[*DEROSSO S.P.A.*]

MODELLO DI ORGANIZZAZIONE E GESTIONE
Ai sensi del Decreto Legislativo 8 giugno 2001, n. 231
e successive modifiche

Approvato dall' Amministratore Unico in data 31.05.2010

INDICE

PARTE SPECIALE

DEFINIZIONI

Codice Etico: documento allegato al Modello che recepisce l'insieme dei diritti, dei doveri e delle responsabilità della Società nei confronti dei terzi portatori di interessi

D.lgs. 231/01: Il Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche

Destinatari: amministratori, dirigenti e dipendenti della Società, collaboratori esterni fornitori e partner della Società a cui le disposizioni del Modello sono rivolte

Enti: entità giuridiche destinatarie delle disposizioni del D.lgs. 231/01

Linee Guida: Linee Guida per la costruzione dei modelli di Organizzazione, Gestione e Controllo elaborate da Confindustria nel documento del 7 marzo 2002 aggiornate al 31 marzo 2008

Modello: il presente modello di organizzazione, gestione e controllo

Organismo di Vigilanza: l'organismo previsto all'art. 3 del presente Modello

Società: la Società De Rosso S.p.A.

TUF: D.lgs. 24 febbraio 1998, n. 58 – Testo Unico in materia di intermediazione finanziaria

PREMESSA

Il decreto legislativo “8 giugno 2001 n. 231”, pubblicato sulla Gazzetta Ufficiale n. 140 del 19 giugno 2001, ha introdotto nuove responsabilità per le società e, indirettamente, per il vertice aziendale. La necessaria prevenzione richiede nuovi accorgimenti organizzativi e di controllo sui quali le principali organizzazioni imprenditoriali (ABI, ANIA, Confindustria) hanno sviluppato e diffuso linee guida e raccomandazioni per le aziende.
In merito alle problematiche introdotte dalla normativa in commento DeRosso S.p.A. ha messo a punto un modello organizzativo specifico
Il presente documento, sottoposto all’approvazione dell’Amministratore Unico, dovrà essere verificato e riesaminato secondo la periodicità stabilita.
Di seguito, sono esposti i criteri che sono stati presi a base per la progettazione e realizzazione del Modello Organizzativo 231.
Il Modello è suddiviso in una Parte Generale (contenente le prescrizioni del Decreto Legislativo, le funzioni e gli obiettivi del Modello stesso, le funzioni di controllo interno, ecc.) e in più Parti Speciali redatte in relazione alle tipologie di reato la cui commissione è astrattamente ipotizzabile in DeRosso S.p.A. in ragione delle attività da essa svolte.

PARTE GENERALE

1. REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DEGLI ENTI

1.1. IL D.LGS. 231/01

Il D.lgs. 231/01 recante *"La disciplina della responsabilità amministrativa delle persone giuridiche delle società e delle associazioni anche prive di responsabilità giuridica, ai sensi dell'art 11 della legge n° 300, 29 settembre 2000"* ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche alle convenzioni internazionali in vigore e segnatamente:

- alla *Convenzione di Bruxelles del 26 luglio 2005,* relativa alla tutela degli interessi finanziari della Comunità Europea;
- alla *Convenzione di Bruxelles del 26 maggio 1997* sulla lotta alla corruzione dei pubblici ufficiali della Comunità Europea o degli Stati Membri;
- alla *Convenzione OCSE del 17 dicembre 1997*, sulla lotta alla corruzione dei Pubblici Ufficiali stranieri nelle transazioni economiche internazionali;
- alla *Convenzione internazionale di New York del 09 dicembre 1999 – art. 2* per la repressione del finanziamento del terrorismo.

Il D.lgs. 231/01 ha introdotto un regime di responsabilità amministrativa per gli Enti per i reati commessi nell'interesse o a vantaggio degli Enti stessi, che va ad aggiungersi alla responsabilità civile e penale in capo alla persona fisica che materialmente commette il reato.

Presupposti perché un Ente possa incorrere in tale responsabilità sono:

a) che il reato sia stato commesso nell'interesse o a vantaggio dell'Ente;
b) che il reato sia stato commesso da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso, ovvero da persone sottoposte alla direzione e vigilanza di uno di tali soggetti.

1.2. FATTISPECIE DI REATO

I reati per i quali l'Ente può essere ritenuto responsabile ai sensi del D.lgs. 231/01 - se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati *ex* art. 5, comma 1, del decreto stesso - possono essere compresi, per comodità espositiva, nelle seguenti categorie:

- delitti contro la pubblica amministrazione, richiamati dagli articoli 24 e 25 del D.lgs. 231/01, fra i quali figurano la malversazione a danno dello Stato, l'indebita percezione di erogazioni a danno dello Stato, la concussione, la corruzione per un atto d'ufficio, la corruzione per un atto contrario ai doveri d'ufficio, la corruzione in atti giudiziari, l'istigazione alla corruzione, la truffa a danno dello Stato, la truffa aggravata per il conseguimento di erogazioni pubbliche, la frode informatica a danno dello Stato;
- delitti informatici e trattamento illecito di dati, richiamati dall'articolo 24-*bis* del D.lgs. 231/01 fra i quali figurano l'accesso abusivo ad un sistema informatico o telematico, l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, l'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, il danneggiamento di informazioni, dati e programmi informatici, il danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, il danneggiamento di sistemi informatici o telematici, danneggiamento di sistemi informatici o telematici di pubblica utilità, la detenzione e diffusione abusiva di codici di

accesso a sistemi informatici o telematici, la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, la frode informatica del soggetto che presta servizi di certificazione di firma elettronica;

- delitti di criminalità organizzata, richiamati dall'art. 24 – ter del D.lgs. 231/01 fra i quali figurano i delitti di associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d.lgs. 286/1998, l'associazione di tipo mafioso anche straniere, scambio elettorale politico-mafioso, sequestro di persona a scopo di estorsione, associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope, l'associazione per delinquere ed i delitti concernenti la fabbricazione ed il traffico di armi da guerra, esplosivi ed armi clandestine;
- delitti contro la fede pubblica, richiamati dall'articolo 25-bis del D.lgs. 231/01 fra i quali figurano la falsificazione di monete, la spendita di monete falsificate, la contraffazione, fabbricazione o detenzione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo; la contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni, l'introduzione nello Stato e commercio di prodotti con segni falsi;
- delitti contro l'industria ed il commercio richiamati dall'art. 25-bis 1 del D.lgs. 231/01 fra i quali sono ricompresi la turbata libertà dell'industria o del commercio, la frode nell'esercizio del commercio, la vendita di sostanze alimentari non genuine come genuine, la vendita di prodotti industriali con segni mendaci, la fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale, la contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari, l'illecita concorrenza con minaccia o violenza, le frodi contro le industrie nazionali;
- i reati societari, richiamati dall'articolo 25-*ter* del d.lgs. 231/01 fra i quali figurano le false comunicazioni sociali, false comunicazioni sociali in danno dei soci o dei creditori, falso in prospetto, falsità nelle relazioni o nelle comunicazioni della società di revisione, impedito controllo, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori, formazione fittizia del capitale, indebita ripartizione dei beni sociali da parte dei liquidatori, illecita influenza sull'assemblea, aggiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza
- delitti in materia di terrorismo e di eversione dell'ordine democratico, richiamati dall'articolo 25-*quater* del D.lgs. 231/01;
- delitti di pratiche di mutilazione degli organi genitali femminili, richiamati dall'art. 25-*quater*.1 d.lgs. 231/01;
- delitti contro la personalità individuale, richiamati dall'articolo 25-*quinquies* del d.lgs. 231/01 (quali la prostituzione minorile, la pornografia minorile, la tratta di persone e la riduzione o mantenimento in schiavitù o in servitù);
- delitti in materia di abusi di mercato, richiamati dall'art. 25-*sexies* d.lgs. 231/01 (abuso di informazioni privilegiate e manipolazione del mercato);
- delitti commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, richiamati dall'art. 25-*septies* d.lgs. 231/01 (omicidio colposo e lesioni colpose gravi o gravissime);
- delitti in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, richiamati dall'art. 25 – *octies* del D.lgs. 231/2001

- delitti in materia di diritto d'autore, richiamati dall'art. 25 – novies del D.lgs. 231/01 e previsti dalla legge 22 aprile 1941, n. 633 recante la Protezione del diritto d'autore e di altri diritti connessi al suo esercizio;
- delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria richiamato dall'art. 25 - decies1 del D.lgs. 231/01.

1.3. SANZIONI

Il D.lgs 231/01 prevede le seguenti sanzioni a carico della Società, in conseguenza della commissione o tentata commissione dei reati sopra menzionati:

- Sanzioni pecuniarie:
  - sono sempre applicate
  - si applicano per quote con un minimo di 100 ed un massimo di 1.000
  - il valore delle quote varia da 500.000 a 3.000.000 di vecchie lire (pari rispettivamente ad Euro 258,23 e ad Euro 1.549,37)
  - non è ammesso il pagamento in misura ridotta;
- sanzioni interdittive (applicabili anche quale misura cautelare) che possono consistere in:
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la pubblica amministrazione;
  - esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi;
  - divieto di pubblicizzare beni e servizi;
- confisca:
  - del prezzo o del profitto del reato
  - "per equivalente", cioè di una somma di denaro, beni o altre utilità di valore equivalente
- pubblicazione della sentenza di condanna

1.4. FUNZIONE DEL MODELLO E POSSIBILE ESIMENTE DALLA RESPONSABILITÀ DELL'ENTE

L'art. 6 del D.lgs. 231/01 prevede una forma specifica di esonero dalla responsabilità qualora l'Ente dimostri che:

1. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
2. il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo della società dotato di autonomi poteri di iniziativa e di controllo;
3. le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
4. non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Il D.lgs. 231/01 prevede, inoltre, che – in relazione all'estensione dei poteri delegati e al rischio di commissione degli illeciti – i modelli di organizzazione e gestione debbano

[1] In realtà, tale disposizione è stata inserita dall'art. 4, comma 1 della legge 3 agosto 2009, n. 116, come articolo 25 – *novies*, non tenendo conto dell'inserimento di tale articolo 25 – *novies* da parte dell'art. 15, comma 7, lettera c) della legge 23 luglio 2009, n. 99. Per tale motivo, l'articolo viene rinumerato convenzionalmente come art. 25 – *decies*.

rispondere alle seguenti esigenze:

1. individuare le attività nel cui ambito esiste la possibilità che vengano commessi i reati e gli illeciti;
2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati ed agli illeciti;
3. individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati ed illeciti;
4. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
5. introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Lo stesso D.lgs. 231/01 prevede che i modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sulla idoneità dei Modelli a prevenire gli illeciti.
È infine previsto che, negli Enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente.
L'adozione del modello di organizzazione, gestione e controllo è facoltativa, ma se l'Ente vuole beneficiare dell'esonero di responsabilità deve dimostrare l'esistenza e l'applicazione del Modello stesso.

2. MODELLO ADOTTATO DALLA SOCIETÀ

2.1. REQUISITI GENERALI

Il presente Modello rappresenta un insieme coerente di principi, procedure e disposizioni che:

i) individuano le aree/i processi di possibile rischio nell'attività aziendale, con particolare riguardo a quelli che comportano un rischio di reato ai sensi del Decreto;
ii) incidono sul funzionamento interno della Società e sulle modalità con le quali la stessa si rapporta con l'esterno;
iii) regolano la diligente gestione di un sistema di controllo delle attività sensibili, finalizzato a prevenire la commissione, o la tentata commissione, dei reati e degli illeciti amministrativi rilevanti ai fini della responsabilità degli Enti.

Il suo scopo è quello di costituire un sistema strutturato ed organico di procedure, nonché di attività di controllo, da svolgersi anche in via preventiva volto a prevenire la commissione dei reati e degli illeciti sanzionati dal D.lgs. 231/01.

2.2. L'ADOZIONE DEL MODELLO

Il presente Modello è stato approvato dall'Amministratore Unico con deliberazione del 31.05.2010.
Nella redazione del Modello, la Società si è conformata alle Linee Guida elaborate da Confindustria al fine di agevolare gli Enti nella definizione dei modelli di organizzazione e gestione.

2.3. STRUTTURA DEL MODELLO

Il presente Modello è costituito da una "*Parte Generale*" e da singole "*Parti Speciali*" predisposte per le diverse tipologie di reati ed illeciti da prevenire individuati secondo le risultanze della Check List allegata al Modello medesimo.
La **Parte Generale** contiene le regole ed i principi generali del Modello, descrivendone principi e struttura, identificando l'organismo di vigilanza e definendo i criteri e le

regole che governano il sistema disciplinare. Questa parte deve mirare a tre fondamentali finalità:
_ Individuazione e mappatura dei rischi
_ articolazione di un sistema di controllo ex-ante
_ designazione dell'Organismo di Vigilanza
La prima **Parte Speciale** – denominata Parte Speciale "A" – trova applicazione per le tipologie specifiche di reati previste dagli artt. 24 e 25 del D.lgs. 231/01, ossia per i reati realizzabili nei confronti della Pubblica Amministrazione.
La seconda Parte Speciale – denominata Parte Speciale "B" – riguarda i delitti contro la fede pubblica in materia di falsità di monete, in carte di pubblico credito e in valori di bolloe in strumenti o segni di riconoscimento (art. 25-*bis* del D.lg. 231/01).
La terza Parte Speciale – denominata Parte Speciale "C" – riguarda i c.d. reati societari (art. 25-*ter* del Decreto).
La quarta e la quinta Parte Speciale – denominate rispettivamente Parte Speciale "D" e Parte Speciale "E" – sono relative ai delitti con finalità di terrorismo o di eversione dell'ordine democratico e ai delitti contro la personalità individuale e contro la persona (artt. 25-*quater* e 25-*quinquies* del D.lgs. 231/01).
La sesta Parte Speciale – denominata Parte Speciale "F" – riguarda i reati e gli illeciti amministrativi di abusi di mercato (art. 25-*sexies* del D.lgs. 231/01 e dall'art. 187-*quinquies* del TUF).
La settima Parte Speciale – denominata Parte Speciale "G" - riguarda i reati di omicidio colposo e lesioni colpose gravi e gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-*septies* del D.lgs. 231/01).
L'ottava Parte Speciale – denominata Parte Speciale "H" - riguarda i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-*octies* del D.lgs. 231/01).
La nona Parte Speciale – denominata Parte Speciale "I" – riguarda i reati transnazionali di cui all'art. 10 della legge 16 marzo 2006, n. 146, , i delitti di criminalità organizzata (art. 24 – ter del D.lgs. 231/01) ed il delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 – decies del D.lgs. 231/01).
La decima Parte Speciale – denominata Parte Speciale "L" – riguarda i delitti informatici e trattamento illecito di dati (art. 24 - *bis* del D.lgs. 231/01).
L'undicesima Parte Speciale – denominata Parte Speciale "M" – riguarda i delitti contro l'industria ed il commercio (art. 25 - bis 1 del D.lgs. 231/01).
La dodicesima Parte Speciale – denominata Parte Speciale "N" - riguarda i delitti in materia di diritto d'autore (art. 25 – novies del D.lgs. 231/01).

2.3BIS. IDENTIFICAZIONE DELLE AREE A RISCHIO

A seguito dell'analisi della struttura organizzativa e delle informazioni acquisite durante i colloqui effettuati con i Responsabili aziendali e alcuni loro Collaboratori, sono state identificate le aree a rischio nell'ambito delle quali è possibile ipotizzare l'eventuale commissione dei reati di cui al Decreto. Per quanto riguarda i reati previsti dall'articolo 25 ter del Decreto, l'identificazione delle aree ha tenuto conto dei flussi di dati e di informazioni a supporto del processo di redazione del bilancio, la diffusione di notizie e la gestione dei rapporti con organismi di controllo e di vigilanza secondo quanto riportato nelle citate Linee Guida emanate dalla Confindustria.
Sulla base delle informazioni acquisite durante i predetti colloqui e successivamente alla individuazione delle aree e attività a rischio reato, sono state focalizzate le possibili modalità di realizzazione dei reati stessi unitamente, per le aree oggetto di analisi, alla esplicitazione dei più significativi fattori di rischio che possono favorire il

verificarsi delle modalità di realizzazione dei reati, nonché dei controlli tesi a mitigare i suddetti fattori di rischio.

2.4. PRINCIPI ISPIRATORI DEL MODELLO

Il sistema di controllo delineato dal Modello si ispira ai principi di:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione, con particolare riferimento a quelle a rischio. Qualunque attività rientrante nelle aree a rischio deve essere adeguatamente documentata affinché si possano acquisire, in qualunque momento, informazioni in merito:
  i) alle principali fasi dell'operazione;
  ii) alle ragioni che hanno portato al suo compimento;
  iii) ai soggetti che ne hanno fornito le necessarie autorizzazioni;
- separazione delle funzioni, con l'obiettivo che nessuno possa gestire in autonomia tutte le fasi di un processo, ma vi sia:
  iv) una netta differenziazione, all'interno di ciascun processo, tra il soggetto che lo inizia, il soggetto che lo esegue e lo conclude e quello che lo controlla;
  v) la documentazione scritta di ciascun passaggio rilevante del processo.

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già operanti nella Società, rilevati in fase di analisi delle attività a rischio, in quanto idonei a valere anche come misure di prevenzione dei reati e degli illeciti sui processi coinvolti nelle aree a rischio.
Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali ed effettuare i controlli sull'attività di impresa, anche in relazione ai reati e agli illeciti da prevenire, la Società ha individuato:

1) il Codice Etico;
2) il sistema di controllo interno;
3) il sistema sanzionatorio di cui ai Contratti Collettivi Nazionali di Lavoro applicabili;
4) ogni altra documentazione relativa ai sistemi di controllo in essere nella Società.

Le regole, le procedure e i principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare e che tutti i destinatari in relazione al tipo di rapporto in essere con la Società sono tenuti a rispettare.

2.5. AGGIORNAMENTO ED ADEGUAMENTO DEL MODELLO

L'Amministratore Unico, salvo quanto di seguito espressamente previsto, ha competenza esclusiva per l'adozione e la modificazione del Modello.
L'Amministratore Unico provvede a modificare tempestivamente il Modello qualora:

- siano individuate significative violazioni o elusioni delle prescrizioni in esso contenute che ne evidenziano l'inadeguatezza a garantire l'efficace prevenzione dei fatti di reato.
- intervengano modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- intervengano modifiche normative;
- ciò risulti necessario alla luce delle risultanze delle verifiche compiute.

Le proposte di modifica al Modello sono preventivamente comunicate all'Organismo di Vigilanza, il quale deve provvedere senza indugio a rendere le stesse modifiche operative ed a curare la corretta comunicazione dei contenuti ai loro destinatari.
L'Organismo di Vigilanza, in ogni caso, deve prontamente segnalare in forma scritta, senza dilazione, all'Amministratore unico e al Collegio Sindacale eventuali fatti che evidenziano la necessità di revisione del Modello.
Il Modello è sottoposto a procedimento di revisione periodica con cadenza quantomeno biennale da disporsi mediante delibera dell'Amministratore Unico.

3. ORGANISMO DI VIGILANZA

3.1. INDIVIDUAZIONE DELL'ORGANISMO DI VIGILANZA

Il compito di vigilare continuativamente sull'efficace funzionamento e sull'osservanza del Modello, nonché di proporne l'aggiornamento all'Amministratore Unico, è affidato all'Organismo di Vigilanza istituito dalla Società e dotato di autonomia e indipendenza nell'esercizio delle sue funzioni.

L'Organismo di Vigilanza riferisce direttamente all'Amministratore Unico e la sua attività non può essere sindacata da alcun organo o struttura della Società.

L'Amministratore Unico nomina i componenti dell'Organismo di Vigilanza. Ciascuno di essi è scelto esclusivamente sulla base dei requisiti di professionalità, onorabilità, competenza, indipendenza e autonomia funzionale.

- *professionalità*

  Questo requisito si riferisce al bagaglio di strumenti e tecniche che l'OdV deve possedere per poter svolgere efficacemente l'attività assegnata. Si tratta di tecniche proprie di chi svolge attività di "verifica". Con riferimento alle competenze giuridiche, considerato che la disciplina in argomento è in buona sostanza una disciplina penale e l'attività dell'Organismo di Vigilanza ha lo scopo di prevenire il compimento di reati, è essenziale la conoscenza della struttura e delle modalità realizzative dei reati, che potrà essere assicurata all'Organismo di Vigilanza anche mediante l'utilizzo delle risorse aziendali, ovvero della consulenza esterna.

- *continuità di azione*

  Per poter dare la garanzia di efficace e costante attuazione di un modello si rende necessaria la presenza di una struttura dedicata all'attività di vigilanza. La definizione degli aspetti attinenti alla continuità dell'azione quali ad esempio la programmazione dell'attività, è rimessa allo stesso Organismo di Vigilanza.

- *onorabilità*

  Requisito che attiene all'onorabilità personale della persona investita della funzione di OdV. Onorabilità valutata sulla base di quanto già previsto per altri settori della normativa societaria (es. Collegio Sindacale, Controllo Interno).

- *autonomia, indipendenza e assenza conflitti di interesse*

  I requisiti sono da valutare in relazione alla funzione dell'OdV e ai compiti che la legge assegna allo stesso. La posizione dell'OdV, nell'ambito della azienda, deve garantire l'autonomia dell'iniziativa di controllo da ogni forma d'interferenza e/o di condizionamento da parte di qualunque componente dell'Azienda (e in particolare dell'organo dirigente). Tali requisiti sembrano assicurati dall'inserimento dell'Organismo in esame come unità di staff in una posizione gerarchica la più elevata possibile e prevedendo il "riporto" al massimo Vertice operativo aziendale ovvero all'Amministratore Unico. Si sottolinea tuttavia, che al fine di garantire la necessaria autonomia di iniziativa e l'indipendenza è indispensabile che all'OdV non siano attribuiti compiti operativi che, rendendolo partecipe di decisioni ed attività, lo metterebbero in conflitto di interesse relativamente all'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

Non possono essere nominati membri dell'Organismo di Vigilanza e, se nominati, decadono dall'ufficio:

- coloro che incorrono nella cause di ineleggibilità e decadenza previste dall'art. 2382 c.c. (interdizione, inabilitazione, fallimento, interdizione – anche temporanea – dai pubblici uffici, incapacità ad esercitare uffici direttivi);
- il coniuge, i parenti e gli affini entro il quarto grado degli amministratori esecutivi della Società, gli amministratori esecutivi, il coniuge, i parenti e gli affini entro il quarto grado degli amministratori delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo;

- coloro che sono stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria;
- coloro che sono stati condannati con sentenza irrevocabile ovvero hanno concordato la pena ai sensi degli art. 444 e ss. c.p.p. in relazione ad uno dei reati previsti dal D.lgs. 231/01.

I membri dell'Organismo di Vigilanza non appartenenti al personale della Società devono essere dotati degli ulteriori seguenti requisiti di eleggibilità:

a) non essere legati alla Società da rapporti continuativi di prestazione d'opera che ne possano ragionevolmente compromettere l'indipendenza;
b) non intrattenere, neppure indirettamente, con la Società o con soggetti legati ad essa, relazioni di natura patrimoniale tali da condizionarne l'autonomia di giudizio.

Applicando tali principi alla realtà aziendale di De Rosso Spa e in considerazione della specificità dei compiti che fanno capo all'Organismo di Vigilanza, il relativo incarico è stato affidato, con delibera del……., alla Dott.ssa Wally Callegari responsabile della funzione deputata al Sistema di Controllo Interno. È pertanto rimesso al suddetto organismo il compito di svolgere, in qualità di Organismo di Vigilanza, le funzioni di vigilanza e controllo previste dal Modello.

I membri dell'Organismo di Vigilanza rimangono in carica per tre esercizi e sono rieleggibili.
L'Organismo di Vigilanza decade dalla data dell'assemblea sociale convocata per l'approvazione del bilancio relativo all'ultimo esercizio della sua carica, pur continuando a svolgere *ad interim* le proprie funzioni fino a nuova nomina dei componenti dell'Organismo.
La revoca dell'incarico di uno o più membri dell'Organismo di Vigilanza prima della scadenza e l'attribuzione di tali poteri ad altro soggetto potrà avvenire esclusivamente per giusta causa e mediante un'apposita delibera dell'Amministratore Unico, informato il Collegio Sindacale.

3.2. COMPITI E FUNZIONI DELL'ORGANISMO DI VIGILANZA

All'Organismo di Vigilanza della Società è affidato l'espletamento dei seguenti compiti:

a) costante verifica dell'efficienza ed efficacia del Modello adottato rispetto alla prevenzione ed all'impedimento della commissione dei reati previsti;
b) verifica del rispetto delle modalità e delle procedure previste dal Modello e rilevazione degli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni;
c) formulazione delle proposte all'Amministratore Unico per gli eventuali aggiornamenti ed adeguamenti del Modello adottato, da realizzarsi mediante le modifiche e/o le integrazioni che si dovessero rendere necessarie in particolare in conseguenza di:
    - significative violazioni delle prescrizioni del Modello;
    - significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
    - modifiche normative;
d) segnalazione all'Amministratore Unico, per gli opportuni provvedimenti, di quelle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;
e) predisposizione di una relazione informativa, su base almeno semestrale, per

l'Amministratore Unico e per il Collegio Sindacale in ordine alle attività di verifica e controllo compiute ed all'esito delle stesse.

Gli incontri con gli organi societari cui l'Organismo di Vigilanza riferisce sono documentati e copia della documentazione viene custodita a cura dell'Organismo medesimo.

Sul piano operativo, è affidato all'Organismo di Vigilanza della Società il compito di:

- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree a rischio, come individuate nelle singole Parti Speciali del Modello;
- regolare il proprio funzionamento anche attraverso l'introduzione di un regolamento delle proprie attività che disciplini, tra l'altro, la calendarizzazione delle attività, le modalità di convocazione, partecipazione, voto e verbalizzazione delle riunioni, la disciplina dei flussi informativi dalle strutture aziendali all'Organismo di Vigilanza, la cadenza temporale dei controlli, l'individuazione dei criteri e delle procedure di analisi. Tale regolamento non necessita di alcuna approvazione da parte di organi societari diversi dall'Organismo di Vigilanza e ciò al fine di tutelare l'indipendenza dell'Organismo medesimo;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e proporre la predisposizione della documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso, contenente le istruzioni, chiarimenti o aggiornamenti;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello;
- coordinarsi con i responsabili delle altre funzioni aziendali (anche attraverso apposite riunioni) per i diversi aspetti attinenti all'attuazione del Modello;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle aree a rischio;
- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di illeciti;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di illeciti (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal D.lgs. 231/01, proponendo, in caso contrario, un aggiornamento degli elementi stessi;
- verificare – con il supporto delle altre funzioni aziendali competenti – il sistema di poteri in vigore, raccomandando eventualmente delle modifiche, ove ritenute necessarie;
- accedere liberamente presso, ovvero convocare, qualsiasi direzione, unità, esponente o dipendente della Società – senza necessità di alcun consenso preventivo – per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei compiti previsti dal D.lgs. 231/01, da tutto il personale dipendente e dirigente.

All'Organismo di Vigilanza non competono, né possono essere attribuiti, neppure in via sostitutiva, poteri di intervento gestionale, decisionale, organizzativo o disciplinare relativi allo svolgimento delle attività della Società.

L'Organismo di Vigilanza ha libero accesso presso tutte le funzioni della Società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D. Lgs. n. 231/01.

L'Organismo di Vigilanza può avvalersi - sotto la sua diretta sorveglianza e responsabilità - dell'ausilio di tutte le strutture della Società ovvero di consulenti esterni.
L'Organismo di Vigilanza ha un'autonomia di mezzi finanziari e logistici che ne garantiscono la piena e continua operatività.
A tal fine, l'Amministratore Unico provvede annualmente a dotare l'Organismo di Vigilanza, su proposta del medesimo, di un fondo adeguato di cui l'Organismo di Vigilanza potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti assegnati (es. consulenze specialistiche, trasferte ecc.).

3.3. FLUSSI INFORMATIVI DALL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza riferisce all'Amministratore Unico ed al Collegio Sindacale in merito a: (i) attuazione del Modello; (ii) rilevamento di eventuali criticità ad esso connesse; (iii) necessità di interventi modificativi di adeguamento.
In particolare, l'Organismo di Vigilanza riferisce:

- in via continuativa, direttamente all'Amministratore Unico;
- con cadenza periodica almeno semestrale al Collegio Sindacale.

L'Organismo di Vigilanza può essere convocato in qualsiasi momento dagli organi societari e potrà a sua volta presentare richiesta in tale senso, per riferire in merito a tutto ciò che riguardi il Modello.

3.4. REPORTING ALL' ORGANISMO DI VIGILANZA

In attuazione del disposto di cui all'art. 6 comma 2 lett. d) del D.lgs. 231/01, l'Organismo di Vigilanza deve essere tempestivamente portato a conoscenza, oltre che della documentazione prescritta nelle singole Parti Speciali del Modello, di ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi, attinente a quegli atti, comportamenti od eventi che possono determinare una violazione del Modello o che, più in generale, siano comunque rilevanti ai fini del D.lgs. 231/01.
L'obbligo di informazione è esteso in via generale a tutti i Destinatari.
In particolare, l'obbligo di dare informazione all'Organismo di Vigilanza è rivolto alle funzioni aziendali a rischio di commissione reato e riguarda:

a) le risultanze periodiche dell'attività di controllo dalle stesse posta in essere per dare attuazione al Modello (*report* riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.);
b) le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

Nella specie le informazioni potranno riguardare, ad esempio:

- le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la magistratura procede per i reati previsti dalla richiamata normativa;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. n. 231/2001;
- le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al D. Lgs. n. 231/2001;
- le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

L'Organismo di Vigilanza dovrà altresì ricevere:

- i prospetti riepilogativi degli eventuali appalti affidati a seguito di gare, ovvero a trattativa privata;
- le notizie relative alle eventuali commesse attribuite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità;
- copia della reportistica periodica in materia di salute e sicurezza sul lavoro;
- copia della documentazione relativa alle eventuali certificazioni di qualità della Società.

Dovranno altresì essere tempestivamente comunicate all'Organismo di Vigilanza le informazioni concernenti:

- il mancato rispetto del Modello, affinché possa esserne valutata la concreta efficacia;
- l'apertura di procedimenti disciplinari per l'accertamento di violazioni del Modello e l'esito degli stessi;
- le modifiche interne alla Società riguardanti gli elementi costitutivi del Modello (ad esempio, modificazioni di poteri/responsabilità, procedure operative, sistemi informativi ecc.);
- gli eventi esterni in grado di condizionare l'efficacia del Modello (ad esempio, mutamenti del contesto normativo ecc.);
- in via residuale, ogni notizia / informazione / dato, che rivesta o possa rivestire un qualche rilievo per il corretto funzionamento del Modello.

Le segnalazioni debbono essere indirizzate all'Organismo: a tale fine è stata configurata la casella di posta elettronica odv@derosso.it a cui le segnalazioni possono essere inviate, per iscritto ed in forma non anonima.
Le comunicazioni a mezzo posta potranno invece essere indirizzate, sempre in forma non anonima, al seguente indirizzo: Organismo di Vigilanza di De Rosso S.p.A. c/o De Rosso S.p.A., , Farra di Soligo (TV).
L'Organismo, fatti salvi gli obblighi di legge, si impegna a garantire l'anonimato ad ogni esponente che ne faccia richiesta.

3.5. CONSERVAZIONE DELLA DOCUMENTAZIONE

A cura dell'Organismo di Vigilanza è conservata presso la Società copia cartacea e/o informatica di tutto il materiale relativo al Modello.
Hanno facoltà di accedere all'archivio cartaceo/informatico l'Amministratore Unico, i membri del Collegio Sindacale, i componenti dell'Organismo di Vigilanza e coloro che siano specificamente autorizzati da uno di tali soggetti, salve le disposizioni in materia di tutela dei dati personali.

4. FORMAZIONE DELLE RISORSE E DIFFUSIONE DEL MODELLO

4.1. FORMAZIONE ED INFORMATIVA AL PERSONALE

La Società predispone specifici interventi formativi rivolti a tutti i dipendenti al fine di assicurare un'adeguata conoscenza, comprensione e diffusione dei contenuti del Modello e del Codice Etico e di diffondere, altresì, una cultura aziendale orientata verso il perseguimento di una sempre maggiore trasparenza ed eticità.
Ogni dipendente è tenuto a: i) acquisire consapevolezza dei contenuti del Modello; ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività; iii) contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.
Al fine di garantire un'efficace e razionale attività di comunicazione, la Società promuove ed agevola - anche attraverso la partecipazione ad una specifica attività formativa - la conoscenza dei contenuti del Modello da parte dei dipendenti, con grado di approfondimento diversificato a seconda del grado di coinvolgimento nelle attività individuate come sensibili ai sensi del D.lgs. 231/2001.

4.2. INFORMAZIONE AI SOGGETTI ESTERNI ED AI CONSULENTI

L'attività di comunicazione dei contenuti del Modello è indirizzata anche nei confronti di quei soggetti terzi che intrattengano con la Società rapporti di collaborazione contrattualmente regolati o che rappresentano la Società senza vincoli di dipendenza (ad esempio: partner commerciali, agenti e consulenti, distributori, procacciatori d'affari e altri collaboratori autonomi).
A tal fine, ai soggetti terzi più significativi la Società fornirà un estratto descrittivo del Modello e/o del Codice Etico.
Si provvederà altresì alla pubblicazione del Modello e del Codice Etico sul sito web della Società www.derosso.it .

5. SISTEMA DISCIPLINARE

5.1. PRINCIPI GENERALI

La definizione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello, a norma dell'art. 6 comma 2° lett. e) del D.lgs. 231/01, costituisce un presupposto essenziale della valenza scriminante del Modello.
Tali violazioni sono assoggettate alle sanzioni disciplinari di seguito previste, a prescindere dall'eventuale giudizio penale.

5.2. SANZIONI NEI CONFRONTI DEI LAVORATORI DIPENDENTI NON DIRIGENTI

I comportamenti tenuti dai lavoratori dipendenti in violazione delle procedure e delle regole comportamentali indicate nel Modello costituiscono illeciti disciplinari.
Pertanto, ai dipendenti che violano il Modello sono irrogabili le sanzioni previste dalle norme disciplinari contenute nel Contratto Collettivo Nazionale di Lavoro vigente che si applica ai rapporti di lavoro aziendali, nel rispetto del principio della gradualità della sanzione e della proporzionalità alla gravità dell'infrazione.

I comportamenti che costituiscono violazione del Modello, corredati dalle relative sanzioni, sono i seguenti:

1. compatibilmente con quanto previsto dal Contratto Collettivo Nazionale applicabile, incorre nel provvedimento, a seconda della gravità, di "rimprovero verbale" o "rimprovero scritto" il lavoratore che violi una delle procedure interne previste dal Modello (ad esempio, che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, eccetera), o adotti nell'espletamento di attività nelle aree sensibili un comportamento non conforme alle prescrizioni del Modello stesso. Tali comportamenti costituiscono una mancata osservanza delle disposizioni impartite dalla Società;
2. compatibilmente con quanto previsto dal Contratto Collettivo Nazionale applicabile, incorre nel provvedimento della "multa sino a 3 ore di lavoro normale", il lavoratore che nel violare le procedure interne previste dal Modello, o adottando nell'espletamento di attività nelle aree sensibili un comportamento non conforme alle prescrizioni del Modello, esponga l'integrità dei beni aziendali ad una situazione di oggettivo pericolo. Tali comportamenti, posti in essere con la mancata osservanza delle disposizioni impartite dalla Società, determinano una situazione di pericolo per l'integrità dei beni della Società e/o costituiscono atti contrari agli interessi della stessa;
3. compatibilmente con quanto previsto dal Contratto Collettivo Nazionale applicabile, incorre nel provvedimento della "sospensione dal servizio e dal trattamento economico per un periodo non superiore a 3 giorni per gli operai e non superiore a 5 giorni per gli impiegati" il lavoratore che nel violare le procedure interne previste dal Modello, o adottando nell'espletamento di attività nelle aree sensibili un comportamento non conforme alle prescrizioni del Modello, arrechi danno alla Società compiendo atti contrari all'interesse della stessa, ovvero il lavoratore che sia recidivo oltre la terza volta nell'anno solare nelle mancanze di cui ai punti 1 e 2. Tali comportamenti, posti in essere per la mancata osservanza delle disposizioni impartite dalla Società, determinano un danno ai beni della Società e/o costituiscono atti contrari agli interessi della stessa;
4. compatibilmente con quanto previsto dal Contratto Collettivo Nazionale applicabile, incorre nel provvedimento del "licenziamento per giusta causa" il lavoratore che adotti, nell'espletamento delle attività nelle aree sensibili, un

comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato rilevante ai fini della responsabilità amministrativa degli enti. Tale comportamento fa venire meno radicalmente la fiducia della Società nei confronti del lavoratore, costituendo un grave nocumento morale e/o materiale per l'azienda.

Le suddette sanzioni saranno applicate nel rispetto dell'art. 7 della Legge 20 maggio 1970, n. 300 e conformemente a quanto previsto nel Contratto Collettivo Nazionale di Lavoro applicabile e nelle procedure aziendali.

E' fatta salva la prerogativa della Società di chiedere il risarcimento dei danni derivanti dalla violazione del Modello da parte di un dipendente.

5.3. SANZIONI NEI CONFRONTI DEI DIRIGENTI

In caso di violazione da parte dei dirigenti delle procedure e regole previste dal Modello o di adozione, nell'espletamento delle attività nelle aree di rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, nei confronti del responsabile saranno applicate le seguenti sanzioni:

1. in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel richiamo scritto all'osservanza del Modello, che costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
2. in caso di grave violazione di una o più prescrizioni del Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del licenziamento con preavviso;
3. laddove la violazione di una o più prescrizioni del Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il lavoratore incorre nel provvedimento del licenziamento senza preavviso.

Le suddette sanzioni saranno applicate nel rispetto dell'art. 7 della Legge 20 maggio 1970, n. 300 e conformemente a quanto previsto nel Contratto Collettivo Nazionale di Lavoro e nelle procedure aziendali.

5.4. SANZIONI NEI CONFRONTI DELL' AMMINISTRATORE UNICO E COLLEGIO SINDACALE

In caso di violazione del Modello da parte dell'Amministratore Unico o del Collegio Sindacale, l'Organismo di Vigilanza informerà tempestivamente l'Amministratore Unico e l'intero Collegio Sindacale, affinché ciascun consigliere o sindaco, singolarmente, ovvero ciascun organo, nel suo complesso, a seconda delle rispettive competenze, provveda ad assumere le iniziative più opportune ed adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione dell'Amministratore Unico, richiesta convocazione/convocazione assemblee con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, revoca delle deleghe da parte dell'assemblea ecc.).

5.5. SANZIONI NEI CONFRONTI DI COLLABORATORI ESTERNI, FORNITORI E PARTNERS

Il Modello spiega la sua efficacia anche nei confronti dei collaboratori esterni, dei fornitori e dei partners della Società. A tale riguardo, si evidenzia che ogni comportamento da essi posto in essere in contrasto con le linee di condotta indicate dal presente Modello e/o dal Codice Etico e tale da comportare il rischio di commissione di un reato sanzionato dal D.lgs. 231/01 potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali, la risoluzione del contratto ovvero il diritto della Società, fatta salva l'eventuale richiesta di risarcimento

dell'eventuale maggior danno.
In ogni caso la Società porterà i propri collaboratori, fornitori e partners a conoscenza – anche per estratto – del presente Modello e/o del Codice Etico, come indicato dal precedente art. 4.2.

6. MODELLO E CODICE ETICO

L'adozione di principi etici rilevanti ai fini della prevenzione dei reati *ex* D. Lgs. 231/01 costituisce un elemento essenziale del sistema di controllo preventivo configurato dalla Società.

Tali principi sono stati inseriti nel Codice Etico, che costituisce parte integrante e sostanziale del Modello, cui si ispirano sia la Parte Generale che le Parti Speciali.

Il Codice Etico contiene l'insieme dei diritti, dei doveri e delle responsabilità della Società nei confronti dei "*portatori d'interesse*" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.) e mira a raccomandare, promuovere o vietare determinati comportamenti, al di là ed indipendentemente da quanto previsto a livello normativo, e prevede sanzioni proporzionate alla gravità delle eventuali infrazioni commesse.

Il Codice Etico è stato approvato dall'Amministratore Unico con la medesima delibera che ha adottato il presente Modello.

7. CORPORATE GOVERNANCE

7.1. PRINCIPI GENERALI

Il sistema di corporate governance della Società, inteso come insieme dei principi e degli strumenti che presidiano al governo della medesima da parte degli organi sociali preposti, è retto dai seguenti principi:

- correttezza;
- trasparenza;
- rispetto della legge e dei regolamenti interni ed esterni alla Società;
- segregazione delle attività;
- tracciabilità delle operazioni.

Al fine di rispettare i principi di cui sopra led evitare pertanto la commissione dei reati previsti dal D.lgs. 231/01, la Società adotta in particolare i seguenti strumenti di corporate governance:

- adeguato sistema delle deleghe e delle procure;
- suddivisione dei poteri per funzioni.

7.2. IL SISTEMA DELLE DELEGHE E DELLE PROCURE

Il sistema di deleghe e procure deve essere caratterizzato da elementi utili ai fini della prevenzione dei reati (in particolare, rintracciabilità ed evidenziabilità delle operazioni sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale. A tal proposito si allega la tabella interfunzionale che indica procure e deleghe affidate ad ognuno; tali deleghe e procure sono formalizzate.

Si intende per "*delega*" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative e per "*procura*" l'atto giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

Ai titolari di una funziona aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza viene conferita una "*procura generale funzionale*" di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la delega.

I requisiti essenziali del sistema delle deleghe, ai fini di un'efficace prevenzione dei reati sono i seguenti:

- tutti coloro che intrattengono per conto della Società rapporti con soggetti terzi ed in particolare con la Pubblica Amministrazione devono essere dotati di delega formale in tal senso;
- le deleghe devono abbinare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma della Società ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna delega deve definire in modo specifico ed inequivoco:
  - i) i poteri del delegato;
  - ii) il soggetto (organo o individuo) a cui il delegato fa capo in via gerarchica;
  - iii) eventualmente, gli altri soggetti ai quali le deleghe sono congiuntamente e disgiuntamente conferite.
- i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei reati, sono i seguenti:

- le procure descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da un'apposita comunicazione aziendale che fissa l'estensione dei poteri di rappresentanza ed i limiti di spesa;
- la procura può essere conferita a persone fisiche espressamente individuate

nella stessa oppure a persone giuridiche, che agiranno a mezzo di propri procuratori investiti, nell'ambito di queste, di analoghi poteri;
- una procedura ad hoc deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le stesse devono essere attribuite, modificate e/o revocate (ad esempio, assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissione, licenziamento, revoca ecc.);
- le procure indicano gli eventuali altri soggetti a cui sono conferiti congiuntamente o disgiuntamente, in tutto o in parte, i medesimi poteri di cui alla procura conferita.

7.3. LA SUDDIVISIONE DEI POTERI PER FUNZIONI

Nessun soggetto deve poter gestire in autonomia un intero processo (c.d. principio di "*segregazione delle attività*").
In ottemperanza a tale principio ed al sistema delle deleghe e delle procure sopra descritto, la Società dovrà ripartire i poteri di rappresentanza e di azione in modo che il sistema organizzativo garantisca che vi sia sempre una netta separazione tra il soggetto che autorizza ad effettuare un'operazione, quello che la contabilizza, quello che la esegue operativamente e quello che la controlla.
A nessun operatore saranno attribuiti poteri illimitati, i poteri e le responsabilità devono essere chiaramente definiti e conosciuti all'interno dell'organizzazione e i poteri autorizzativi e di firma saranno coerenti con le responsabilità organizzative assegnate.
In tal senso l'organizzazione ha definito un organigramma aziendale e un mansionario specifico per funzione.

7.4. PRINCIPI GENERALI PER LA REDAZIONE DELLE PROCEDURE PER LA PREVENZIONE DEI REATI

Il presente paragrafo prevede l'espresso obbligo, a carico di tutto il personale direttivo ed i dipendenti interessati, e, tramite apposite clausole contrattuali, a carico di consulenti, fornitori e partner, di:

1. una stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione ed alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
2. gestione di qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

Il presente paragrafo prevede, conseguentemente, l'espresso divieto a carico degli esponenti aziendali in via diretta, e a carico dei collaboratori esterni tramite apposite clausole contrattuali, di porre in essere:

1. comportamenti tali da integrare le fattispecie di reato sopra considerate;
2. comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Per ciascuna delle operazioni di carattere significativo, rientranti nei tipi individuati all'articolo che precede sono previste specifiche procedure, in forza delle quali:

a) sia sempre individuato un responsabile relativo al procedimento;
b) siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
c) sia possibile procedere alla tracciabilità e verificabilità *ex post* delle transazioni

fatte con la Pubblica Amministrazione;

d) tutta la comunicazione in entrata ed uscita da e verso la Pubblica Amministrazione deve avvenire in forma scritta;
e) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
f) i documenti riguardanti l'attività di impresa siano archiviati e conservati, a cura della funzione aziendale competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
g) qualora il servizio di archiviazione e/o conservazione dei documenti sia svolto, per conto della Società, da un soggetto ad essa estraneo, il servizio deve essere regolato da un contratto nel quale si preveda, tra l'altro, che il soggetto che presta il servizio alla Società rispetti specifiche procedure di controllo idonee a non permettere la modificazione successiva dei documenti archiviati, se non con apposita evidenza;
h) sia garantito il controllo dei flussi finanziari aziendali ed in particolare dei flussi relativi alle fatture passive;
i) l'accesso ai documenti già archiviati, di cui alle due lettere precedenti, sia sempre motivato e consentito solo alle persone autorizzate in base alle norme interne, al Collegio Sindacale, al revisore dei conti ed all'Organismo di Vigilanza;
j) non siano corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrua rispetto alle prestazioni rese alla Società e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
k) la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea
l) fermo il rispetto del D.lgs. 231/07 in materia di antiriciclaggio, nessun tipo di pagamento può esser effettuato in contanti o in natura**,** al di fuori dei pagamenti di modico valore ed ove – per ragioni concrete – non sia possibile provvedere tramite canali bancari o attraverso titoli non trasferibili;
m) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle attività di pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

Nell'ambito dei suddetti comportamenti, è comunque fatto divieto, in particolare, di:

- effettuare prestazioni in favore di outsourcer, consulenti, partner, collaboratori e terzi in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, o in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- effettuare elargizioni in denaro o accordare indebiti vantaggi di qualsiasi natura - anche a favore di terzi collegati - (ad esempio la promessa di assunzione) a funzionari pubblici.

In tal senso l'organizzazione è dotata di un sistema di protocollazione digitale di tutta la documentazione aziendali.

PARTE SPECIALE A – Reati contro la pubblica amministrazione

1. REATI

Si riportano, di seguito, le rubriche dei reati contro la Pubblica Amministrazione presi in considerazione dal D.lgs. 231/01.

- *Malversazione a danno dello Stato* (art. 316-*bis* c.p.);
- *Indebita percezione di erogazioni a danno dello Stato* (art.316-*ter* c.p.);
- *Truffa a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare* (art. 640 c.p., 2° comma, n. 1);
- *Truffa aggravata per il conseguimento di erogazioni pubbliche* (art. 640-*bis* c.p.);
- *Frode informatica* (art. 640-*ter* c.p.);
- *Corruzione per un atto d'ufficio* (art. 318 c.p. - art. 321 c.p.);
- *Istigazione alla corruzione* (art. 322 c.p.);
- *Concussione* (art. 317 c.p.);
- *Corruzione per un atto contrario ai doveri di ufficio* (art. 319 c.p. - art. 319-*bis* c.p. - art. 321 c.p.);
- *Corruzione in atti giudiziari* (art. 319-*ter* c.p., 2° comma - art. 321 c.p.);
- *Corruzione di persona incaricata di un pubblico servizio* (art. 320 c.p.);
- *Concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri* (art. 322-*bis* c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

I reati qui considerati hanno come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione.

Per "*Pubblica Amministrazione*" si intendono tutti quei soggetti, pubblici o privati, che svolgono una funzione pubblica o un pubblico servizio. Tale categoria di reati comporta necessariamente un contatto o un rapporto con soggetti appartenenti alla Pubblica Amministrazione, che possono essere distinti in pubblici ufficiali o incaricati di pubblico servizio.

Il "*pubblico ufficiale*" è colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa e può formare o manifestare la volontà della pubblica amministrazione ovvero esercitare poteri autoritativi o certificativi.

A titolo esemplificativo e non esaustivo si considerano Pubblici Ufficiali i membri delle amministrazioni statali e territoriali, i membri delle amministrazioni sovranazionali (ad esempio, dell'Unione Europea), i NAS, i membri delle Autorità di Vigilanza, i membri delle Forze dell'Ordine e della Guardia di Finanza, i membri delle Camere di Commercio, gli amministratori di enti pubblici economici, i membri delle Commissioni Edilizie, i Giudici, gli Ufficiali Giudiziari, gli organi ausiliari dell'Amministrazione della Giustizia (ad esempio, i curatori fallimentari).

L'"*incaricato di un pubblico servizio"* è invece colui il quale a qualunque titolo presta un pubblico servizio.

A norma dell'art. 358 c.p. "*per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale"*.

A titolo esemplificativo e non esaustivo si considerano incaricati di pubblico servizio i dipendenti del SSN, gli addetti all'ufficio cassa di un Ente pubblico, i dipendenti di Enti Ospedalieri, dell'ASL, dell'INAL, dell'INPS, i dipendenti di Aziende Energetiche Municipali; i dipendenti di Uffici Postali ed Uffici Doganali; i membri dei Consigli Comunali, i dipendenti delle Ferrovie dello Stato e della Società Autostrade.

Sulla scorta della documentazione raccolta a riguardo della Società, nell'ambito delle

attività che:

- implicano rapporti con pubblici ufficiali, incaricati di pubblico servizio, organi ispettivi, enti pubblici erogatori di contributi e finanziamenti agevolati, enti pubblici e soggetti incaricati di pubblico servizio titolari di poteri autorizzativi, concessori, abilitativi, certificativi o regolatori;
- comportano la partecipazione a pubbliche gare o a trattative con enti pubblici per l'affidamento di lavori in appalto o in concessione, in riferimento alle procedure di selezione, di autorizzazione del subappalto, di gestione dell'eventuale contenzioso con il committente, di collaudo delle opere eseguite o di controllo di conformità del prodotto rispetto alle previsioni di contratti, disciplinari o capitolati;

sono individuate, presso la Società, le operazioni a rischio evidenziate nella *Check List* allegata, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui agli artt. 24 e 25 del D.lgs. 231/01.
La Società partecipa frequentemente a gare d'appalto indette dalle pubbliche amministrazioni, per la fornitura e posa in opera di arredamenti contract.
Beneficia inoltre dei contributi pubblici legati a progetti di formazione e consulenza basati sull'utilizzo di fondi messi a disposizione dalla Regione, dal Fondo Sociale Europeo e da Fondimpresa, e partecipa quindi alle procedure per l'ottenimento di tali erogazioni.
Per l'adempimento alle normative in materia di ambiente e sicurezza, anche in funzione della certificazione secondo le norme UNI EN ISO 14001:2004, l'azienda richiede ad enti pubblici locali il rilascio di autorizzazioni allo scarico, alle emissioni in atmosfera ed allo svolgimento di altre attività necessarie per la propria produzione.
La Società intrattiene altresì rapporti con l'amministrazione finanziaria e, in caso di verifiche o ispezioni, con le rilevanti pubbliche autorità.
Talvolta, adotta politiche marketing e di omaggistica ai clienti che vanno regolate per i casi in cui i medesimi riguardino in via incidentale soggetti facenti parte della Pubblica Amministrazione.
Alla luce di quanto sopra e dell'individuazione delle attività sensibili relative alla presente Sezione Speciale, si ritiene opportuno predisporre apposite modalità di comportamento e controllo a riguardo di:

i) processo commerciale contract (legato a gare d'appalto pubbliche);
ii) gestione procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici regionali, nazionali o comunitari, e successivo impiego dei fondi ottenuti.
iii) gestione dei rapporti occasionali con l'amministrazione finanziaria e le autorità di vigilanza e controllo;
iv) marketing ed omaggistica a clienti;
v) gestione affari legali ed attività giudiziale e stragiudiziale;
vi) affidamento incarichi e responsabilità a consulenti esterni.

3. PRINCIPI PROCEDURALI SPECIFICI

Per tutte le operazioni a rischio che concernono le attività sensibili individuate nella presente Parte Speciale, va individuato un responsabile interno per l'attuazione dell'operazione, che corrisponde, salvo diversa indicazione, al Controllo Interno.
Il responsabile interno:

- può chiedere informazioni e chiarimenti a tutte le funzioni aziendali, alle unità operative o ai singoli soggetti che si occupano o si sono occupati dell'operazione a rischio;
- informa periodicamente l'Organismo di Vigilanza dei fatti rilevanti relativi alle

operazioni a rischio della propria funzione;
- informa tempestivamente l'Organismo di Vigilanza di qualunque criticità o conflitto di interessi sorto nell'ambito dei rapporti tra la propria funzione e la Pubblica Amministrazione.

Misure per la prevenzione

E' fatto espresso divieto a carico degli esponenti aziendali, a carico dei collaboratori esterni e Partner di:

_ effettuare elargizioni in denaro a pubblici funzionari

_ accordare altri vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione

_ riconoscere compensi a collaboratori esterni che non trovino riscontro al tipo di incarico da svolgere e alle prassi vigenti in ambito locale

_ distribuire omaggi e regali al di fuori delle prassi aziendali

_presentare dichiarazioni non veritiere a organismi pubblici

_ destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi e finanziamenti per scopi diversi da quelli cui erano destinati.

Partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici

Con riferimento a tale area, le procedure devono prevedere che:

- il responsabile interno per l'attuazione dell'operazione verifichi che le dichiarazioni e la documentazione presentata al fine di ottenere il finanziamento siano complete e rappresentino la reale situazione economica, patrimoniale e finanziaria della Società;
- l'impiego delle risorse finanziarie ottenute come contributo, sovvenzione o finanziamento pubblico sia destinato esclusivamente alle iniziative e al conseguimento delle finalità per le quali il finanziamento è stato richiesto e ottenuto;
- l'impiego di tali risorse sia sempre motivato dal soggetto richiedente, che ne deve attestare la coerenza con le finalità per le quali il finanziamento è stato richiesto e ottenuto.

In tal senso l'organizzazione ha definito dei processi di approvazione e di controllo della documentazione presentata e si affida a società accreditate dalla regione per la gestione dei contributi.

Partecipazione a procedure di gara indette da enti pubblici italiani o stranieri

Con riferimento a tale area le procedure devono prevedere che:

- sia verificata la corretta applicazione della procedura di partecipazione ai bandi, sia con riferimento alla fase di ricezione dell'informazione circa la natura del bando cui si vorrà partecipare anche in forma associata (ovvero il modo con cui si è venuti a conoscenza del bando), sia con riferimento alla valutazione del bando stesso, alla sua approvazione, sia alla predisposizione e spedizione della documentazione all'ente (o alla capofila) che indice il relativo bando;
- sia verificata l'esistenza di eventuali conflitti di interessi, inerenti anche la possibilità di partecipare al bando;
- vengano effettuati i controlli sulla documentazione attestante l'esistenza di condizioni essenziali per partecipare ai bandi sia direttamente che tramite raggruppamenti temporanei di imprese;
- nel caso di ATI o RTI, si effettuerà il controllo sulla sussistenza dei requisiti di onorabilità e professionalità dei partner della Società;
- si proceda alla tracciabilità e verificabilità *ex post* delle transazioni fatte con la

Pubblica Amministrazione tramite adeguati supporti documentali / informativi;
- i partner, i collaboratori ed i consulenti che possono eventualmente partecipare al bando o che richiedono la partecipazione della Società, devono essere scelti e valutati con metodi trasparenti e secondo specifica procedura aziendale;
- siano monitorati i poteri anche con riferimento alla verifica delle firme autorizzative per i bandi vinti e per quelli a cui si partecipa.

In tal senso esiste una procedura derl sistema qualità legata all'area contract che specifica tutti i passi operativi e autorizzativi

Gestione dei rapporti occasionali con l'amministrazione finanziaria e le autorità di vigilanza e di controllo (ad esempio, in caso di ispezioni)

Con riferimento a tale area di rischio, le procedure devono prevedere che:
- durante eventuali ispezioni giudiziarie, tributarie e amministrative e quelle poste in essere dalle Attività di Vigilanza di settore (quali ad esempio quelle preposte al rispetto della normativa sulla sicurezza, alle verifiche tributarie, INPS), deve essere individuato in ambito aziendale un responsabile, incaricato di assicurare il coordinamento tra gli addetti delle diverse unità aziendali, ai fini del corretto espletamento da parte di questi ultimi delle attività di propria competenza e nell'ottica della massima collaborazione e trasparenza nei confronti dell'Autorità;
- tale responsabile ha inoltre il compito di assicurare il coordinamento tra i diversi uffici aziendali competenti ed i funzionari delle Autorità, ai fini dell'acquisizione da parte di questi ultimi degli elementi richiesti;
- di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali;
- il responsabile incaricato provvede a stendere un'apposita informativa sull'indagine avviata dall'Autorità, che deve essere periodicamente aggiornata in relazione agli sviluppi dell'indagine stessa ed al suo esito;
- tale informativa deve essere inviata all'Organismo di Vigilanza, nonché agli altri uffici aziendali competenti in relazione alla materia trattata.
- La figura di riferimento è il Controllo Interno in collaborazione con il Responsabile Amministrativo

Marketing ed omaggistica a enti/funzionari pubblici

E' fatto divieto di distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, vale a dire, ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, o comunque rivolta ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale.

In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda.

Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore, o perché volti a promuovere la *brand image* della Società.

Tutti i regali offerti eccedenti il modico valore devono essere documentati in modo idoneo, per consentire all'Organismo di Vigilanza di effettuare verifiche al riguardo. Verrà predisposta a cura dell'area commerciale una lista degli enti/funzionari a cui si intende mandare un omaggio/regalo. Questa dovrà indicare almeno, l'ente/azienda, il referente del cliente, la natura del rapporto e il valore dell'omaggio/regalo. Questa lista sarà verificata e convalidata dall'Organismo di Vigilanza con apposita firma di approvazione al fine di verificare la presenza di enti/funzionari pubblici. E' comunque vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei

paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda.
Qualora la Società sponsorizzi o comunque contribuisca economicamente alla realizzazione di eventi indetti dalla Pubblica Amministrazione, l'importo sponsorizzato od erogato dalla Società dovrà mantenersi entro i limiti del modico valore.
Il responsabile della funzione si assicurerà che l'erogazione venga effettuata in favore dell'ente organizzatore e non di soggetti persone fisiche appartenenti allo stesso.
Per ogni sponsorizzazione effettuata dalla Società deve essere redatto un breve resoconto scritto contenente quantomeno il nominativo dell'ente beneficiario, la natura dell'elargizione, le ragioni che hanno sostenuto la valutazione ad accoglierla ed il valore complessivo della stessa.

Gestione affari legali ed attività giudiziale e stragiudiziale;
La gestione degli affari legali dell'azienda è gestita dal Responsabile Amministrativo con specifica approvazione inerente ad azioni o documentazione legale da parte dell'Amministratore Unico. Inoltre per questa attività si affida alla professionalità di studi legali. Tutta la gestione di queste attività è specificatamente riportata e gestita in un file excell a cura del responsabile amm.vo.

Affidamento incarichi e responsabilità a consulenti esterni.
L'affidamento di incarichi e responsabilità a consulenti esterni è definito secondo un rapporto contrattuale, che prevede ambito di intervento del consulente e responsabilità ad esso delegate; per l'adempimento di tali attività viene stabilito un valore contrattuale che trova riscontro nella fatturazione del consulente stesso.
Tutte le attività eseguite da personale esterno devono essere svolte secondo i principi sopra stabiliti, con un comportamento del tutto assimilabile a quello del personale dipendente.
All'interno dell'azienda ci sono diversi referenti che curano in base all'ambito di interesse il rapporto con i consulenti di riferimento.
Tutti i consulenti esterni sono assoggettati a un contratto definito in gestione all'area amministrativa.
Le delibere di nomina dei membri degli organismi societari devono sempre dar conto, seppur sinteticamente, delle ragioni che hanno condotto alla scelta di quel determinato soggetto.

4. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.
La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.

PARTE SPECIALE B – Falsità in monete, in carte di pubblico credito e in valori di bollo

1. REATI

Si riportano, di seguito, le rubriche di tutti i reati presi in considerazione dal D.lgs. 231/01.

- *Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate* (art. 453 c.p.);
- *Alterazione di monete* (art. 454 c.p.);
- *Spendita e introduzione nello Stato, senza concerto, di monete falsificate* (art. 455 c.p.);
- *Spendita di monete falsificate ricevute in buona fede* (art. 457 c.p.);
- *Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati* (art. 459 c.p.);
- *Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo* (art. 460 c.p.);
- *Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata* (art. 461 c.p.);
- *Uso di valori di bollo contraffatti o alterati* (art. 464 c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla base dell'analisi dell'attività della Società e dei suoi processi, si ritiene che non vi siano operazioni a rischio.

PARTE SPECIALE C – Reati societari

1. REATI

Si riportano, di seguito, le rubriche di tutti i reati presi in considerazione dal D.lgs. 231/01.

- *False comunicazioni sociali* (art. 2621 c.c.);
- *False comunicazioni sociali in danno dei soci o dei creditori* (art. 2622 c.c.);
- *Falsità nelle relazioni o nelle comunicazioni delle società di revisione* (art. 2624 c.c.);
- *Impedito controllo* (art. 2625 c.c.);
- *Indebita restituzione dei conferimenti* (art. 2626 c.c.);
- *Illegale ripartizione di utili e riserve* (art. 2627 c.c.);
- *Illecite operazioni sulle azioni o quote sociali o della società controllante* (art. 2628 c.c.);
- *Operazioni in pregiudizio ai creditori* (art. 2629 c.c.);
- *Omessa comunicazione del conflitto di interessi* (art. 2629-*bis* c.c.)
- *Formazione fittizia del capitale sociale* (art. 2632 c.c.);
- *Indebita ripartizione dei beni sociali da parte dei liquidatori* (art. 2633 c.c.);
- *Illecita influenza sull'assemblea* (art. 2636 c.c.);
- *Aggiotaggio* (art. 2637 c.c.);
- *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza* (art. 2638 c.c.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla scorta delle informazioni assunte a riguardo della Società, nell'ambito:

- delle attività di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti di impresa;
- delle attività o delle condotte tenute in relazione allo svolgimento dei controlli previsti dalla legge, dalle procedure contemplate dal sistema di controllo interno, dal Modello o dalle procedure per la sua attuazione, idonee a ostacolare i controlli sull'attività o sulla rappresentazione contabile dell'attività di impresa;
- delle situazioni o attività in potenziale conflitto di interessi e, in genere, potenzialmente pregiudizievoli per i soci, i creditori e i terzi,

sono individuate, presso la Società quali operazioni a rischio nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 25-*ter* del Decreto le ordinarie attività gestionali della Società riferibili alla tenuta della contabilità, alla redazione del bilancio ed alla *corporate governance*.

Si ritiene quindi opportuno predisporre apposite procedure a riguardo:

i) della redazione del bilancio;
ii) della tenuta della contabilità;
iii) della gestione, archiviazione e conservazione delle informazioni;
iv) ai rapporti con il collegio sindacale e con il revisore dei conti;
v) alla gestione delle risorse finanziarie;
vi) ai rapporti con le autorità di vigilanza.

3. PRINCIPI PROCEDURALI SPECIFICI

<u>Redazione del bilancio e delle altre scritture contabili</u>

La Società si adopera per disporre di un sistema amministrativo – contabile affidabile, al fine di rappresentare correttamente i fatti di gestione nell'interesse dei soci, dei creditori e dei terzi.

Le rilevazioni contabili devono pertanto basarsi su informazioni precise, esaustive,

verificabili e riflettere la natura e la tipologia dell'operazione cui si riferiscono, nel rispetto dei vincoli esterni (disposizioni legislative e regolamentari e principi contabili), nonché delle politiche, dei piani e delle procedure interne: le stesse, inoltre, devono essere corredate della relativa documentazione di supporto, necessaria a consentire analisi e verifiche obiettive dei dati in esse contenuti.
Le suddette rilevazioni contabili devono:

- consentire la ricostruzione della situazione economica, patrimoniale e finanziaria della Società, sia per scopi interni (report), che nei rapporti con i terzi (bilanci, documenti informativi ecc.);
- fornire gli strumenti per identificare, prevenire e gestire, nei limiti del possibile, rischi di natura finanziaria o frodi a danno dei creditori o dei terzi potenzialmente interessati ad entrare in contatto con la Società;
- permettere l'effettuazione di controlli volti a garantire la salvaguardia del valore delle attività e la protezione dalle perdite.

Il personale delle funzioni interessate è tenuto ad operare affinché i fatti di gestione siano rappresentati correttamente e tempestivamente, in modo che il sistema amministrativo – contabile possa conseguire tutte le finalità sopra descritte.
La Società, nello svolgimento dell'attività di formazione del bilancio e delle altre comunicazioni sociali, si ispira ai seguenti principi e criteri operativi:

- l'adozione di procedure contabili costantemente aggiornate che prevedano una chiara elencazione dei dati e delle notizie che ciascuna funzione aziendale deve fornire alla funzione che cura la predisposizione del bilancio e dei documenti contabili, con relativa tempistica di consegna;
- la trasmissione dei dati e delle informazioni alla funzione responsabile deve avvenire attraverso un supporto che consenta di tenere tracciati i vari passaggi: copia della trasmissione deve essere conservata ed archiviata, a cura delle funzioni coinvolte;
- i soggetti che forniscono i dati alla funzione incaricata dell'amministrazione e della finanza e/o ad eventuali soggetti esterni che li affianchino nell'attività, devono essere in grado di attestare la veridicità, la completezza e la coerenza delle informazioni trasmesse, mediante esplicita dichiarazione debitamente sottoscritta, ed all'occorrenza devono fornire le relative evidenze documentali;
- qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile, chi ne sia a conoscenza informi senza indugio l'Organismo di Vigilanza;
- la bozza di bilancio e gli altri documenti contabili siano messi a disposizione degli Amministratori, dei Sindaci e del revisore dei conti con ragionevole anticipo rispetto alla riunione dell'Amministratore Unico per l'approvazione dello stesso.

Vista l'importanza di tale attività l'organizzazione ha definito una procedura specifica sulla veridicità delle voci di bilancio e una sulla valorizzazione e gestione magazzino

<u>Tenuta della contabilità</u>

Ogni operazione aziendale che si riflette sul sistema contabile, inclusa la mera attività di inserimento dei dati, deve avvenire sulla scorta di adeguata evidenza documentale.
Si considera adeguato ogni valido ed utile supporto documentale atto a fornire tutti gli elementi, dati ed informazioni necessari alla puntuale ricostruzione, all'occorrenza, dell'operazione e dei motivi che le hanno dato luogo.
Il supporto documentale deve essere adeguato alla complessità dell'operazione e deve consentire un agevole controllo.
Le movimentazioni finanziarie attive e passive della Società devono sempre essere

riconducibili ad eventi certi, documentati e strettamente inerenti.
In particolare, ogni documento contabile è soggetto a protocollazione specifica nell'ambito dell'esercizio in essere, ed è univocamente riconducibile alla scrittura contabile relativa. Nello specifico esistono i seguenti tipi di protocollazione:

- fatture attive
- fatture passive
- contabili
- liste pagamenti automatici

Inoltre tutti i documenti vengono scansionati ed archiviati all'interno di database elettronici.
Attraverso questa specifica modalità De Rosso Spa garantisce la piena rintracciabilità tra dato e documento giustificativo a supporto.

Gestione, documentazione, archiviazione e conservazione delle informazioni

In merito all'archiviazione di tutti i documenti contabili, gestionali e amministrativi, si rimanda al Documento di Programmazione della Sicurezza dei dati previsto dalla legge 196 del 30 giugno 2006, nel quale l'azienda ha specificato le modalità autorizzative, di gestione e archiviazione dei dati e dei documenti aziendali sia su supporto cartaceo che informatico. In esso sono inoltre espressamente richiamate le responsabilità e gli incarichi attinenti.
Tale documento garantisce il rispetto dei seguenti principi:

- i documenti riguardanti la formazione delle decisioni che governano le operazioni delle attività sensibili indicate nella presente parte speciale, nonché quelli che danno attuazione alle decisioni, siano archiviati e conservati a cura della funzione competente per l'operazione;
- l'accesso ai documenti già archiviati sia consentito solo alle persone autorizzate in base alle procedure operative aziendali, al collegio sindacale, al revisore dei conti ed all'Organismo di Vigilanza;
- la trasmissione delle informazioni nell'ambito della Società sia consentita esclusivamente alle persone autorizzate e avvenga solo attraverso mezzi tecnici che garantiscano la sicurezza della trasmissione e il rispetto del principio di riservatezza delle informazioni.

IL DPS è periodicamente soggetto a revisione e aggiormanento a cura della Direzione dei sistemi informativi. Le modifiche al documento stesso verranno comunicate al OdV.

Rapporti con il collegio sindacale e con il revisore dei conti

Le procedure prevedono che:

- per ciascuna funzione sia individuato un responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al collegio sindacale ed al revisore dei conti;
- il responsabile della funzione a cui è richiesta un'informazione dal collegio sindacale o dal revisore dei conti verifichi la completezza, inerenza e correttezza della documentazione trasmessa;
- le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal collegio sindacale e dal revisore dei conti, siano documentate e conservate a cura del responsabile di funzione;
- tutti i documenti relativi ad operazioni all'ordine del giorno delle riunioni dell'assemblea o dell'Amministratore Unico o, comunque, relativi a operazioni sulle quali il collegio sindacale debba esprimere parere siano messi a disposizione di quest'ultimo con ragionevole anticipo rispetto alla data della riunione;

- sia garantito al revisore dei conti il libero accesso alla contabilità aziendale per un corretto svolgimento dell'incarico.

Gestione delle risorse finanziarie

La procedura deve prevedere quanto segue:

a) non vi sia identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
b) siano stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali ed alle responsabilità organizzative affidate alle singole persone;
c) il superamento dei limiti di cui al punto precedente possa avvenire solo nel rispetto delle vigenti procedure di autorizzazione e previa adeguata motivazione;
d) le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie debbano avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile. Il processo decisionale deve essere verificabile;
e) l'impiego di risorse finanziarie sia motivato dal soggetto richiedente, che ne attesta la congruità:
    i) in caso di operazioni ordinarie, se comprese entro la soglia quantitativa stabilita, la motivazione può essere limitata al riferimento alla classe o tipologia di spesa alla quale appartiene l'operazione;
    ii) in caso di operazioni diverse dalle ordinarie o eccedenti la soglia quantitativa stabilita, la motivazione deve essere analitica.

Tutte le operazioni finanziarie elettroniche vengono predisposte dalle figure operative dell'amministrazione e quindi approvate con firma elettronica a cura del Responsabile Amministrativo

Rapporti con le autorità di vigilanza

Nella predisposizione di comunicazioni alle Autorità pubbliche di Vigilanza e nella gestione dei rapporti con le stesse, la Società pone particolare attenzione al rispetto:

- delle disposizioni di legge e di regolamento concernenti le comunicazioni, periodiche e non, da inviare a tali Autorità;
- degli obblighi di trasmissione alle Autorità suddette dei dati e documenti previsti dalle norme in vigore, ovvero specificamente richiesti dalle predetta Autorità (ad esempio bilanci, verbali delle riunioni degli organi societari);
- degli obblighi di collaborazione da fornire nel corso di eventuali accertamenti ispettivi.

Inoltre, la Società adotta idonee procedure per la gestione ed il controllo delle comunicazioni alle Autorità pubbliche di Vigilanza.

Le procedure da osservare, per garantire il rispetto di quanto espresso al precedente punto, devono essere conformi ai seguenti criteri:

1) deve essere data attuazione a tutti gli interventi di natura organizzativo – contabile necessari a garantire che il processo di acquisizione ed elaborazione di dati ed informazioni assicuri la corretta e completa predisposizione delle comunicazioni ed il loro puntuale invio alle Autorità pubbliche di Vigilanza, secondo le modalità ed i tempi previsti dalla normativa di settore;
2) deve essere data adeguata evidenza delle procedure seguite in attuazione di quanto richiesto al precedente punto, con particolare riferimento all'individuazione dei responsabili che hanno proceduto alla raccolta ed all'elaborazione dei dati e delle informazioni ivi previste;

3) deve essere assicurata, in caso di accertamenti ispettivi svolti dalle Autorità in questione, una adeguata e trasparente collaborazione da parte delle unità aziendali competenti e di tutti i dipendenti;
4) per il caso di ispezioni disposte dalle Autorità, si fa integrale richiamo alla relativa procedura riportata nella Parte Speciale A.

4. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.
La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.
In maniera specifica, inoltre, OdV deve:
_ esaminare eventuali segnalazioni specifiche provenienti dagli organismi di controllo o da qualsiasi dipendente e disposizione degli accertamenti necessari
_ organizzazione di una riunione con il Collegio Sindacale e il Responsabile Amm.vo prima della seduta di esame di bilancio con stesura di un verbale finale

PARTE SPECIALE D – Delitti con finalità di terrorismo o di eversione dell'ordine democratico

1. REATI

L'art. 25 *quater* del D.lgs. 231/02 prende in considerazione i delitti aventi finalità di trerrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali ed i delitti posti in essere in violazione di quanto previsto dall'art. 2 della Convenzione internazionale per la repressione del finanziamento al terrorismo fatta a New York il 9 dicembre 1999.

All'interno di tali fattispecie si possono includere i seguenti reati:

- Associazione con finalità di terrorismo anche internazionale o di eversione
- dell'ordine democratico (Art. 270 bis c.p.);
- Assistenza agli associati (Art. 270 ter c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (Art. 270 quater c.p.)
- Addestramento con finalità di terrorismo anche internazionale (Art. 270 quinquies c.p.);
- Condotte con finalità di terrorismo (Art. 270 sexies c.p.)
- Attentato con finalità terroristiche o di eversione (Art. 280 c.p.)
- Atto di terrorismo con ordigni micidiali o esplosivi (Art. 280 bis c.p.)
- Sequestro di persona a scopo di terrorismo o di eversione (Art. 289 bis c.p.)
- Istigazione a commettere alcuno dei delitti preveduti dai capi primo e secondo del titolo (Art. 302 c.p.)

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società non intrattiene rapporti con Paesi a rischio terroristico.

Si ritiene, quindi, che non siano ravvisabili rischi specifici con riferimento alla presente Parte Speciale.

PARTE SPECIALE E – Delitti contro la personalità individuale

1. REATI

Si riportano, di seguito, le rubriche dei reati contro la personalità individuale presi in considerazione dal D.lgs. 231/01:

- *Pratiche di mutilazione degli organi genitali femminili (*art. 583-*bis* c.p.).
- *Riduzione in schiavitù* (art. 600 c.p.);
- *Prostituzione minorile* (art. 600-*bis* c.p.);
- *Pornografia minorile* (art. 600-*ter* c.p., 1° e 2° comma);
- *Detenzione di materiale pornografico* (art. 600-*quater* c.p.);
- *Iniziative turistiche volte allo sfruttamento della prostituzione minorile* (art. 600-*quinquies* c.p.);
- *Tratta e commercio di schiavi* (art. 601 c.p.);
- *Alienazione e acquisto di schiavi* (art. 602 c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società non intrattiene rapporti con soggetti terzi che operano nei Paesi a bassa protezione di diritti individuali.

Si ritiene, quindi, che non siano ravvisabili rischi specifici con riferimento alla presente Parte Speciale.

PARTE SPECIALE F – Abusi di mercato

1. REATI

Si riportano, di seguito, le rubriche dei reati contro la personalità individuale presi in considerazione dal D.lgs. 231/01:

- *Abuso di informazioni privilegiate* (art. 184 TUF);
- *Manipolazione del mercato* (art. 185 TUF).

Il TUF, come modificato dalla legge n. 62 del 2005, prevede all'art. 187-*quinquies* la responsabilità amministrativa degli enti per gli illeciti amministrativi relativi agli abusi di mercato, di seguito elencati.

- *Abuso di informazioni privilegiate* (art. 187-*bis* TUF);
- *Manipolazione del mercato* (art. 187-*ter* TUF).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società non svolge attività interente agli strumenti finanziari di cui all'art. 180 lett. a) e b) del TUF.

Si ritiene, quindi, che non siano ravvisabili rischi specifici con riferimento alla presente Parte Speciale.

PARTE SPECIALE G – Reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

1. REATI

Si riportano, di seguito, le rubriche dei reati presi in considerazione dall'art. 25 - *septies* del D.lgs. 231/01

- *Omicidio colposo commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 589 c.p.);*
- *Lesioni gravi e gravissime colpose commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 590, terzo comma, c.p.)*

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Sulla scorta della documentazione raccolta e dell'analisi dei processi della Società, nell'ambito:

- di tutti i settori di attività della Società e delle sue unità produttive;
- di tutte le attività e delle unità produttive alle quali siano addetti sia lavoratori dipendenti della Società sia i lavoratori dipendenti di imprese esterne e/o lavoratori autonomi, a cui la Società affida lavori in appalto e/o in sub appalto;

sono individuati i fattori di rischio riportati nella Check list allegata.

Si rileva, peraltro, che la Società non presenta elementi di criticità ulteriori rispetto a quelli ineliminabili connessi all'ordinaria attività imprenditoriale che costituisce l'oggetto sociale.

Vista l'estrema sensibilità della Società per la sicurezza sul luogo di lavoro, si raccomanda a tutti i Destinatari di attenersi con la massima scrupolosità alle disposizioni di legge ed ai principi che seguono.

3. PRINCIPI GENERALI PER LA REDAZIONE DELLE PROCEDURE PER LA PREVENZIONE DEI REATI DI OMICIDIO E LESIONI COLPOSE COMMESSE IN VIOLAZIONE DELLE NORME A TUTELA DELLA SALUTE, DELLA SICUREZZA , DELL'IGIENE DEI LUOGHI DI LAVORO

Nell'ambito della fattispecie di reato introdotta con l'art. 9 della legge 3 agosto 2007, n. 123 recante "*Misure in tema di tutela della salute e della sicurezza sul lavoro* le disposizioni di cui al D.lgs. 231/01 sono state integrate con la previsione normativa di cui all'art. 25 *septies* del D.lgs. 231/01 relativo al reato di "*omicidio colposo e lesioni colpose gravi o gravissime, commessi con la violazione delle norme infortunistiche e sulla tutela dell'igiene e della sicurezza sul lavoro*".

Al fine di prevenire la commissione di tali reati, è necessario:

- osservare tutte le leggi ed i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle disposizioni legislative in materia di sicurezza e salute dei lavoratori contenute nel D.lgs. 9 aprile 2008, n. 81 (Testo Unico sulla Sicurezza);
- gestire qualsiasi rapporto inerente la normativa per la sicurezza sulla base di criteri di massima correttezza e trasparenza.

Nell'ambito dei suddetti comportamenti:

- la Società gestisce le aree di attività riguardanti la pianificazione, l'organizzazione e la revisione del servizio di prevenzione e protezione dai rischi in modo unitario, individuando il responsabile per ogni operazione o pluralità di operazioni;
- gli incarichi eventualmente conferiti in materia di sicurezza sui luoghi di lavoro vengono redatti per iscritto, conservati e protocollati unitamente alle qualifiche dell'incaricato;
- le eventuali deleghe di funzioni da parte del datore di lavoro dovranno risultare da atto scritto recante data certa, dovranno essere conferite a soggetti che posseggano tutti i requisiti di professionalità ed esperienza

richiesti dalla specifica natura delle funzioni delegate, dovranno attribuire al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate, dovranno attribuire al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate e la delega dovrà essere accettata per iscritto.

Il Modello deve essere integrato con il sistema degli adempimenti aziendali nascenti dagli obblighi di prevenzione e protezione imposti dall'ordinamento legislativo e con le procedure interne nascenti dalle esigenze di gestione della sicurezza sul lavoro.

A tal fine, il soggetto nominato Responsabile dei servizi di prevenzione e protezione provvederà, d'intesa con il delegato alla sicurezza e l'Organismo di Vigilanza, ad armonizzare le attività già svolte dalla Società in materia di gestione della sicurezza con quanto previsto dal D.lgs. 231/01 evitando, per quanto possibile, duplicazioni.

Nell'ambito di un sistema integrato di controllo in materia di sicurezza sul lavoro, il Responsabile dei servizi di prevenzione e protezione assumerà la gestione del sistema di sicurezza e svolgerà attività di coordinamento tra i delegati alla sicurezza e le diverse funzioni nominate a diverso titolo (ASPP, Addetto al Servizio di Prevenzione e Prevenzione, Preposto, RLS). Agli ASPP è delegato il controllo tecnico – operativo o di primo grado, mentre l'Organismo di Vigilanza, interagendo con il delegato alla sicurezza, viene incaricato del controllo sull'efficienza ed efficacia delle procedure rilevanti ai sensi del D.lgs. 231/01 o di secondo grado.

4. PRINCIPI PROCEDURALI SPECIFICI

In ogni caso, le procedure dovranno riferirsi a tutti gli obblighi giuridici relativi:

i) al rispetto degli standard tecnico – strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
ii) alle attività di valutazione dei rischi, di predisposizione delle misure di prevenzione e protezione conseguenti;
iii) alle attività di natura organizzativa, quali le emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentati dei lavoratori per la sicurezza;
iv) alle attività di sorveglianza sanitaria;
v) alle attività di informazione e formazione dei lavoratori;
vi) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
vii) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
viii) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Le procedure debbono prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra esposte.

Le procedure dovranno assicurare un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

In relazione alle aree e fattori a rischio, vanno previste specifiche procedure in forza delle quali:

a) siano valutati tutti i rischi per la salute e sicurezza;
b) sia programmata la prevenzione, mirata ad un complesso che integri in modo coerente nella prevenzione le condizioni tecniche produttive dell'azienda nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;
c) siano eliminati i rischi e, ove ciò non sia possibile, siano ridotti al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;
d) siano rispettati i principi ergonomici nell'organizzazione del lavoro, nella

concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, in particolare al fine di ridurre gli effetti sulla salute del lavoro monotono e di quello ripetitivo;

e) siano ridotti i rischi alla fonte;
f) sia sostituito ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
g) sia limitato al minimo il numero dei lavoratori che sono, o che possono essere, esposti al rischio;
h) sia limitato l'utilizzo degli agenti chimici, fisici e biologici sui luoghi di lavoro;
i) sia data priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;
j) vi sia il controllo sanitario dei lavoratori;
k) sia allontanato il lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione;
l) siano informati ed adeguatamente formati i lavoratori;
m) siano informati e adeguatamente formati i dirigenti e i preposti;
n) siano informati e adeguatamente formati i rappresentanti dei lavoratori per la sicurezza;
o) siano date istruzioni adeguate ai lavoratori;
p) sia garantita la partecipazione e consultazione dei lavoratori;
q) sia garantita la partecipazione e consultazione dei rappresentanti dei lavoratori per la sicurezza;
r) siano programmate le misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione di codici di condotta e di buone prassi;
s) siano adottate le misure di emergenza da attuare in caso di primo soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;
t) siano usati i segnali di avvertimento e di sicurezza;
u) vi sia la regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti;
v) i soggetti responsabili dell'individuazione, dell'attuazione e del controllo sulle misure relative alla sicurezza, all'igiene e alla salute durante il lavoro dispongano del tempo, delle risorse e dei mezzi necessari per il corretto esercizio delle proprie funzioni.

In tale ambito è stato definito un organigramma aziendale sulla sicurezza e affidato il ruolo di RSPP ad un professionista interno. Il contratto definito con quest'ultimo garantisce inoltre un monitoraggio continuo dell'applicazione del sistema di sicurezza definito e implementato dall'organizzazione. Le attività di monitoraggio del RSPP sono registrate su apposita documentazione.
E' stata inoltre definita e redatta una procura specifica per la gestione della sicurezza in azienda.
E' stato redatto e approvato con data certa il Documento di Valutazione dei Rischi.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.
La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.

PARTE SPECIALE H – Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

1. REATI

Si riportano, di seguito, le rubriche dei reati presi in considerazione dall'art. 25 - *octies* del D.lgs. 231/01

- *Ricettazione (art. 648 c.p.)*
- *Riciclaggio (art. 648-bis c.p.)*
- *Impiego (art. 648-ter c.p.)*

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

In relazione ai reati di cui alla presente sezione, nell'ambito di attività finanziarie o di acquisto o cessione di beni che potenzialmente possano avere ad oggetto denaro, beni o altre utilità di provenienza illecita sono individuate, presso la Società le operazioni a rischio indicate nell'allegata Check List.

Le aree sensibili sono quelle in cui incorre la normale operatività di un'azienda industriale.

Alla luce dell'esame di tale operatività, si è ritenuto di predisporre procedure per

- la gestione della liquidità;
- gestione amministrativa e contabile del cliente;
- il ricevimento delle materie prime negli stabilimenti di produzione;
- l'individuazione di comportamenti sospetti con riferimento ai reati di cui alla presente Parte Speciale.

3. PRINCIPI PROCEDURALI SPECIFICI

<u>Gestione della liquidità</u>

Le procedure adottate dalla Società devono prevedere il rispetto della normativa *pro tempore* in vigore in materia di antiriciclaggio e dei relativi limiti di utilizzo del contante e dei titoli al portatore. Attualmente le procedure dispongono che non vengano effettuati o ricevuti trasferimenti di contanti, libretti di deposito e titoli al portatore per un importo superiore ad Euro 12.500,00, nonché che gli assegni bancari e postali per importi uguali o maggiori ad Euro 12.500,00 rechino l'indicazione del beneficiario e la clausola di non trasferibilità.

Esiste una procedura interna di gestione della cassa tenuta dall'area amm.va.

<u>Gestione della contabilità e dell'amministrazione</u>

Con riferimento all'area in esame, è necessario, sia in fase di inserimento in anagrafica di clienti e fornitori, che successivamente:

- identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da fonte affidabile ed indipendente;
- creare uno specifico dossier clienti e fornitori onde raccogliere e censire le informazioni critiche e significative degli stessi, ovvero a titolo di esempio: il legale rappresentante, la nazione di residenza, il tipo di attività economica svolta, la compagine societaria, eventuali precedenti penali ecc., al fine di poter desumere i requisiti di onorabilità e professionalità delle controparti con le quali la Società opera;
- verificare l'attendibilità commerciale e professionale di fornitori e partner commerciali;
- valutare, anche attraverso dati forniti da fonti esterne, la solvibilità del cliente e definire conseguentemente il limite del credito e le modalità di pagamento;
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti e controparti effettivamente coinvolte

Le anagrafiche clienti e fornitori sono gestite su sistema gestionale con specifiche autorizzazioni di inserimento, modifica e visualizzazione.

Ricevimento delle materie prime negli stabilimenti di produzione

La procedure adottate dalla Società prevedono che il ricevimento delle materie prime negli stabilimenti di produzione possa avvenire solo se la merce è accompagnata da idoneo documento di trasporto; il personale che si occupa del ricevimento della merce è tenuto a non effettuare alcun tipo di pagamento al momento della consegna.

Solamente il personale autorizzato, facente parte dell'ufficio amministrativo, ha la facoltà di effettuare pagamenti alla consegna della merce a fronte di presentazione di regolare fattura diretta; il pagamento in contanti non dovrà mai superare il limite € 12.500,00 ed essere effettuato e registrato direttamente dal responsabile della cassa.

La procedura del sistema qualità definisce specificatamente le modalità documentali e amministrative di controllo della merce al ricevimento

Individuazione di comportamenti sospetti

La Società adotta adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

Segnala a tale personale i principali indici di anomalia connessi all'attività di riciclaggio desumibili dal profilo soggettivo, dal comportamento e dalla dislocazione territoriale del cliente, dal profilo economico – patrimoniale e dalle caratteristiche e finalità dell'operazione richiesta.

In particolare, debbono essere considerati indici di anomalia i casi in cui:

- un cliente, in assenza di plausibili giustificazioni, richiede lo svolgimento di operazioni palesemente non abituali, non giustificati ovvero non proporzionate all'esercizio normale della sua professione o attività;
- un cliente richiede l'esecuzione di operazioni che impiegano disponibilità che appaiono eccessive rispetto al suo profilo economico – patrimoniale;
- il cliente si rifiuta o si mostra ingiustificatamente riluttante a fornire le informazioni occorrenti a dichiarare l'attività esercitata, a presentare documentazione contabile o di altro genere, a segnalare rapporti intrattenuti con altri professionisti, a fornire ogni altra informazione che, in circostanze normali viene acquisita nello svolgimento delle normali attività aziendali;
- il cliente fornisce informazioni palesemente inesatte o incomplete, tali da manifestare l'intento di occultare informazioni essenziali;
- il cliente usa documenti identificativi che sembrano contraffatti;
- il cliente rifiuta di o solleva obiezioni a pagare il prezzo della prestazione con bonifico o assegno bancario;
- le dichiarazioni del cliente in relazione all'operazione del cliente appaiono incongruenti;
- il cliente effettua transazioni con controparti in località inusuali per lo stesso;
- l'operazione appare non economicamente conveniente per il cliente e/o manca un'apparente regione per utilizzare i servizi dell'operatore;
- l'operazione appare eccessivamente complessa o insolita per lo scopo dichiarato;
- il cliente intende regolare il pagamento dell'operazione con una somma notevole di denaro contanti.

Ove alcuni di tali indici di anomalia vengano riscontrati, si dovrà procedere alla tempestiva segnalazione all'Organismo di Vigilanza.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.

La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza..

PARTE SPECIALE I – Reati transnazionali di cui all'art. 10 della legge 16 marzo 2006, n. 146

1. REATI

Si riportano, di seguito, le rubriche dei reati transnazionali presi in considerazione dall'art. 10 della legge 16 marzo 2006, n. 146:

- *Associazione a delinquere* (art. 416 c.p.);
- *Associazione di tipo mafioso* (. art. 416-bis c.p.);
- *Associazione per delinquere finalizzata al contrabbando di tabacchi esteri* (art. 291- *quater* D.p.r. 43/1973);
- *Associazione finalizzata al traffico illecito di sostanze stupefacenti e psicotrope* (art. 74 D.p.r. 309/1990);
- *Disposizioni contro l'immigrazione clandestina* (art. 12, commi 3, 3-*bis*, 3-*ter*, 5 D. Lgs. 286/1998);
- *Intralcio alla giustizia: induzione a non rendere dichiarazioni* (art. 377-*bis* c.p.);
- *Intralcio alla giustizia: favoreggiamento personale* (art. 378 c.p.).

3. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Nell'ambito delle attività che comportano possibili contatti anche indiretti con organizzazioni criminali organizzate, sono individuate presso la Società le operazioni a rischio indicate nella Check List allegata, nello svolgimento o nell'esecuzione delle quali possono essere commessi i reati di cui all'art. 10 della Legge 146/2006.

Per quanto si ritenga che, alla luce dell'attività sociale svolta, il rischio non si presenti particolarmente elevato, la Società ritiene di predisporre idonee procedure per

- valutazione e selezione dei fornitori;
- valutazione della clientela, gestione del credito e concessione di affidamenti;
- rapporti con soggetti coinvolti in procedimenti giudiziari.

3. PRINCIPI PROCEDURALI SPECIFICI

<u>Valutazione, qualifica e selezione dei fornitori di beni e servizi</u>

La procedura deve necessariamente prevedere quanto segue:

a) sia formalizzato il processo di selezione e valutazione del fornitore, nonché della gestione del rapporto con il medesimo;
b) sia individuato per ciascuna fase di selezione, valutazione e gestione del fornitore un responsabile interno e i livelli autorizzativi di formazione e attuazione delle decisioni;
c) siano preventivamente identificati e costantemente aggiornati indici di rischio di reato e di possibili anomalie in relazione a ciascuna categoria di fornitori;
d) per le fasi di selezione e di valutazione del fornitore siano individuati idonei criteri e modalità di scelta del fornitore che garantiscano un processo comparativo degli offerenti. Qualora il processo comparativo non sia possibile o sia giudicato non necessario, la funzione competente lo segnali al livello gerarchico superiore, dando adeguata motivazione;
e) siano stabilite idonee modalità di raccolta e conservazione della documentazione relativa al processo di selezione, valutazione e gestione del fornitore;
f) ogni rapporto con i fornitori sia disciplinato da contratto scritto, sottoscritto esclusivamente dal soggetto dotato di idonei poteri secondo il sistema di deleghe e procure vigente, nel quale sia chiaramente prestabilito il prezzo del bene o della prestazione da ricevere o i criteri per determinarlo;
g) i contratti di approvvigionamento che possano presentare carattere inusuale o anomalo per tipologia o oggetto della richiesta, siano sempre preventivamente valutati e autorizzati dalla direzione generale della Società, informato

l'Organismo di Vigilanza;

h) in caso di dubbio sulla qualifica o sulla permanenza della qualifica in capo al fornitore oppure in caso di sopravvenienza di profili di anomalia nei rapporti con il fornitore o nella tipologia delle richieste da questi avanzate, la commessa sia assegnata o il rapporto sia mantenuto solo previa espressa autorizzazione della direzione generale, informato l'Organismo di Vigilanza;
i) chiunque ne sia a conoscenza, segnali immediatamente all'Organismo di Vigilanza oppure al proprio superiore gerarchico, che riferirà all'Organismo di Vigilanza, eventuali anomalie nelle prestazioni dovute dal fornitore, discordanze significative o ripetute tra materiale o servizio ricevuto rispetto a quanto concordato o particolari richieste avanzate dal fornitore alla Società;
j) nei contratti che regolano i rapporti con i fornitori sia valutata l'opportunità di prevedere apposite clausole che richiamano gli adempimenti e le responsabilità derivanti dal D.lgs. 231/01 e dal rispetto del presente Modello e delle sue parti integranti.

Nel sistema qualità esiste una specifica procedura di selezione e valutazione dei fornitori

<u>Valutazione della clientela, la gestione del credito, la concessione di affidamenti alla clientela, la gestione delle condizioni economico-finanziarie (prezzi e sconti) definite nei contratti con i clienti</u>

La procedura deve prevedere quanto segue:

a) ogni rapporto di cessione di beni o servizi sia disciplinato da contratto scritto, sottoscritto esclusivamente dal soggetto dotato di idonei poteri secondo il sistema di deleghe e procure vigente, nel quale sia chiaramente prestabilito il prezzo del bene o della prestazione da effettuare o i criteri per determinarlo;
b) siano previste modalità e limiti per la concessione di sconti commerciali rispetto al listino prezzi della Società, anche tenendo conto delle oscillazioni dei prezzi di mercato;
c) non vi sia identità soggettiva fra coloro che propongono, coloro che autorizzano la concessione del credito al cliente, coloro che devono dare evidenza contabile dell'operazione e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
d) siano stabiliti limiti alla concessione di credito alla clientela da parte del responsabile della funzione, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali ed alle responsabilità organizzative affidate; le operazioni che superino la soglia quantitativa siano preventivamente valutate e approvate dall'organismo superiore a quello che cura la funzione;
e) l'affidamento della clientela sia sempre subordinato a una valutazione generale della affidabilità finanziaria e della consistenza patrimoniale del cliente, svolta attraverso la raccolta di informazioni da fonti interne (struttura e organizzazione della Società, protesti, visure ipotecarie e catastali, ecc.) e da fonti esterne, ricorrendo a banche dati ufficiali aggiornate. In caso di rilascio di garanzie personali da parte di terzi a favore dei clienti, siano effettuati accertamenti idonei sul soggetto garante, individuando indici di rischio o anomalia;
f) le operazioni di affidamento della clientela siano documentate a cura della funzione proponente e, una volta approvate, siano registrate nell'anagrafica clienti in conformità ai principi di correttezza professionale;
g) siano effettuati controlli periodici da parte del responsabile della funzione di controllo crediti di sede sugli affidamenti in essere presso la Società, anche in relazione all'esposizione aggiornata del cliente;

h) qualora l'esposizione del cliente superi i parametri indicati dalle procedure interne, la fornitura sia bloccata, salva diversa valutazione responsabile della funzione di controllo crediti, opportunamente motivata;
i) chiunque ne sia a conoscenza segnali immediatamente all'Organismo di Vigilanza oppure al proprio superiore gerarchico, che riferirà all'Organismo di Vigilanza, eventuali anomalie nelle prestazioni dovute al cliente, discordanze significative o ripetute tra materiale ceduto o servizio prestato rispetto a quanto concordato o particolari richieste avanzate dal cliente alla Società.

I mansionari aziendali descrivono nel dettaglio le responsabilità di gestione dei rapporti con i clienti (fidi, scontistica, condizioni di fornitura, ecc)

Rapporti con soggetti coinvolti in procedimenti giudiziari

La procedura deve prevedere quanto segue:

- è fatto assoluto divieto di indurre con qualsiasi modalità soggetti terzi che sono chiamati a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale a non rendere dichiarazioni o a rendere dichiarazioni mendaci;
- ove un dipendente della Società venga indotto da uno dei Destinatari del Modello a non rendere dichiarazioni od a rendere dichiarazioni mendaci, il medesimo dovrà senza indugio riferirne all'Organismo di Vigilanza.

4. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.

La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.

PARTE SPECIALE L – Delitti informatici e trattamento illecito di dati

1. REATI

Si riportano, di seguito, le rubriche dei delitti informatici e trattamento illecito di dati presi in considerazione dall'art. 24 *bis* del D.lgs. 231/01:

- *accesso abusivo ad un sistema informatico o telematico* (art. 615 ter c.p.);
- *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617 quater c.p.);
- *installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche* (art. 617 quinquies c.p.);
- *danneggiamento di informazioni, dati e programmi informatici* (art. 635 bis c.p.);
- *danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità* (art. 635 ter c.p.);
- *danneggiamento di sistemi informatici o telematici* (art. 635 quater c.p.);
- *danneggiamento di sistemi informatici o telematici di pubblica utilità* (art. 635 quinquies c.p.)
- *detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici* (art. 615 quater c.p.);
- *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615 quinquies);
- *documenti informatici* (art. 491 bis c.p.);
- *frode informatica del soggetto che presta servizi di certificazione di firma elettronica* (art. 640 quinquies c.p.)

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall'art. 24-bis del D.Lgs. 231/2001, sono relative alla gestione ed al monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione
- gestione e protezione della postazione di lavoro
- gestione degli accessi verso l'esterno
- gestione e protezione delle reti
- gestione degli output di sistema e dei dispositivi di memorizzazione
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.)

L'organizzazione ha implementato un sistema di sicurezza dei dati descritto del DPS aziendale e ha nominato un Amministratore di sistema responsabile in questi ambiti

3. PRINCIPI GENERALI DI COMPORTAMENTO PER LA PREVENZIONE DEI REATI

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione. Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che De Rosso si pone sono i seguenti:

- **Riservatezza**: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- **Integrità**: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato

esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- **Disponibilità**: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica. Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di De Rosso, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del D.Lgs. 231/2001); violare i principi e le procedure aziendali previste nella presente parte speciale.

4. PRINCIPI PROCEDURALI SPECIFICI

Per la prevenzione specifica delle attività e operazioni a rischio sopra elencate, De Rosso ha individuato dei principi procedurali che tutto il personale che abbia accesso e utilizzo a dati e apparecchiature informatiche deve seguire. Tali procedure prevede non i seguenti divieti:

1. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
2. accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
3. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
4. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
5. detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
6. svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
7. svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
8. istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
9. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
10. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
11. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la

preventiva autorizzazione del Responsabile dei Sistemi Informativi;
3. in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;
5. evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc…);
7. evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia all'Area Sistemi Informativi
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.
La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.

PARTE SPECIALE M – Delitti contro l'industria e il commercio

1. REATI

L'art. 17, comma 7 lettera b) della legge 23 luglio 2009, n. 99 ha inserito tra i reati presupposto del D.lgs. 231/01 le seguenti fattispecie:

- turbata libertà dell'industria o del commercio (Art. 513 c.p.);
- frode nell'esercizio del commercio (Art. 515 c.p.);
- vendita di sostanze alimentari non genuine come genuine (Art. 516 c.p.);
- vendita di prodotti industriali con segni mendaci (Art. 517 c.p.);
- fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (Art. 517-ter c.p.);
- contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (Art. 517-quater. c.p.).
- illecita concorrenza con minaccia o violenza (Art. 513-bis. c.p.);
- frodi contro le industrie nazionali (Art. 514 c.p.).

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

La Società, in considerazione dell'attività svolta, non ha rinvenuto rischi specifici di particolare rilevanza con riferimento alla presente Parte Speciale.

L'unico reato in astratto configurabile sembra essere quello – potenzialmente comune a tutte le realtà imprenditoriali - dell'illecita concorrenza con minaccia o violenza di cui all'art. 513 – bis c.p.

Tuttavia, anche tenuto conto del contenuto del Codice Etico in vigore che già ribadisce l'obbligo di operare nel rispetto delle leggi vigenti e dell'etica professionale, si ritiene di non dover predisporre una procedura ad hoc per prevenire tale rischio e ci si limita a richiamare l'attenzione dei Destinatari sull'opportunità di mantenere in tutte le situazioni un comportamento improntato alla massima correttezza nei rapporti con i competitors e con i terzi in generale.

PARTE SPECIALE N – Delitti in materia di diritto d'autore

1. REATI

L'art. 15, comma 7 lettera c) della legge 23 luglio 2009, n. 99 ha esteso la responsabilità amministrativa degli enti ai seguenti delitti in materia di violazione del diritto d'autore:

- *messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett a) bis);*
- *reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3);*
- *abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1);*
- *riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2);*
- *abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941);*
- *mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941);*
- *fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies l. 633/1941).*

2. IDENTIFICAZIONE DELLE ATTIVITÀ E DELLE OPERAZIONI A RISCHIO

Nell'ambito delle attività sociali che possono comportare la commissione di uno dei delitti in materia di diritto d'autore di cui all'art. 25 - nonies del D.lgs. 231/01 sono state individuate le operazioni a rischio.

La Società ritiene opportuno regolamentare l'utilizzo delle proprie risorse informatiche per assicurare che non vengano poste in essere condotte in violazione delle norme sul diritto d'autore.

Alla luce dell'esame dell'operatività della Società, si è quindi ritenuto di predisporre procedure per:

- acquisto e sottoscrizione nuove licenze da parte della Società di software e banche dati;
- controllo della validità delle licenze sublicenze dei software e delle banche dati in essere
- monitoraggio e controllo della rete informatica interna

Tutto questo è stato espressamente indicato nel DPS aziendale. L'Amministratore di sistema, così come previsto dalla legge sulla privacy effettua un monitoraggio periodico del sistema informatico, della sua sicurezza, dei software presenti e dello scambio delle informazioni/dati.

3. PRINCIPI GENERALI PER LA REDAZIONE DELLE PROCEDURE PER LA PREVENZIONE DEI REATI

Per ciascuna delle operazioni di carattere significativo individuate sono previste specifiche procedure in forza delle quali siano garantiti i seguenti requisiti:

- i software installati sui personal computer della Società siano sempre muniti di valida licenza di utilizzo;
- la rete informatica della Società ed i dati presenti nella stessa siano preservati da accessi ed utilizzi impropri;
- sia fornito accesso da e verso l'esterno a mezzo di connessione internet esclusivamente ai sistemi informatici dei soggetti che ne abbiano effettiva necessità ai fini lavorativi;
- il personale ritenuto esposto al rischio di commissione dei reati in materia di diritto d'autore sia sempre adeguatamente formato e sensibilizzato a tenere comportamenti corretti.
- Sulla base di tali principi, la presente Parte Speciale prevede l'espresso divieto adi:
- installare sui sistemi informativi della Società programmi per elaboratore non assistiti da valida licenza d'utilizzo;
- installare sui sistemi informatici della Società software (c.d. P2P, di files sharing o istant messaging) mediante i quali è possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di files, quali filmati, documenti, canzoni, opere letterarie;
- scaricare sui personal computer della Società programmi prelevati da internet o da sistemi peer to peer, anche qualora trattasi di software gratuiti (freeware) o shareware, salvo espressa autorizzazione del responsabile dei sistemi informativi;
- installare sui personal computer della Società apparati di comunicazione propri (ad esempio modem);
- ascoltare sui personal computer della Società files audio o musicali, nonché visionare video e/o immagini, su qualsiasi supporto essi siano memorizzati, se non a fini prettamente lavorativi.

I Destinatari debbono pertanto:

1. utilizzare esclusivamente i software, le applicazioni, i files e le apparecchiature informatiche fornite dalla Società e farlo esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
2. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
3. rispettare le policy interne in merito ai dispositivi antintrusione e antivirus;
4. custodire le password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;

5. non prestare o permettere a terzi l'uso delle apparecchiature informatiche della Società o dell'archivio informatico della stessa, senza la preventiva autorizzazione del responsabile dei sistemi informativi;
6. astenersi dall'effettuare copie non specificamente autorizzate dal responsabile dei sistemi informativi di dati e di software di proprietà della Società;
7. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
8. qualora per la connessione alla rete internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;

Per ciascuna delle operazioni di carattere significativo individuate nella presente Parte Speciale sono previste specifiche procedure in forza delle quali:

a) sia previsto (compatibilmente con la normativa vigente in materia di diritto del lavoro e di diritto alla privacy) il costante monitoraggio della rete informatica interna;
b) siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio relativo ai reati informatici e sia attuata una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica;
c) la rete informatica della Società sia dotata di adeguate protezioni, così da evitare la non corretta duplicazione, riproduzione, trasmissione o divulgazione di opere dell'ingegno protette, ed in particolare delle opere letterarie nella disponibilità della Società;
d) sia prevista l'attuazione di un tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici contenuti nel sistema informativo della Società;
e) sia assicurato che tutti i supporti informatici alienati o smaltiti (personal computer, floppy disc, CD o DVD) siano resi illeggibili prima della loro vendita o distruzione, così da evitare l'involontaria diffusione di programmi e/o contenuti protetti.

4. PRINCIPI PROCEDURALI SPECIFICI

Installazione ed utilizzo dei programmi per elaboratore

La Società adotta una procedura che assicuri che su tutti i suoi personal computer possano essere installati esclusivamente programmi per elaboratore muniti di valida licenza di utilizzo ed approvati dalla Società.

E' altresì installato sul server aziendale un software che permette che i personal computer della Società accedano ai soli siti web selezionati dal responsabile dei sistemi informativi a seconda della necessità di utilizzo dei dipendenti.

La Società verifica con cadenza periodica la corrispondenza delle licenze in essere con il numero di personal computer di sua proprietà.

5. ATTUAZIONE DEI PRINCIPI E DELLE PRESCRIZIONI

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale.

La presente Parte Speciale e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.