures, roles and responsibilities in case of emergency situations;
- operational procedures for the relinquishment of workplace or dangerous zones where immediate and serious hazard is persisting;
- organizational measures for the detection of timing and procedures of the application for the issue or renewal of fire prevention certificate as well as the issue of provisional authorization;

check lists are prepared with the purpose of adopting operational measures aimed to avoid the occurrence of accidents, preparing, among the other things, a list of critical tasks and processes with an impact on health and safety, PPEs shared with the Head of Prevention and Protection Service, dangerous products and processes, critical equipment;

an emergency plan is defined and tested (also by emergency tests), as well as a procedure to manage emergencies suitable to mitigate the effects on people's health and external environment;

specific procedures about accidents are established concerning:

- definition of roles, responsibilities and operational procedures to prepare and compile the accident register;
- a check list to define the types of industrial accidents, according to the provisions of the regulations currently in force;

organizational measures are defined which establish the participation of the Competent Physician and RSPP in the definition of roles and workers' responsibility;

roles and responsibilities are established to define and implement the organizational procedures aimed to protect workers from risks related to the activities which they perform, to their workplace and to the use of equipment and machines; as well as risk related to the use of dangerous substances, chemical, physical, biological and cancerogenic agents;

a duty of fire risk assessment is established, as well as a duty of preparation and updating of fire safety register and the preparation of an emergency plan;

***15.36. Staff involvement in workers' health and safety***

Periodical meetings are established with managers, workers and their representatives;

previous consulting of workers' representatives is established concerning the risk detection and assessment and definition of preventive measures;

***15.37. Planning of environment protection aids in compliance with regulatory requirements***

A budget, annual investment plans and specific programs are prepared to identify and allocate the resources required to achieve purposes of environment protection;

***15.38. Monitoring of environment protection aids in compliance with regulatory requirements***

A procedure is prepared for a regular and continuous monitoring of data/markers representing the main features of the various protection system aids, establishing, among the other things:

- roles and responsibilities;
- definition and formalization of specific markers of performance for the protection aids, which allow to assess their efficacy and efficiency;
- regulation of monitoring activities;
- analysis and implementation of corrective actions for any system failures;

the monitoring procedure should establish the traceability of the occurred accidents, missed accidents and potentially dangerous situations, their detection and recording and the investigation about them;

***15.39. Audit activities concerning environmental protection***

Organizational provisions are detected concerning the application area, frequency, procedures, skills, roles, responsibilities as well as the requirements for the performance of audit activities as well as recording and communication of results about concrete and effective application of technical and organizational solutions concerning management and control of all the operational aspects, in compliance with legal requirements and corporate regulations;

regular controls are established and scheduled of the implementation of the adopted measures destined to neutralize the risk of environment-related crimes; corrective actions are also established whenever deviations are detected from the provisions stated in the mentioned specific technical and organizational solutions, as well as the control of implementation and efficacy of the mentioned corrective actions;

an organizational provision is established regulating roles, responsibilities and operational procedures of the specific periodical reporting, concerning the Managing Director and the Body, about the activities carried out and with the purpose of assessing the efficacy and adequacy of the system of protection of environment;

***15.40. Involvement of the staff in environmental protection***

Periodical meetings are established with managers, workers and their representatives in order to raise a higher awareness about topics of environmental protection;

***15.41. Detection of specific aids for particularly risk areas***

*Storage and employ of toxic gases*

Specific procedures are established for the loading and unloading logbooks, the managing of stores as a function of the maximum allowed load;

Specific procedures are established for the selection of the staff in charge licensed by the Ministry of Interiors and to be renewed periodically;

Specific procedures are established for the training, check of the training, examinations and licenses of the new hired staff;

*Safety of electric systems and fire extinguishing system*

specific procedures are established for:

- the request for work compliance and proper installation certificate when the order is made;
- filing of original documentation;
- delivery of certification to the fireworks service, at the time of renewal of CPI Certificate;
- periodical controls by ARPA or other notifying bodies;

*Management of waste register and annual statement of waste production and disposal*

specific procedures are established for:

- periodical authorization for dumping of special/dangerous solid and liquid wastes;
- load and unload record keeping;
- management of waste transfer to companies authorized for waste disposal;
- filling of ecological forms;
- waste homologation;
- dispatch and control of delivery;
- check of disposal carried out;
- annual MUD statement;
- identification and CER coding of new wastes;
- filing of documentation every ten years;

*Management of annual statement about the production of substances precursor of chemical weapons*

Specific procedures are established

*Fire prevention*

specific procedures are established for:

- request for assenting opinion about fire prevention in new plants, request for site inspection and updating of CPI certificate;
- request for issue of CPI certificate of the plant with sworn expertise and the statement "nothing has changed";
- fire prevention register and periodical controls of extinguishing equipment and fire detection systems (the issue of fire prevention certificates is related to the non-increased risk procedures established in Decree of Law no. 334/99);

*Regular control of remarkable accidents related to some dangerous substances*

Specific procedures are established:

- for the obligation of notification in case of overcoming the storage limits of dangerous substances (Articles 6 & 7 of Decree of Law 334/99;
- for the control of remaining amounts of dangerous substances due to the missing overcoming of the limits of notification;

*Safety management system*

specific procedures are established for the system consisting of:

- document of corporate policy signed by the legal representative and handed out to all the employees;
- re-assessment of frequency system at least every two years or on occasion of special events or significant changes;
- documentation of the Safety Management System;
- manual of Safety Management System procedures;
- management of system and process changes, management of accidents or near-accidents;
- internal *Auditors* and *self audit* system;

- staff training according to the legislation and to the Safety Management System in a broad sense;
- general and department emergency plans;
- general and department emergency teams;
- emergency and first aid teams ;
- training of the new staff about emergencies;
- OHSAS ISO 18001 certificate of SOS system;
- assessment of dangers and analysis of first-level hazards;
- assessment of legal requirements to be met at each new system/process;
- document of non-increased risk for new processes and plants;
- periodical risk assessment (5 years) for the whole factory;

*Potential safety setting, clearance and environmental clean-up of polluted areas*

specific procedures are established to develop:

- site characterization;
- plan of plant safety setting and implementation;
- provisional clearance plan and implementation;
- final clearance plan and implementation;
- periodical assessment of site condition, waste water processing, analytical monitoring on a periodical basis and re-assessment of handling efficacy;
- statement of clearance performed and reporting to authorities;

*Management of pressurized equipment*

specific procedures are established for:

- purchase and installation of equipment exclusively manufactured by qualified suppliers complying with pressurized equipment requirements;
- the requirement to supply the manufacturer with information about work in-progress and project technical specifications for the equipment correct capacity flow;
- the requirement to get an EC certificate of compliance and manual of use and maintenance available for all the facilities and filing of equipment in the logbook of ISPSEL (National Institute for Prevention and Safety at Work);

*Run-in and use of pressurized equipment– implementing the PED (Pressurized Equipment Directive*

specific procedures are established for:

- request to ISPSEL for the first control of new installation;
- filing of all the documents concerning each piece of equipment and controls carried out;
- management of safety valves protecting pressurized equipment;
- management of safety valves protecting non-pressurized equipment;
- PED requalification of all the pipes installed before year 2000 with a DN 80-diameter or more;
- certification of all the pipes newly installed or replacing the old ones depending on the fluid and system of operation;

*Authorizations to waste water discharge, atmospheric emissions and waste fluid storage*

specific procedures are established;

*Periodical analyses of discharge and reporting to Arpa (also for emissions)*

specific procedures are established;

*Assessment of chemicals restriction authorization*

specific procedures are established for:

- previous registration of all the substances;
- immediate registration for 4-5 substances;
- compliance with other requirements of the regulations in force;

*Road transports of dangerous goods*

specific procedures are established for:

- continuous check of correct transport of dangerous goods;
- check of correct labeling of dangerous goods according to the criteria of European legislation;

*Managing of environmental integrated authorization*
specific procedures are established

*Substance classification, labeling and packaging:*

specific procedures are established for:

- updating of substance classification;
- updating of safety forms with the new classification in the new format;
- issue of new labeling;

*Waste traceability*

specific procedures are established for the periodical compliance with the regulations concerning traceability of special dangerous wastes;

### *15.42. Management of information technology instruments*

*Confidentiality and data access*

confidential information should be protected both in transmission and in storage and filing steps, so to be exclusively available to the persons authorized to know it and, in general, each specific datum should be exclusively used by authorized subjects (confidentiality principle);

a protection system should be arranged which is suitable to detect and univocally qualify the users who want to access a processing or transmitting system;

a logical access system should be developed which is suitable to control the use of resources by processes and users, and which is expressed through management and control of the rights of access;

authentication should be carried out before further operational interactions between system and user; the relevant information should be stored and accessed only by authorized users;

***Data integrity***

Each datum of the company should match the one originally entered into the computer system or the one resulting to be legitimately changed and it should not be possible to change or alter any information by non authorized subjects (integrity principle);

*Data availability*

Corporate data should be always available according to process continuity requirements and in compliance with the regulations about historical storage (availability principle);

*Non-repudiation*

specific measures should be applied to grant that the processes can always be controlled and checked and that actions carried out can be ascribed to the individual subjects (so-called non-repudiation);

*Computer information safety, checks of vulnerability*

resources and relevant vulnerabilities or protection deficiencies, should be exhaustively identified and classified with reference to a specific threat, and to the following components: a) infrastructures (including the technological ones such as networks and systems); b) hardware; c) software; d) documentation; e) data and information; f) human resources;

internal and external threats against resources should be fully identified and grouped according to the following types: a) errors and malfunctioning; b) frauds and thefts; c) dangerous software; d) physical damages; e) system overload; f) failure to comply with the legislation in force;

in general, an activity of computer safety should be regularly planned and updated on a periodical basis, establishing a preventive protection system;

a corporate policy should be planned and implemented, establishing the modes by which the different users can access the applications, data and programs as well as a set of control procedures suitable to check if the access is allowed or prohibited according to the mentioned standards and to control the proper working of off-switching rules of non-active gates;

potential dangers which could result from materialization of threats should be established in advance, considering their possible occurrence and the possible counter-measures according to a cost-benefit analysis of investments for their arrangement;

a broad plan of preventive and corrective actions should be defined, to be implemented and re-assessed on a periodical basis taking in consideration the risks to be managed;

the residual risk should be documented and expressly accepted;

*Computer information safety, checks of proper use of instruments*

periodical random checks are carried out on the proper use of computer and electronic instruments by Company's internal and outside subjects;

controls carried out should be documented and the relevant results and evidence should be properly stored;

*Computer information safety, continuity in IT services*

an emergency system should be defined, i.e. all the technical and organizational procedures

should be prepared to face emergency situations and to grant transaction continuity through mechanisms of overcoming anomalous situations;

processes and mechanisms are established and implemented to grant resource redundancy so that they can be restored in a short time in case of unavailability of data processing protection supports, in order to assure confidentiality, integrity and availability to network channels and networking components;

*Computer information safety – analysis of IT events*

a full analysis of recorded events should be carried out aimed to detect and report anomalous events which – deviating from the established standards, thresholds and procedures – could be indicative of possible threats;

*Computer information safety – recording of IT events*

a system of tracing and monitoring of events and interventions for network safety setting should be arranged;

*Data – safety backup copies*

a safety data backup should be carried out at fixed intervals;

*Data - quality control*

technological aids should be established for a preventive control and continuous monitoring of data quality and HW-SW product performance;

*Physical safety* - sale server

a physical safety of sites containing IT systems should be granted;

a system of physical credential management should be organized (badge, pin, access codes, token authenticator, biometrical values);

*Procedures - operating instructions – management of accounts*

creation, change and removal of accounts and profiles should be regulated;

a password or assessment codes are established to access each terminal and should be exclusively known by the qualified staff and changed at fixed intervals;

formal procedures should be established to assign special privileges (e.g. system manager, *super user*);

*Logical and physical inventory - hardware and software*

a hardware and software inventory should be prepared, made available to users and constantly updated;

a corporate policy is planned and implemented to manage and control physical safety of sites and resources operating there, involving a precise knowledge of material and immaterial assets forming the company's assets to be protected (technological resources and information);

*Computer information safety* - Access Log

a periodical review of system administrators' logs should be performed in the manufacturing premises;

system operators should not access systems or data different from the ones on which they have been called to operate;

a constant tracing of users' access to the corporate network should be carried out;

controls should be carried out on the accesses of the applicative systems by the users;

*Computer information safety - Access to manufacturing premises*

a proper separation should exist between development, test and manufacturing premises and in particular the staff in charge of the development of applicative systems should not access the manufacturing premises;

*Computer information safety - encryption*

a policy is developed to use encryption controls to protect information;

the process of generation, distribution and storage of keys is regulated;

the management of the keys is regulated as a support of the encryption techniques by the COMPANY;

*Computer information safety - use of digital signature*

the use of digital signature on documents is regulated, making reference to the responsible subject, authorization levels, use of certification systems, possible use and sending of documents with storage procedure;

*Data - reuse of storage supports*

instruments are established to reuse storage supports under safety conditions (erasing or initialization of reusable supports in order to allow their reuse without safety problems);

***Privacy activity and regulations***

Minimum safety measures are adopted for personal data processing by electronic instruments (authentication and authorization systems, antivirus, backup);

safety activities are implemented to support DPS editing (periodical risk analysis, at least every year) on personal data processing carried out and audit activities aimed to detect uncovered areas with relevant planning of safety measures to be adopted;

*Procedures and operating instructions – Safety policy for in-house staff*

an information safety policy should be defined - password management and use, log-in and log-out procedures, e-mail use, modes of use of movable supports, use of protection systems (antivirus, antispam, antiphishing, antispy);

*Computer information safety - awareness and training of in-house staff*

a training and/or communication policy concerning safety is implemented to make all users and/or special professionals aware of the safety problems;

regulatory, technical and guidelines documents are compiled, divulgated and stored for a proper use of IT system by users and for an effective safety management by the concerned business functions;

*Suppliers of IT services/products - management of relations*

relations with suppliers of IT services are controlled on a periodical basis and proper caution provisions should be included in the relevant agreements;

*Suppliers of IT services/products - outsourcing controls and services*

IT assessments are performed on a periodical basis, in particular if services are carried out in outsourcing agreements.