



**Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto
Legislativo 231/2001**

Approvato dal C.d.A. di Telespazio S.p.A.
nella seduta del 9 Giugno 2009

INDICE**Parte Generale**

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001 n. 231 E SUCCESSIVE MODIFICHE ED INTEGRAZIONI	1
1.1. il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società ed associazioni.....	1
1.2. Sanzioni.....	5
1.3. Presupposto di esclusione della responsabilità dell'Ente.....	6
2. LINEE GUIDA DI CONFINDUSTRIA	8
3. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE DA PARTE DI TELESPAZIO S.P.A.	9
3.1. Motivazioni di Telespazio S.p.A. nell'adozione del modello di organizzazione e gestione.....	9
3.2. Finalità del Modello.....	10
3.3. Struttura del Documento.	11
3.4. Adozione e gestione del Modello nelle società controllate, partecipate e nelle strutture associative.....	11
3.5. Modifiche ed integrazioni del Modello.	12
4. ORGANISMO DI VIGILANZA	13
4.1. Identificazione dell'Organismo di Vigilanza.	13
4.2. Funzioni e poteri dell'Organismo di Vigilanza.	14
4.3. Modalità e periodicità di riporto agli Organi Societari.	16
4.4. Flussi informativi nei confronti dell'Organismo di Vigilanza.....	17
4.4.1. Segnalazioni da parte di esponenti aziendali o da parte di terzi.....	17
4.4.2. Obblighi di informativa relativi ad atti ufficiali	18
5. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE.	19
5.1. Formazione del personale.	19
5.2. Informativa a collaboratori esterni e Partner.....	19
6. IL SISTEMA SANZIONATORIO	20
6.1. Principi generali.....	20

6.2. Sanzioni per i lavoratori dipendenti (non dirigenti)	20
6.3. Misure nei confronti dei dirigenti	21
6.4. Misure nei confronti degli Amministratori.....	22
6.5. Misure nei confronti di Collaboratori, Consulenti ed altri soggetti terzi	22
7. CONFERMA APPLICAZIONE E ADEGUATEZZA DEL MODELLO	22

Parte Speciale "A"

Reati in danno della Pubblica Amministrazione

A.1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (artt. 24 e 25 del Decreto).....	25
A.2. NOZIONE DI PUBBLICO UFFICIALE E INCARICATO DI PUBBLICO SERVIZIO (ARTT. 357-358 C.P.)	28
A.3. AREE A RISCHIO	30
A.4. DESTINATARI DELLA PARTE SPECIALE - PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO	32
A.5. AREE DI ATTIVITÀ A RISCHIO: ELEMENTI FONDAMENTALI DEL PROCESSO DECISIONALE	34
A.5.1. Singole operazioni a rischio: individuazione dei Responsabili Interni e Schede di Evidenza.....	34
A.5.2. Istruzioni e verifiche dell'OdV	34

Parte Speciale "B"

Reati societari, reati ed illeciti di Market Abuse - Altri reati

B.1. LA TIPOLOGIA DEI REATI SOCIETARI E DEI REATI E ILLECITI DI MARKET ABUSE (artt. 25 ter e 25 sexies del Decreto)	38
B.2. ALTRI REATI	41
B.3. PRINCIPALI AREE DI ATTIVITA' A RISCHIO DI COMMISSIONE DEI REATI	43
B.4. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO.....	45
B.5. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI.....	46

B.5.1.	bilanci ed altre comunicazioni sociali	46
B.5.2	Esercizio dei poteri di controllo sulla gestione sociale.	47
B.5.3	Tutela del capitale sociale.....	48
B.5.4.	Prospetti informativi.....	48
B.5.5.	Attività soggette a vigilanza.	49
B.5.6.	Gestione Rapporti con le Società' di Revisione.....	49
B.6.	COMPITI DELL'ORGANISMO DI VIGILANZA	50

Parte Speciale "C"

Reati in materia di salute e sicurezza sul lavoro

C.1.	LA TIPOLOGIA DEI REATI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO. (ART. 25 –SEPTIES DEL DECRETO)	53
C.2.	PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI	54
C.3.	DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO.....	55
C.4.	PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI.....	56
C.5.	COMPITI DELL'ODV	65

Parte Speciale "D"

Ricettazione, riciclaggio impiego di denaro, beni o utilità di provenienza illecita

D.1.	LA TIPOLOGIA DEI REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 25 –OCTIES DEL DECRETO)	67
D.2.	PRINCIPALI AREE DI ATTIVITA' A RISCHIO DI COMMISSIONE DEI REATI	69
D.3.	DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	69
D.4.	PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI.....	70
D.5.	COMPITI DELL'ODV	71

Parte Speciale "E"
Delitti informatici e trattamento illecito dei dati

E.1. LA TIPOLOGIA DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (ART. 24–BIS DEL DECRETO)	73
E.2. PRINCIPALI AREE DI ATTIVITA' A RISCHIO DI COMMISSIONE DEI REATI	80
E.3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO	80
E.4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI	83
E.5. COMPITI DELL'ODV	89

PARTE GENERALE

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231 E SUCCESSIVE MODIFICHE ED INTEGRAZIONI

1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE, SOCIETÀ ED ASSOCIAZIONI

In attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto legislativo n. 231 (di seguito denominato il "Decreto"), entrato in vigore il 4 luglio 2001, con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche, alle quali l'Italia aveva già da tempo aderito. In particolare, si tratta della Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea, della Convenzione firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri, e della Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa (assimilabile sostanzialmente alla responsabilità penale) a carico degli Enti (da intendersi come società, associazioni, consorzi, ecc., di seguito denominati "Enti") per reati tassativamente elencati e commessi nel loro interesse o vantaggio da:

- persone fisiche che rivestono posizione di vertice ("*apicali*") (rappresentanza, amministrazione o direzione dell'Ente o di altra unità organizzativa o persone che esercitano, di fatto, la gestione ed il controllo); ovvero:
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al precedente punto.

La responsabilità dell'Ente si aggiunge a quella della persona fisica, che ha commesso materialmente il reato.

Il Decreto coinvolge, quindi, con la previsione della sopra detta responsabilità amministrativa, nella repressione degli illeciti penali previsti dal Decreto, gli Enti che abbiano tratto interesse e/o vantaggio dalla commissione del reato. Tra le sanzioni comminabili, quelle certamente più gravose per l'Ente sono rappresentate dalle misure interdittive, quali la sospensione o revoca di autorizzazioni, licenze o concessioni, il divieto di contrattare con la pubblica amministrazione, l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi. La suddetta responsabilità si configura anche in relazione a reati commessi all'estero, purché per la loro repressione non

proceda lo Stato del luogo in cui siano stati commessi.

La tipologia di reati attualmente prevista è la seguente:

- i. reati commessi nei rapporti con la Pubblica Amministrazione,
- ii. reati in tema di falsità in monete, carte di pubblico credito e valori in bollo, introdotti nella disciplina dalla legge 406/2001, art. 6, che ha inserito nel D. Lgs 231/2001 l'art. 25 *bis*,
- iii. reati in materia societaria introdotti nella disciplina dal D.Lgs 61/2002, che ha inserito nel d.lgs.231/2001 l'art. 25 *ter*, aggiornato con la L. 262/2005,
- iv. delitti con finalità di terrorismo o di eversione dell'ordine democratico introdotti nella disciplina dalla Legge 7/2003, che ha inserito nel d.lgs 231/2001 l'art. 25 *quater*,
- v. pratiche di mutilazione degli organi genitali femminili, introdotto dalla Legge 9 gennaio 2006, n. 7, che ha comportato l'inserimento nel d.lgs. 231/01 dell'art. 25 *quater* 1,
- vi. delitti in tema di riduzione o mantenimento in schiavitù o in servitù, di tratta di persone e di acquisto e alienazione di schiavi, di sfruttamento sessuale dei bambini e di pedopornografia anche a mezzo internet, introdotti nella disciplina con Legge 228/2003 e dalla Legge 38/2006, che hanno inserito e modificato nel d.lgs 231/2001 l'art. 25 *quinquies*,
- vii. i reati di abuso di informazioni privilegiate e di manipolazione del mercato indicati all'art. 9 della legge 18 Aprile 2005 n° 62 (Legge Comunitaria 2004) che a sua volta recepisce la direttiva 2006/6/CE – previsti dalla parte V, titolo I bis, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998 n° 58 – sono recepiti dal Legislatore nazionale attraverso l'art. 25 *sexies* del d.lgs.231/01;
- viii. reati transnazionali in materia di associazioni criminose, riciclaggio, traffico di migranti, intralcio alla giustizia previsti dalla Legge n. 146 del 2006, che ratifica la Convenzione ed i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001;
- ix. reati ed illeciti commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro previsti dall'art. 9 della L. 123/07, sul riordino della normativa in materia di sicurezza e salute sui luoghi di lavoro, con l'introduzione dell'art. 25 *septies* nel corpo del d.lgs.231/01. Successivamente, in data 30 aprile 2008 è stato pubblicato il d.lgs. n° 81 del 9 aprile 2008, recante "Attuazione dell'art. 1 della sopra citata L. 123/07 in materia della salute e della sicurezza nei luoghi di lavoro". Tale Decreto persegue la finalità di riordino e riforma delle vigenti norme in materia di salute e sicurezza dei lavoratori, mediante il coordinamento delle medesime in un unico testo normativo;

- x. reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita introdotti con l'emanazione del d.lgs. 231/07, di recepimento della Direttiva 2005/60/CE del Parlamento Europeo in materia di antiriciclaggio attraverso l'aggiunta dell'art. 25 *octies* nel corpo del d.lgs.231/01;
- xi. delitti informatici e trattamento illecito dei dati, previsti dalla Legge n. 48 del 18 marzo 2008, di ratifica e esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004, con l'introduzione dell'art.24-bis nel corpo del d.lgs.231/01.

Stante la particolare natura di Telespazio S.p.A. si ritiene che dei reati previsti fino ad oggi nel Decreto e sue successive integrazioni (che hanno determinato il presente aggiornamento del Modello già adottato nel 2004) e modificazioni possano potenzialmente riguardare la Società quelli riportati sub i, iii, vi, vii, viii, ix, x, xi.

In particolare:

Reati in danno della Pubblica Amministrazione:

- i. indebita percezione di contributi, finanziamenti o altre erogazioni da parte di un Ente pubblico (art. 316 ter c.p.),
- ii. truffa in danno dello Stato o d'altro Ente pubblico (art. 640, 2° comma, n. 1 c.p.),
- iii. truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.),
- iv. frode informatica in danno dello Stato o di altro Ente pubblico (art. 640 ter c.p.),
- v. corruzione per un atto d'ufficio (art. 318 c.p.),
- vi. corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.),
- vii. corruzione in atti giudiziari (art. 319 ter c.p.),
- viii. istigazione alla corruzione (art. 322 c.p.),
- ix. corruzione di persone incaricate di pubblico servizio (art. 320 c.p.)
- x. concussione (art. 317 c.p.),
- xi. malversazione a danno dello Stato o di altro Ente pubblico (art. 316 bis c.p.),
- xii. peculato, 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.)

Reati societari, reati e illeciti di market abuse:

- i. false comunicazioni sociali (art. 2621 c.c.);
- ii. false comunicazioni sociali in danno dei soci o dei creditori (art. 2622 c.c.);
- iii. falso in prospetto, (art. 173 bis d.lgs. 24.02.1998 n. 58 e successive modificazioni ed integrazioni: "TUF");
- iv. falsità nelle relazioni o nelle comunicazioni della Società di Revisione (art. 2624 c.c.);
- v. impedito controllo (art. 2625 c.c.);
- vi. indebita restituzione dei conferimenti (art. 2626 c.c.);
- vii. illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- viii. illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- ix. delitto di operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- x. omessa comunicazione conflitto d'interessi (art. 2629 bis c.c.);
- xi. omessa convocazione dell'assemblea (art. 2631 c.c.);
- xii. formazione fittizia di capitali (art. 2632 c.c.);
- xiii. indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- xiv. illecita influenza sull'assemblea (art. 2636 c.c.);
- xv. aggio (art. 2637 c.c.);
- xvi. ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.);
- xvii. abuso di informazioni privilegiate (art. 184 TUF);
- xviii. manipolazione del mercato (art. 185 TUF).

Altri reati:

- i. riduzione o mantenimento in schiavitù o in servitù, tratta di persone e di acquisto e alienazione di schiavi, sfruttamento sessuale dei bambini e pedopornografia anche a mezzo internet, introdotti nella disciplina con Legge 228/2003 e dalla Legge 38/2006.
- ii. reati gravi che prevedano un gruppo criminale organizzato e che abbiano la caratteristica della transnazionalità previsti dall'art. 10 della legge 16 marzo 2006 n. 146.

Reati commessi in violazione di norme di sicurezza ed antinfortunistiche:

- i. omicidio colposo (artt. 589 c.p.);
- ii. lesioni gravi e gravissime commessi in violazione di norme di sicurezza ed antinfortunistiche (art 590, comma 3 c.p.).

Reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita:

- i. ricettazione (art. 648 c.p.);
- ii. riciclaggio (art. 648-bis c.p.);
- iii. impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).

Delitti informatici e trattamento illecito dei dati:

- i. documenti informatici (art.491 bis c.p.);
- ii. accesso abusivo ad un sistema informatico o telematico (Art. 615 ter c.p.);
- iii. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater);
- iv. diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art.615 quinquies c.p.);
- v. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- vi. installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- vii. danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- viii. 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.);
- ix. danneggiamento di sistemi informatici e telematici (art. 635-quater c.p.);
- x. danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies c.p.).

1.2. SANZIONI.

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

- Sanzioni pecuniarie;
- Sanzioni interdittive;

- Confisca;
- Pubblicazione della sentenza.

In particolare le principali sanzioni interdittive, non applicabili alla commissione di reati societari di cui all'art. 25 ter del Decreto, concernono:

- l'interdizione dall'esercizio dell'attività;
- il divieto di contrattare con la Pubblica Amministrazione;
- la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- l'esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi;
- il divieto di pubblicizzare beni o servizi.

Le sanzioni pecuniarie, applicabili a tutti gli illeciti, sono determinate attraverso un sistema basato su "quote" in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 ad un massimo di Euro 1.549,37.

Nel caso di sanzioni pecuniarie applicabili per la commissione dei reati di cui all'art. 25 ter del Decreto, l'importo delle quote può variare fra un minimo di Euro 516,46 ed un massimo di Euro 3.098,74 (così come modificate dall'art. 39, 5 comma della Legge n. 262 del 28 dicembre 2005).

Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione (art. 11 del Decreto Legislativo n. 231/2001).

1.3. PRESUPPOSTO DI ESCLUSIONE DELLA RESPONSABILITÀ DELL'ENTE.

Istituita la responsabilità amministrativa degli Enti, l'art. 6 del Decreto stabilisce che l'Ente non ne risponde nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, *"modelli di organizzazione di gestione e controllo idonei a prevenire reati della specie di quello verificatosi"*.

La medesima norma prevede, inoltre, l'istituzione di un organo di controllo interno all'Ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei predetti modelli, nonché di curarne l'aggiornamento.

Detti modelli di organizzazione, gestione e controllo (di seguito denominati i "Modelli"), ex art. 6, commi 2 e 3, del D. Lgs. 231/2001, devono rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Ove il reato venga commesso da soggetti 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 soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento è stato affidato a un Organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo;
- i soggetti hanno commesso il reato eludendo fraudolentemente il Modello;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di controllo in ordine al Modello.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Lo stesso Decreto prevede che i Modelli possano 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 sull'idoneità dei modelli a prevenire i reati.

E' infine previsto che, negli Enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente.

2. LINEE GUIDA DI CONFINDUSTRIA

La predisposizione del presente Modello è ispirata alle Linee Guida emanate da Confindustria il 7 marzo 2002 ed integrate in data 3 ottobre 2002 con l'"Appendice integrativa in tema di reati societari" (di seguito le "Linee Guida"), successivamente aggiornate in data 24 maggio 2004 e 31 marzo 2008.

Il percorso da queste indicato per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

- individuazione delle *aree a rischio*, volta a verificare in quali aree/settori aziendali sia possibile la realizzazione dei reati;
- predisposizione di un sistema di controllo in grado di ridurre i rischi attraverso l'adozione di appositi protocolli. A supporto di ciò soccorre l'insieme coordinato di strutture organizzative, attività e regole operative applicate, su indicazione del vertice apicale, dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno. Le componenti più rilevanti del sistema di controllo preventivo proposto da Confindustria sono:
 - codice etico;
 - sistema organizzativo;
 - procedure manuali ed informatiche;
 - poteri autorizzativi e di firma;
 - sistemi di controllo e gestione;
 - comunicazioni al personale e sua formazione.

Il sistema di controllo inoltre deve essere uniformato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- introduzione di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal Modello;

- individuazione di un OdV i cui principali requisiti siano:
 - autonomia ed indipendenza,
 - professionalità,
 - continuità di azione.
- obbligo da parte delle funzioni aziendali, e segnatamente di quelle individuate come maggiormente "a rischio", di fornire informazioni all'OdV, sia su base strutturata (informativa periodica in attuazione del Modello stesso), sia per segnalare anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (in quest'ultimo caso l'obbligo è esteso a tutti i dipendenti senza seguire linee gerarchiche);
- possibilità di attuare in seno ai gruppi soluzioni organizzative che accentrino presso l'OdV della capogruppo le risorse operative da dedicare alla vigilanza anche nelle società del gruppo stesso a condizione che:
 - in ogni controllata sia istituito l'OdV;
 - sia possibile per l'OdV della controllata avvalersi delle risorse allocate presso l'OdV della capogruppo sulla base di un predefinito rapporto contrattuale;
 - i dipendenti dell'OdV della capogruppo, nell'effettuazione dei controlli presso le altre società del gruppo, assumano la veste di professionisti esterni che svolgono la loro attività nell'interesse della controllata, riportando direttamente all'OdV di quest'ultima, con i vincoli di riservatezza propri del consulente esterno.

Resta inteso che la scelta di non seguire in alcuni punti specifici le Linee Guida non inficia la validità di un Modello. Questo infatti essendo redatto con riferimento alla peculiarità di una società particolare, può discostarsi dalle Linee Guida che per loro natura hanno carattere generale.

3. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE DA PARTE DI TELESPAZIO S.P.A.

3.1. MOTIVAZIONI DI TELESPAZIO S.P.A. NELL'ADOZIONE DEL MODELLO DI ORGANIZZAZIONE E GESTIONE.

Telespazio S.p.A., al fine di assicurare sempre più condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto conforme alle proprie politiche aziendali, ed in sintonia con le indicazioni della Capogruppo Finmeccanica, procedere all'adozione di un Modello di organizzazione e di gestione in linea con le prescrizioni del Decreto e sulla base delle Linee Guida emanate da Confindustria.

Tale iniziativa, unitamente all'adozione sin dal 2003 del Codice Etico , è stata assunta nella convinzione che l'adozione di tale Modello - al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento

facoltativo e non obbligatorio - possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della Società e di tutti gli altri soggetti alla stessa cointeressati (Clienti, Fornitori, Partner, Collaboratori a diverso titolo), affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

3.2. FINALITÀ DEL MODELLO.

Il Modello predisposto da Telespazio S.p.A. si basa su un sistema strutturato ed organico di procedure nonché di attività di controllo che nella sostanza:

- individuano le aree/i processi di possibile rischio nell'attività aziendale vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della società in relazione ai rischi/reati da prevenire tramite:
 - un Codice Etico, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali assunti dai dipendenti, amministratori e collaboratori a vario titolo della Società;
 - un sistema di deleghe di funzioni e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
- determinano una struttura organizzativa coerente volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
- individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporre l'aggiornamento.

Pertanto il Modello si propone come finalità quelle di:

- migliorare il sistema di Corporate Governance;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto di Telespazio S.p.A. nelle "aree di attività a rischio", la consapevolezza di

poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;

- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di Telespazio S.p.A. che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale.
- ribadire che Telespazio S.p.A. non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui Telespazio S.p.A. intende attenersi.

3.3. STRUTTURA DEL DOCUMENTO.

Il presente documento (Modello) è costituito da una "Parte Generale" e da singole "Parti Speciali", predisposte per le diverse tipologie di reato considerate di possibile rischio da parte di Telespazio S.p.A., contemplate nel Decreto 231/2001. Nella parte generale, dopo un richiamo ai principi del decreto, vengono illustrate le componenti essenziali del Modello con particolare riferimento all'Organismo di Vigilanza, la formazione del personale e diffusione del Modello nel contesto aziendale, il sistema disciplinare e le misure da adottare in caso di mancata osservanza delle prescrizioni del Modello. La Parte Speciale "A" trova applicazione per le tipologie specifiche di reati previste ai sensi degli articoli 24 e 25 del Decreto, ossia per i reati realizzabili in danno della Pubblica Amministrazione. La Parte Speciale "B" trova applicazione per le tipologie specifiche di reati previste ai sensi degli artt. 25 *ter* e 25 *sexies* del Decreto, cioè per i c.d. reati societari, reati e illeciti di market abuse, e per quelli sopra qualificati come "Altri". La Parte Speciale "C" è relativa alle tipologie specifiche di reati previste ai sensi dell' articolo 25 *septies* del Decreto, ossia i reati ed illeciti commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. La Parte Speciale "D" è relativa alle tipologie specifiche di reati previste ai sensi dell'art.25 *octies*, ossia i reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita. La Parte Speciale "E" è relativa alle tipologie specifiche di reati previsti ai sensi dell'art. 24 *bis*, ossia i delitti informatici e trattamento illecito dei dati.

3.4. ADOZIONE E GESTIONE DEL MODELLO NELLE SOCIETÀ CONTROLLATE, PARTECIPATE E NELLE STRUTTURE ASSOCIATIVE.

Le società, di diritto italiano, controllate direttamente o indirettamente da Telespazio S.p.A. dovranno dotarsi di un proprio Modello di Organizzazione, Gestione e Controllo ex d.lgs. 231/01 che sia in linea con le prescrizioni del Decreto.

Nel far ciò le predette società prenderanno come base di riferimento il Modello di Telespazio S.p.A. che dovrà comunque essere armonizzato alle singole realtà con specifici adattamenti che lo rendano efficace nelle diverse aree di attività a rischio proprie di ciascuna entità aziendale ed in questa individuate.

Ciascuna società controllata dovrà provvedere all'istituzione di un proprio Organismo di Vigilanza con il compito primario di esercitare i controlli sull'attuazione del Modello secondo le procedure in esso descritte e sulla base delle indicazioni contenute nell'art. 6 del Decreto 231/01.

L'Organismo di Vigilanza di ciascuna società controllata:

- i. dovrà coordinarsi con Telespazio S.p.A. al fine di garantire l'adozione di un Modello di Organizzazione, Gestione e Controllo in linea con le prescrizioni del Decreto, con le Linee Guida Confindustria e con i principi del presente Modello;
- ii. dovrà trasmettere a Telespazio S.p.A. il Modello di Organizzazione, Gestione e Controllo adottato ed i suoi eventuali successivi aggiornamenti.

Negli altri Enti partecipati di diritto italiano, Telespazio S.p.A. - attraverso il proprio rappresentante nell'organo amministrativo o in sede assembleare - suggerisca formalmente la necessità di adeguarsi alla disciplina ex d. lgs. 231/2001 e faccia quanto in proprio potere per soddisfare tale necessità.

Relativamente alla costituzione di nuove strutture associative, sempre su base nazionale, Telespazio S.p.A. verifica, fin dall'origine, se gli altri Partner si siano uniformati al d.lgs. 231/2001 anche richiedendo la sottoscrizione di una dichiarazione in tal senso da parte dei Partner medesimi.

Relativamente ai rapporti partecipativi con società estere, Telespazio S.p.A. richiede almeno l'adozione del Codice Etico e comunica agli organi deliberanti l'opportunità di dotarsi di idonei strumenti preventivi sotto il profilo procedurale, al fine di tutelarsi da possibili impatti riconducibili alla responsabilità amministrativa dell'ente.

In ogni caso, ogni dipendente o collaboratore di Telespazio S.p.A. al quale sia affidato l'incarico di svolgere attività per conto o nell'interesse di Enti partecipati da Telespazio S.p.A. deve attenersi rigorosamente alle regole previste nel Codice Etico e nel Modello di Organizzazione, Gestione e Controllo adottato da Telespazio S.p.A., operando in ogni caso tramite uno specifico mandato consulenziale conferito dagli enti interessati della Controllante Telespazio S.p.A.

3.5. MODIFICHE ED INTEGRAZIONI DEL MODELLO.

Essendo il presente Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a del Decreto)

la sua adozione, così come le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di Telespazio S.p.A.

In particolare è demandato al Consiglio di Amministrazione di Telespazio S.p.A., di integrare il presente Modello con ulteriori Parti Speciali relative ad altre tipologie di reati che, per effetto di nuove normative, possano essere ulteriormente collegate all'ambito di applicazione del Decreto Legislativo 231/01.

4. ORGANISMO DI VIGILANZA

4.1. IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA.

In base alle previsioni del d.lgs. 231/2001, il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei Modelli, nonché di curarne l'aggiornamento, deve essere affidato ad un Organismo interno alla Società (art. 6, comma 1, lett. B, del Decreto) e diverso dal Consiglio di Amministrazione.

Telespazio S.p.A. ha ritenuto, pertanto, di nominare inizialmente, con delibera del Consiglio di Amministrazione del 14 aprile 2003, come membro dell'Organismo di Vigilanza il Responsabile della Funzione Internal Auditing. Successivamente, in sintonia con le indicazioni della Capogruppo, il Consiglio di Amministrazione di Telespazio S.p.A., in data 28 giugno 2006, ha nominato un nuovo Organismo di Vigilanza in forma collegiale; in particolare si rappresenta che lo Statuto ed il Regolamento dell'OdV che ne regolano l'operatività, sono stati rispettivamente approvati dal C.d.A. aziendale in data 28 giugno 2006 e il 5 settembre 2006.

L'Organismo di Vigilanza è composto da tre membri, tra cui un membro del Collegio Sindacale, che ne è il Presidente, dal Responsabile pro-tempore della Funzione Internal Auditing e dal Responsabile pro-tempore della Funzione Affari Legali e Societari e può essere integrato da non più di due membri.

Tale scelta è stata assunta in considerazione della specificità dei compiti che ad esso fanno capo, delle previsioni del Decreto e delle indicazioni contenute nelle Linee Guida emanate da Confindustria, in modo da garantire in capo all'Organismo i più opportuni requisiti di autonomia, indipendenza, professionalità e continuità d'azione, che il Decreto stesso richiede per tale funzione.

In particolare, in considerazione anche di quanto al riguardo previsto dalle citate Linee Guida, i predetti requisiti vengono di seguito dettagliati:

Autonomia e indipendenza

I requisiti di autonomia e indipendenza, garantiti dalla collegialità dell'Organismo di Vigilanza, fanno sì che l'Organismo di Vigilanza possa svolgere il proprio ruolo senza condizionamenti diretti o indiretti da parte dei soggetti controllati.

A garanzia dell'indipendenza, l'Organismo di Vigilanza risponde direttamente al Consiglio di Amministrazione e riferisce anche al Collegio Sindacale nel caso di anomalie o irregolarità rilevanti ai fini del d.lgs. n. 231/2001, riscontrate in capo al Consiglio di Amministrazione nella sua collegialità.

Professionalità

L'Organismo di Vigilanza possiede al suo interno competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere.

Tali caratteristiche unite all'indipendenza, garantiscono l'obiettività di giudizio.

Continuità d'azione

Per poter dare la garanzia di efficace e costante attuazione e Vigilanza del Modello, l'Organismo di Vigilanza è dotato di una struttura dedicata in maniera costante all'attività di monitoraggio delle procedure aziendali. Ai fini di un migliore e più efficace espletamento dei compiti e delle funzioni ad esso attribuite e regolamentate nello statuto, l'Organismo di Vigilanza può avvalersi, per lo svolgimento della propria attività operativa, della Funzione Internal Auditing della Società e di quelle altre Funzioni che, di volta in volta, si potranno rendere utili all'espletamento delle attività indicate.

L'Organismo può inoltre ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello, osservando le procedure interne aziendali previste per l'assegnazione di incarichi di consulenza.

Lo statuto dell'Organismo di Vigilanza stabilisce e regola, tra l'altro, le modalità con le quali devono essere trasmesse le informazioni ed i documenti richiesti dall'Organismo di Vigilanza stesso, al fine di garantire l'effettività di azione nei confronti dell'organizzazione aziendale.

L'Organismo può anche delegare lo svolgimento di compiti specifici ad uno o più dei suoi componenti, ferma restando la sua responsabilità collegiale.

4.2. FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA.

L'attività dell'OdV di Telespazio S.p.A. consiste in particolare nel:

- vigilare sull'applicazione del Modello in relazione alle diverse tipologie di reati contemplate dal Decreto;

- verificare l'efficacia del Modello e la sua capacità di prevenire la commissione dei reati di cui al Decreto;
- individuare e proporre al Consiglio di Amministrazione aggiornamenti e modifiche del Modello stesso in relazione alla mutata normativa o alle mutate condizioni aziendali;
- monitorare costantemente il sistema delle procedure aziendali inerenti la prevenzione e gestione dei rischi di reato ex d.lgs. 231/01 e l'applicazione del sistema di Corporate Governance, suggerendo, se del caso, le modifiche necessarie.

Pertanto sul piano operativo sono affidati all'OdV della Telespazio S.p.A. i seguenti compiti:

- attivare le procedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree a rischio, resta comunque demandata al management operativo e forma parte integrante del processo aziendale;
- verificare periodicamente la mappa delle aree a rischio reato al fine di adeguarla ai mutamenti dell'attività e/o della struttura aziendale. A tal fine il Management e gli addetti alle attività di controllo, nell'ambito delle singole funzioni, devono segnalare all'OdV le eventuali situazioni in grado di esporre l'azienda al rischio di reato. Tutte le comunicazioni devono essere scritte (anche via e-mail o fax) e non anonime;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle aree di attività a rischio come definite nelle singole Parti Speciali del Modello;
- promuovere idonee iniziative per la diffusione del Modello, e predisporre la documentazione organizzativa interna necessaria al funzionamento del Modello stesso contenente istruzioni, chiarimenti o aggiornamenti;
- raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni di cui al successivo paragrafo 4.4) rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV (v. successivo paragrafo 4.4);
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello portate all'attenzione dell'OdV da segnalazioni o emerse nel corso dell'attività di vigilanza dello stesso;
- verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di reati (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a proporre aggiornamenti degli elementi stessi.

- coordinarsi con la Funzione Internal Audit e le altre Funzioni Aziendali per il monitoraggio delle attività nelle aree a rischio. L'OdV riceve dal Management e dalle funzioni aziendali comunicazione di ogni attività da esse svolta, relativamente ad eventuali situazioni che possano esporre l'Azienda ai rischi di reato contemplati dal d.lgs. 231/01; inoltre l'OdV ha libero accesso a tutta la documentazione aziendale rilevante, anche qualora essa includa dati sensibili ai sensi della Legge sulla privacy, il cui trattamento sia reso possibile dall'autorizzazione generale del Garante (G.U. 190/04), ovvero da specifiche autorizzazioni;
- controllare l'effettiva presenza, la regolare tenuta, e l'efficacia della documentazione richiesta in conformità alle singole Parti Speciali del Modello per i diversi tipi di reato. All'OdV devono essere segnalate le attività maggiormente significative o le operazioni contemplate dalle Parti Speciali, e devono essergli messi a disposizione i dati di aggiornamento della documentazione, al fine di consentire l'attività di controllo.

Per lo svolgimento dei compiti suddetti l'OdV:

- può accedere ai documenti aziendali;
- dispone di risorse finanziarie e professionali adeguate;
- si avvale del supporto e la cooperazione delle varie strutture aziendali che possano essere interessate o comunque coinvolte nelle attività di controllo.

Lo statuto dell'OdV, approvato dal CdA di Telespazio in data 28 giugno 2006, ne dettaglia specificatamente compiti, funzioni e poteri.

4.3. MODALITÀ E PERIODICITÀ DI RIPORTO AGLI ORGANI SOCIETARI.

L'Organismo di Vigilanza riferisce periodicamente al Consiglio di Amministrazione in ordine allo svolgimento dei suoi compiti, con particolare riferimento alla corretta attuazione del Modello ed all'eventuale emersione di fatti critici.

L'attività informativa può anche essere svolta, informalmente e su base continuativa, nei confronti del Presidente e dell'Amministratore Delegato, ed anche da parte di singoli componenti dell'Organismo.

Un formale rapporto scritto deve essere inviato, con frequenza semestrale, al Consiglio di Amministrazione ed al Collegio Sindacale in ordine all'attività di vigilanza svolta ed alle sue risultanze.

Nei due mesi successivi alla chiusura di ogni esercizio sociale l'Organismo di Vigilanza rimette al Consiglio di Amministrazione ed al Collegio Sindacale una relazione sul quadro generale delle attività svolte, in genere, sui rapporti tenuti con le funzioni aziendali e con lo stesso Collegio Sindacale.

In ogni caso l'Organismo di Vigilanza deve informare senza indugio il Consiglio di Amministrazione in caso di rilevazione di violazioni del Modello e del Codice Etico, ovvero nei casi di necessità di modificare il Modello, o di innovazioni normative in materia di responsabilità amministrativa degli Enti.

L'OdV di Telespazio S.p.A. potrà, comunque, essere convocato in qualsiasi momento dai suddetti organi o potrà a sua volta presentare richiesta in tal senso, per riferire in merito al funzionamento del Modello od a situazioni specifiche.

4.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

4.4.1. Segnalazioni da parte di esponenti aziendali o da parte di terzi.

In ambito aziendale dovrà essere portata a conoscenza dell'OdV, oltre alla documentazione prescritta nelle singole Parti Speciali del Modello secondo le procedure ivi contemplate, ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione del Modello nelle aree di attività a rischio.

Valgono al riguardo le seguenti prescrizioni:

- devono essere raccolte eventuali segnalazioni relative alla violazione del Modello o comunque conseguenti a comportamenti non in linea con le regole di condotta adottate dalla Società stessa;
- l'OdV valuterà le segnalazioni ricevute e le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna;
- le segnalazioni, in linea con quanto previsto dal Codice Etico, dovranno essere in forma scritta e non anonima ed avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'OdV agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate erroneamente e/o in mala fede;
- al fine di facilitare il flusso di segnalazioni ed informazioni verso l'OdV, è prevista l'istituzione di "canali informativi dedicati" (casella di posta elettronica: ODV@Telespazio.com - Top Fax Call: 06-40999165);
- le segnalazioni pervenute all'OdV devono essere raccolte e conservate in un apposito archivio al quale sia consentito l'accesso solo da parte dei membri dell'OdV.

4.4.2. Obblighi di informativa relativi ad atti ufficiali

Oltre alle segnalazioni anche ufficiose di cui al capitolo precedente, devono essere obbligatoriamente trasmesse all'OdV di Telespazio S.p.A. le informative concernenti:

- 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 Decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello organizzativo con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;

- sistema organizzativo e separazione dei ruoli.

Il sistema organizzativo deve rispettare i requisiti di:

- chiarezza, formalizzazione e comunicazione, con particolare riferimento all'attribuzione di responsabilità, alla definizione delle linee gerarchiche e all'assegnazione delle attività operative;
- separazione dei ruoli, ovvero le strutture organizzative sono articolate in modo da evitare sovrapposizioni funzionali e la concentrazione su di una sola persona di attività che presentino un grado elevato di criticità o di rischio.

Al fine di garantire tali requisiti, la Società è dotata di strumenti organizzativi (organigrammi, documenti organizzativi, procedure, ecc.) improntati a principi generali di:

- conoscibilità all'interno della Società;
 - chiara descrizione delle linee di riporto;
 - chiara e formale delimitazione dei ruoli, con descrizione dei compiti e delle responsabilità attribuite a ciascuna funzione.
- Deleghe di poteri.
Il sistema di deleghe riguarda sia i poteri autorizzativi interni, dai quali dipendono i processi decisionali dell'azienda in merito alle operazioni da porre in essere, sia i poteri di rappresentanza per la firma di atti o documenti destinati all'esterno e idonei a vincolare la Società

(cosiddette "procure" speciali o generali). Le deleghe di poteri devono rispettare i seguenti requisiti: (i) essere chiaramente definite e formalmente assegnate tramite comunicazioni scritte; (ii) essere coerenti con le responsabilità ed i compiti delegati e con le posizioni ricoperte nell'ambito della struttura organizzativa; (iii) prevedere limiti di esercizio in coerenza con i ruoli attribuiti, con particolare attenzione ai poteri di spesa e ai poteri autorizzativi e/o di firma delle operazioni e degli atti considerati "a rischio" in ambito aziendale; (vi) essere aggiornate in conseguenza dei mutamenti organizzativi.

All'OdV, pertanto, deve essere comunicata sia la struttura organizzativa sia il sistema di deleghe di Telespazio S.p.A. ed ogni modifica che intervenga sulle stesse.

5. FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE.

5.1. FORMAZIONE DEL PERSONALE.

Telespazio S.p.A. promuove la conoscenza del Modello, dei relativi protocolli interni e dei loro aggiornamenti tra tutti i dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e contribuire alla loro attuazione.

Ai fini dell'attuazione del Modello la Funzione Risorse Umane, Organizzazione e Information Technology gestisce in cooperazione con l'OdV, la formazione del personale che sarà articolata sui livelli qui di seguito indicati:

- Vertice Aziendale, dirigenti e personale con funzioni di rappresentanza dell'Ente: corso di formazione iniziale, accesso all'intranet aziendale con spazio dedicato all'argomento e aggiornato in collaborazione con l'OdV; occasionali e-mail di aggiornamento;
- Altro personale: informativa in sede di assunzione per i neo assunti; corso di formazione iniziale realizzato con modalità "e-learning" attraverso supporto informatico, esteso di volta in volta a tutti i neo assunti; nota informativa interna; accesso ad intranet; e-mail di aggiornamento.

5.2. INFORMATIVA A COLLABORATORI ESTERNI E PARTNER.

Telespazio S.p.A. promuove la conoscenza e l'osservanza del Modello anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori.

A questi verranno pertanto fornite apposite informative sui principi, le politiche e le procedure che Telespazio S.p.A. ha adottato sulla base del presente Modello, nonché i testi delle clausole contrattuali che,

coerentemente a detti principi, politiche e procedure, verranno adottate dalla Società.

6. IL SISTEMA SANZIONATORIO

6.1. PRINCIPI GENERALI

Ai sensi degli artt. 6, comma 2, lett. e), e 7, comma 4, lett. b) del Decreto Legislativo 231/2001, i modelli di organizzazione, gestione e controllo, la cui adozione ed attuazione (unitamente alle altre situazioni previste dai predetti articoli 6 e 7) costituisce condizione *sine qua non* quale presupposto di esenzione di responsabilità della Società in caso di commissione dei reati di cui al Decreto, possono ritenersi efficacemente attuati solo se prevedano un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in essi indicate.

Tale sistema disciplinare deve rivolgersi tanto ai lavoratori dipendenti quanto ai collaboratori e terzi che operino per conto della Società, prevedendo idonee sanzioni di carattere disciplinare in un caso e di carattere contrattuale/negoziale (es. risoluzione del contratto, cancellazione dall'elenco fornitori, ecc.) nell'altro caso.

L'applicazione delle sanzioni disciplinari prescinde dall'avvio o dall'esito di un eventuale procedimento penale, in quanto i modelli di organizzazione e le procedure interne costituiscono regole vincolanti per i destinatari, la violazione delle quali deve, al fine di ottemperare ai dettami del citato Decreto Legislativo, essere sanzionata indipendentemente dall'effettiva realizzazione di un reato o dalla punibilità dello stesso.

6.2. SANZIONI PER I LAVORATORI DIPENDENTI (NON DIRIGENTI)

Con riguardo ai lavoratori dipendenti, il sistema disciplinare relativo al personale dipendente non dirigente applicato in Telespazio S.p.A. è specificamente regolato dal vigente Contratto Collettivo Nazionale di Lavoro applicato in Azienda nonché dagli eventuali accordi ed atti ad esso correlati .

Per le sanzioni irrogabili e le relative esemplificazioni di ipotesi di infrazioni (che per loro stessa natura non hanno carattere né pretesa di esaustività circa la casistica dei comportamenti rilevanti ai fini dei provvedimenti disciplinari) si rinvia ai documenti sopra citati.

Al riguardo, si sottolinea in particolare, che la Società rende edotti i propri dipendenti del fatto che il Modello di Organizzazione, Gestione e Controllo costituisce espressione del potere del datore di lavoro di impartire disposizioni per l'esecuzione e per la disciplina del lavoro (art. 2104 c.c.) e che, conseguentemente il mancato rispetto e/o la violazione delle stesse, delle regole di comportamento imposte dal Codice Etico e/o dalle

procedure aziendali, ad opera di lavoratori dipendenti della Società, costituiscono inadempimento alle obbligazioni derivanti dal rapporto di lavoro e illecito disciplinare (art. 2106 c.c.) e, in quanto tali, possono comportare la comminazione delle sanzioni previste dalla normativa vigente e dalla contrattazione collettiva.

Al fine quindi di ottemperare alle previsioni del d.lgs. 231/2001 con riguardo all'adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto da parte dei dipendenti non dirigenti delle misure previste nei Modelli di Organizzazione, Gestione e Controllo, e/o del Codice Etico la Società si avvale quindi del sistema disciplinare già esistente sopra richiamato.

In ogni caso, la Società potrà, al fine di attribuire al Sistema sanzionatorio una maggiore chiarezza, ulteriormente integrare e ampliare, dandone conoscenza a tutti i dipendenti, con le previste e consuete modalità, l'elenco esemplificativo di comportamenti sanzionabili con alcune ipotesi riferite all'osservanza del Modello ex d.lgs. 231/2001 e del Codice Etico.

Nella contestazione degli illeciti e nell'irrogazione delle sanzioni devono essere rispettate le procedure previste dalla legge, dal CCNL e da eventuali ulteriori accordi vigenti.

Nell'irrogazione della sanzione disciplinare sarà necessariamente rispettato il principio della proporzionalità tra infrazione e sanzione e si terrà conto di eventuali circostanze attenuanti la gravità del comportamento (attività diretta a rimuovere o impedire le conseguenze dannose, entità del danno o delle conseguenze, ecc.).

L'adeguatezza del sistema disciplinare alle prescrizioni del Decreto 231/2001 sarà costantemente monitorata dall'Organismo di Vigilanza, al quale dovrà essere garantito un adeguato flusso informativo in merito alle tipologie di sanzioni comminate ed alle circostanze poste a fondamento delle stesse.

L'accertamento delle suddette infrazioni, eventualmente su segnalazione dell'Organismo di Vigilanza, la gestione dei procedimenti disciplinari e l'irrogazione delle sanzioni restano di competenza delle Funzioni aziendali a ciò preposte e delegate.

6.3. MISURE NEI CONFRONTI DEI DIRIGENTI

Con riguardo ai dirigenti, in assenza di un sistema disciplinare applicabile agli stessi ed in considerazione del particolare rapporto fiduciario con il datore di lavoro, in caso di violazione dei principi generali dei modelli di organizzazione, gestione e di controllo, delle regole di comportamento imposte dal Codice Etico e/o dalle procedure aziendali, la Società, provvederà ad assumere nei confronti dei responsabili i provvedimenti ritenuti idonei ai sensi di legge e del CCNL applicabile ai Dirigenti industriali

in funzione delle violazioni commesse, tenuto conto che le stesse costituiscono inadempimento alle obbligazioni derivanti dal rapporto di lavoro.

6.4. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

In caso di violazione della normativa vigente, dei modelli di organizzazione e controllo e/o del Codice Etico da parte di componenti del Consiglio di Amministrazione della Società, l'Organismo di Vigilanza informerà l'intero Consiglio d'Amministrazione ed il Collegio Sindacale, i quali dovranno assumere le opportune iniziative ai sensi di legge, coinvolgendo, ove necessario, l'Assemblea.

6.5. MISURE NEI CONFRONTI DI COLLABORATORI, CONSULENTI ED ALTRI SOGGETTI TERZI

Ogni comportamento posto in essere dai collaboratori, dai consulenti o da altri terzi collegati alla Società da un rapporto contrattuale non di lavoro dipendente, in violazione delle previsioni del d.lgs. 231/2001 e/o del Codice Etico per le parti di loro competenza, potrà determinare l'applicazione di penali o, nel caso di grave inadempimento, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento del danno.

A tal fine è previsto, con particolare attenzione alle attività affidate a terzi in "*outsourcing*", l'inserimento nei contratti di specifiche clausole che diano atto almeno della conoscenza del Decreto e del Codice Etico di Telespazio S.p.A. da parte del terzo contraente.

Compete all'Organismo di Vigilanza valutare l'idoneità delle misure adottate dalla Società nei confronti dei collaboratori, dei consulenti e dei terzi e di ogni altro soggetto a qualunque titolo operante per conto della Società e provvedere al loro eventuale aggiornamento.

7. CONFERMA APPLICAZIONE E ADEGUATEZZA DEL MODELLO

Il Modello Organizzativo sarà soggetto a due tipologie di verifiche:

- attività di monitoraggio sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso) attraverso l'istituzione di un sistema di dichiarazioni periodiche da parte dei destinatari del Modello con il quale si conferma che sono state rispettate le indicazioni ed i contenuti del medesimo (vedi scheda di evidenza allegata alla parte speciale "A").

I responsabili delle aree a rischio individuate hanno il compito di far compilare le dichiarazioni ai loro sottoposti e di ritrasmetterle all'Organismo di Vigilanza che ne curerà l'archiviazione ed effettuerà, a campione, il relativo controllo.

- Verifiche delle procedure: annualmente l'effettivo funzionamento del presente Modello sarà verificato con le modalità stabilite dall'OdV. Inoltre, sarà intrapresa una *review* di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'OdV e dagli altri soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal Decreto, con verifiche a campione.

L'esito di tale verifica, con l'evidenziazione delle possibili manchevolezze ed i suggerimenti delle azioni da intraprendere, sarà comunicata al Consiglio di Amministrazione della Società.

PARTE SPECIALE "A"

Reati in danno della Pubblica Amministrazione

A.1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)

Si riporta di seguito una breve descrizione dei reati contemplati negli artt. 24 e 25 del Decreto.

i. Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.)

Il reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri Enti pubblici o dall'Unione Europea.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316 bis c.p.), non assume alcun rilievo la destinazione dei finanziamenti pubblici erogati, poiché il reato si consuma al momento del loro - indebito - ottenimento.

Va infine evidenziato che tale reato, avendo natura residuale, si configura solo qualora la condotta non integri gli estremi del più grave reato di truffa aggravata ai danni dello Stato (art. 640 bis c.p.).

ii. Truffa aggravata in danno dello Stato o di altro Ente pubblico (art. 640, comma 2 n. 1, c.p.)

Il reato si configura qualora, utilizzando artifici o raggiri e in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro Ente pubblico o dell'Unione Europea.

Tale reato può realizzarsi quando, ad esempio, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenerne l'aggiudicazione.

iii. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.)

Il reato si configura qualora la condotta di truffa sopra descritta abbia ad oggetto finanziamenti pubblici, comunque denominati, erogati dallo Stato, dai altri Enti pubblici o dall'Unione Europea.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

iv. Frode informatica in danno dello Stato o di altro Ente pubblico (art. 640 ter, comma 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro Ente pubblico.

In concreto, il reato in esame potrebbe configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto.

v. Corruzione (artt. 318-319 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio si faccia dare o promettere, per sé o per altri, denaro o altra utilità per compiere, omettere o ritardare atti del suo ufficio ovvero per compiere atti contrari ai suoi doveri di ufficio.

Il reato si configura altresì nel caso in cui l'indebita offerta o promessa sia formulata con riferimento ad atti – conformi o contrari ai doveri d'ufficio – già compiuti dal pubblico agente.

Il reato sussiste dunque sia nel caso in cui il pubblico ufficiale, dietro corrispettivo, compia un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia nel caso in cui compia un atto contrario ai suoi doveri (ad esempio: garantire l'illegittima aggiudicazione di una gara).

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

A norma dell'art. 321 c.p., le pene previste per i pubblici ufficiali e gli incaricati di pubblico servizio si applicano anche ai privati che danno o promettono a quest'ultimi denaro o altra utilità.

vi. Corruzione in atti giudiziari (art. 319 ter)

Il reato si configura nel caso in cui taluno offra o prometta ad un pubblico ufficiale o ad un incaricato di un pubblico servizio denaro o

altra utilità al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Potrà dunque essere chiamata a rispondere del reato la società che, essendo parte in un procedimento giudiziario, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario) al fine di ottenerne la positiva definizione.

vii. Istigazione alla corruzione (art. 322 c.p.)

La pena prevista per tale reato si applica a chiunque offra o prometta denaro ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per indurlo a compiere un atto contrario o conforme ai doveri d'ufficio, qualora la promessa o l'offerta non vengano accettate. Parimenti, si sanziona la condotta del pubblico agente che solleciti una promessa o un'offerta da parte di un privato.

viii. Concussione (art. 317 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua qualità o del suo potere, costringa o induca taluno a dare o promettere indebitamente, a sé o ad altri, denaro o altra utilità.

Il reato in esame presenta profili di rischio contenuti ai fini del d.lgs. 231/01: trattandosi infatti di un reato proprio di soggetti qualificati, la responsabilità dell'Ente potrà ravvisarsi solo nei casi in cui un Dipendente od un Agente della Società, nell'interesse o a vantaggio della stessa, *concorra* nel reato del pubblico ufficiale o dell'incaricato di pubblico servizio, che, approfittando della loro posizione, esigano prestazioni non dovute.

ix. Malversazione a danno dello Stato (art. 316 bis c.p.)

Il reato punisce il fatto di chi, avendo ottenuto dallo Stato, da altro Ente pubblico o dalla Unione Europea, finanziamenti, comunque denominati, destinati a favorire la realizzazione di opere o attività di pubblico interesse, non li destina agli scopi previsti.

Poiché il fatto punito consiste nella mancata destinazione del finanziamento erogato allo scopo previsto, il reato può configurarsi anche con riferimento a finanziamenti ottenuti in passato e che non vengano ora destinati alle finalità per cui erano stati erogati.

A completamento dell'esame dei reati previsti dall'art. 24 del decreto (concussione, corruzione, istigazione alla corruzione e corruzione in atti

giudiziari), si evidenzia che, a norma dell'art. 322 bis c.p., i suddetti reati sussistono anche nell'ipotesi in cui essi riguardino pubblici ufficiali stranieri, ossia coloro che svolgano funzioni analoghe a quelle dei pubblici ufficiali italiani nell'ambito di organismi comunitari, di altri Stati membri dell'Unione Europea, di Stati esteri o organizzazioni pubbliche internazionali.

A.2. NOZIONE DI PUBBLICO UFFICIALE E INCARICATO DI PUBBLICO SERVIZIO (ARTT. 357-358 C.P.)

Preliminare all'analisi dei delitti di concussione e corruzione è la delimitazione delle nozioni di pubblico ufficiale e incaricato di pubblico servizio, soggetti attivi di detti reati.

In particolare, vengono definiti pubblici ufficiali o incaricati di un pubblico servizio:

- 1) soggetti che svolgono una pubblica funzione legislativa o amministrativa, quali, ad esempio:
 - parlamentari e membri del Governo;
 - consiglieri regionali e provinciali;
 - parlamentari europei e membri del Consiglio d'Europa;
 - soggetti che svolgono funzioni accessorie (addetti alla conservazione di atti e documenti parlamentari, alla redazione di resoconti stenografici, di economato, tecnici, ecc.);
- 2) soggetti che svolgono una pubblica funzione giudiziaria, quali, ad esempio:
 - magistrati (magistratura ordinaria di tribunali, Corti d'Appello, Suprema Corte di Cassazione, Tribunale Superiore delle Acque, TAR, Consiglio di Stato, Corte Costituzionale, tribunali militari, giudici popolari delle Corti d'Assise, giudici di pace, vice pretori onorari ed aggregati, membri di collegi arbitrali rituali e di commissioni parlamentari di inchiesta, magistrati della Corte Europea di Giustizia, nonché delle varie corti internazionali, ecc.);
 - soggetti che svolgono funzioni collegate (ufficiali e agenti di polizia giudiziaria, guardia di finanza e carabinieri, cancellieri, segretari, custodi giudiziari, ufficiali giudiziari, testimoni, messi di conciliazione, curatori fallimentari, operatori addetti al rilascio di certificati presso le cancellerie dei tribunali, periti e consulenti del Pubblico Ministero, commissari liquidatori nelle procedure fallimentari, liquidatori del concordato preventivo, commissari straordinari dell'amministrazione straordinaria delle grandi imprese in crisi ecc.);

- 3) soggetti che svolgono una pubblica funzione amministrativa, quali, ad esempio:
- dipendenti dello Stato, di organismi internazionali ed esteri e degli enti territoriali (ad esempio funzionari e dipendenti dello Stato, dell'Unione Europea, di organismi sopranazionali, di Stati esteri e degli Enti territoriali, ivi comprese le Regioni, le Province, i Comuni e le Comunità montane; soggetti che svolgano funzioni accessorie rispetto ai fini istituzionali dello Stato, quali componenti dell'ufficio tecnico comunale, membri della commissione edilizia, capo ufficio amministrativo dell'ufficio condoni, messi comunali, addetti alle pratiche riguardanti l'occupazione del suolo pubblico, corrispondenti comunali addetti all'ufficio di collocamento, dipendenti delle aziende di Stato e delle aziende municipalizzate; soggetti addetti all'esazione dei tributi, personale sanitario delle strutture pubbliche, personale dei ministeri, delle soprintendenze ecc.);
 - dipendenti di altri enti pubblici, nazionali ed internazionali (ad esempio funzionari e dipendenti della Camera di Commercio, della Banca d'Italia, delle Autorità di Vigilanza, degli istituti di previdenza pubblica, dell'ISTAT, dell'ONU, della FAO, ecc.);
 - privati esercenti pubbliche funzioni o pubblici servizi (ad esempio notai, Enti privati operanti in regime di concessione o la cui attività sia comunque regolata da norme di diritto pubblico o che comunque svolgano attività di interesse pubblico o siano controllate in tutto o in parte dallo Stato, ecc.).

Non sono considerate pubblico servizio le attività che, pur disciplinate da norme di diritto pubblico o da atti autoritativi, consistono tuttavia nello svolgimento di semplici mansioni di ordine o nella prestazione di opera meramente materiale (cioè attività di prevalente natura applicativa od esecutiva, non comportanti alcuna autonomia o discrezionalità o che prevedono unicamente il dispiegamento di energia fisica: ad esempio, operatore ecologico, dipendente comunale addetto alla sepoltura di salme ecc.).

La figura del pubblico ufficiale e dell'incaricato di pubblico servizio sono individuate non sulla base del criterio della appartenenza o dipendenza da un Ente pubblico, ma con riferimento alla natura dell'attività svolta in concreto dalla medesima, ovvero, rispettivamente, pubblica funzione e pubblico servizio.

Anche un soggetto estraneo alla pubblica amministrazione può dunque rivestire la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, quando eserciti una delle attività definite come tali dagli artt. 357 e 358 c.p. (ad es. vedasi, dipendenti di istituti bancari ai quali siano affidate mansioni rientranti nel "pubblico servizio", ecc.).

Inoltre, l'art. 322 bis estende la punibilità dei reati di corruzione e di concussione e di altri reati contro la PA anche alle ipotesi in cui l'illecito coinvolga:

- un membro della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei Conti delle Comunità europee;
- un funzionario, agente operante presso le Comunità europee o un soggetto che svolga funzioni equivalenti;
- un soggetto che, nell'ambito di altri Stati membri dell'Unione europea, svolge funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio;
- un soggetto che esercita funzioni o attività corrispondenti a quelle dei pubblici ufficiali e dell'incaricato di pubblico servizio nell'ambito di Stati esteri non appartenenti all'Unione europea od organizzazioni pubbliche internazionali.

A.3. AREE A RISCHIO

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato e tale da comprendere anche la Pubblica Amministrazione di Stati esteri).

Vengono pertanto definite aree a rischio tutte quelle aree aziendali che per lo svolgimento della propria attività intrattengono rapporti con le pubbliche amministrazioni. Aree di Supporto vengono definite quelle aree di attività aziendale che gestiscono strumenti di tipo finanziario e/o mezzi sostitutivi che, pur non intrattenendo rapporti con la Pubblica Amministrazione, possono supportare la commissione di reati.

Tenuto conto, pertanto della molteplicità dei rapporti che Telespazio S.p.A., intrattiene con le Amministrazioni Pubbliche in Italia ed all'estero, sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

Aree a rischio reato:

- 1) Commercializzazione e Gestione del Cliente;
- 2) Marketing e Comunicazione;
- 3) Relazioni Istituzionali;
- 4) Gestione del Contenzioso;
- 5) Finanziamenti agevolati per le attività formative;
- 6) Gestione dei rapporti con uffici finanziari e tributari;
- 7) Gestione delle commesse;
- 8) Gestione delle attività relative ad autorizzazioni e licenze;
- 9) Gestione delle attività connesse ai finanziamenti agevolati;
- 10) Gestione con Enti Istituzionali e Previdenziali;
- 11) Gestione delle attività di collaudo;
- 12) Gestione delle attività di import ed export;

- 13) Gestione degli adempimenti previsti dalla normativa di sicurezza del lavoro;
- 14) Gestione della sicurezza industriale;
- 15) Gestione del sistema qualità;
- 16) Gestione dei contratti di agenzia.

Aree di supporto:

- 17) Gestione dei sistemi informativi;
- 18) Budget e Controllo di gestione;
- 19) Contabilità clienti;
- 20) Contabilità fornitori;
- 21) Finanza e tesoreria;
- 22) Amministrazione e Fiscale;
- 23) Gestione del patrimonio aziendale;
- 24) Gestione della movimentazione delle merci;
- 25) Affari societari;
- 26) Attività di cortesia commerciale;
- 27) Approvvigionamenti;
- 28) Selezione del personale;
- 29) Sviluppo e formazione risorse umane;
- 30) Gestione amministrativa del personale.

Eventuali integrazioni delle suddette aree d'attività a rischio potranno essere proposte dal Presidente, dall'Amministratore Delegato e dal Direttore Generale di Telespazio S.p.A. al Consiglio di Amministrazione della società.

Le aree a rischio reato così identificate hanno costituito il punto di riferimento nella definizione delle procedure di controllo da implementare ai fini dell'adeguamento dell'attuale sistema di controlli interno.

La tipologia e la periodicità delle procedure di controllo implementate sulle diverse aree a rischio reato, sono state definite tenendo in considerazione la rilevanza dei singoli punti di contatto con la Pubblica Amministrazione.

A.4. DESTINATARI DELLA PARTE SPECIALE - PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO

La presente Parte Speciale si riferisce a comportamenti posti in essere da Amministratori, Dirigenti e Dipendenti ("Esponenti Aziendali") operanti nelle aree di attività a rischio nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i "Destinatari").

La presente Parte Speciale prevede l'espresso divieto, per gli Esponenti Aziendali, in via diretta, e per i Collaboratori esterni e Partner, tramite apposite clausole contrattuali di:

- 1) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
- 2) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- 3) porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti (sanciti anche dal Codice Etico adottato in ambito Telespazio S.p.A.) è fatto divieto in particolare di:

- 1) effettuare elargizioni in denaro a pubblici funzionari;
- 2) distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice Etico, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto 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 (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. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte). I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- 3) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto 2);

- 4) effettuare prestazioni in favore dei Partner che non trovino adeguata giustificazione nel contesto del rapporto associativo costituito con i Partner stessi;
- 5) riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- 6) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- 7) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- 1) i rapporti nei confronti della P.A. per le suddette aree di attività a rischio devono essere gestiti in modo unitario, procedendo alla nomina di un apposito responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio;
- 2) gli accordi di associazione con i Partner devono essere definiti per iscritto con l'evidenziazione di tutte le condizioni dell'accordo stesso - in particolare per quanto concerne le condizioni economiche concordate per la partecipazione congiunta alla procedura - e devono essere proposti o verificati o approvati da almeno due soggetti appartenenti a Telespazio S.p.A.;
- 3) gli incarichi conferiti ai Collaboratori esterni devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito ed essere sottoscritti conformemente alle deleghe ricevute;
- 4) nessun tipo di pagamento può esser effettuato in cash o in natura;
- 5) le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
- 6) coloro che svolgono una Funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità.

A.5. AREE DI ATTIVITÀ A RISCHIO: ELEMENTI FONDAMENTALI DEL PROCESSO DECISIONALE

A.5.1. SINGOLE OPERAZIONI A RISCHIO: INDIVIDUAZIONE DEI RESPONSABILI INTERNI E SCHEDE DI EVIDENZA

Occorre dare debita evidenza delle operazioni svolte nelle aree a rischio di cui al precedente paragrafo A.3

A tal fine il Presidente, l'Amministratore Delegato, il Direttore Generale e i Responsabili delle Funzioni all'interno delle quali vengano svolte operazioni a rischio divengono *responsabili interni* di ogni singola operazione a rischio da loro direttamente svolta o attuata nell'ambito della Funzione a loro facente capo. Detti responsabili:

- divengono i soggetti referenti dell'operazione a rischio;
- sono responsabili in particolare dei rapporti con le P.A., per le attività con esse svolte.

Le attività a rischio debbono essere portate a conoscenza dell'OdV dai suddetti responsabili tramite la compilazione di apposite Schede di evidenza (di seguito le "Schede") da aggiornarsi su base periodica (vedere format allegato) da cui risulti:

- le Pubbliche Amministrazioni che hanno competenza sulle procedure oggetto dell'operazione;
- la dichiarazione rilasciata dal Responsabile Interno, per sé e per i sub-responsabili interni delegati a svolgere attività che comportano rapporti con la Pubblica Amministrazione, da cui risulti che lo stesso è pienamente a conoscenza degli adempimenti da espletare e degli obblighi da osservare nello svolgimento delle operazioni e che non è incorso in reati considerati dal Decreto;
- l'indicazione delle principali iniziative e dei principali adempimenti svolti nell'espletamento delle operazioni.

Sulle operazioni in questione l'OdV potrà predisporre ulteriori controlli dei quali verrà data evidenza scritta.

A.5.2. ISTRUZIONI E VERIFICHE DELL'ODV

E' compito dell'OdV:

- 1) curare l'emanazione e l'aggiornamento di istruzioni standardizzate relative a:
 - la compilazione omogenea e coerente delle Schede di Evidenza;
 - gli atteggiamenti da assumere nell'ambito delle Attività a rischio e, in genere, nei rapporti da tenere nei confronti della P.A..

Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

- 2) verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile interno od ai sub responsabili;
- 3) verificare periodicamente, con il supporto delle altre funzioni competenti, la validità di opportune clausole standard finalizzate:
 - all'osservanza da parte dei Collaboratori esterni e dei partner delle disposizioni del Decreto;
 - alla possibilità di Telespazio S.p.A. di effettuare efficaci azioni di controllo nei confronti dei Destinatari del Modello al fine di verificare il rispetto delle prescrizioni in esso contenute;
 - all'attuazione di meccanismi sanzionatori (quali il recesso dal contratto nei riguardi di Partner o di Collaboratori esterni) qualora si accertino violazioni delle prescrizioni;
- 4) indicare al management le eventuali integrazioni ai sistemi di gestione finanziaria già presenti in Telespazio S.p.A., con l'evidenza degli accorgimenti opportuni a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

 TELESPAZIO <small>A Finmeccanica / Thales Company</small>	Scheda di evidenza	Doc Nr: XXX-SDE-ZZZ Pag. ____ di ____
---	---------------------------	--

Nominativo Responsabile Interno: _____

Periodo di riferimento: _____

Funzione Aziendale: _____

All'Organismo di Vigilanza di Telespazio S.p.A.

Premesso che:

- Telespazio S.p.A. ha predisposto il proprio Modello di Organizzazione, Gestione e controllo ai sensi del d. lgs. 231/01;
- tale Modello è stato approvato dal Consiglio di Amministrazione del 23/02/2004 ed aggiornato con delibera del 28/06/2006 e del 09/06/2009;
- la Parte Speciale A ("Reati in danno della Pubblica Amministrazione") al punto A.5.1 prevede, da parte di ogni Responsabile Interno, la predisposizione di schede di evidenza dell'attività svolta con la Pubblica Amministrazione.

Il sottoscritto dichiara che nel periodo in esame ha trattato con le Pubbliche Amministrazioni di seguito indicate le seguenti principali iniziative/attività:

Data incontro / contatto	Pubblica Amministrazione/ Ente Pubblico	Referente Pubblica Amministrazione/ Ente Pubblico	Oggetto dell'incontro / contatto	Referente Telespazio

L'eventuale documentazione è disponibile presso i competenti Uffici della Società.

Il sottoscritto dichiara di essere a conoscenza di quanto contenuto nel Modello di Organizzazione Gestione e Controllo di Telespazio S.p.A. e non segnala, con riferimento ai propri rapporti con le Pubbliche Amministrazioni di cui sopra – ed a quelli intrattenuti con le medesime da propri collaboratori all'uopo delegati e le cui attività sono state debitamente controllate e monitorate – alcuna anomalia o infrazione al Modello stesso.

(firma)

.....

Data:/...../.....

PARTE SPECIALE "B"

Reati societari, reati e illeciti di market abuse

Altri reati

B.1. LA TIPOLOGIA DEI REATI SOCIETARI E DEI REATI E ILLECITI DI MARKET ABUSE (ARTT. 25 TER E 25 SEXIES DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25 *ter* e 25 *sexies* del Decreto la cui commissione possa comunque comportare un beneficio per la Società.

i. False comunicazioni sociali (artt. 2621 e 2622 c.c.)

Si tratta di due modalità di reato la cui condotta tipica coincide quasi totalmente e che si differenziano per il verificarsi o meno di un danno patrimoniale per i soci o i creditori. La prima (art. 2621 c.c.) è una fattispecie di pericolo ed è costruita come una contravvenzione dolosa; la seconda (art. 2622 c.c.) è costruita come un reato di danno.

Le due fattispecie si realizzano con l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali che, ancorché oggetto di valutazioni, non siano veritieri e possano indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico d'esercizio al lordo delle imposte non superiore al 5% o una variazione del patrimonio netto non superiore all'1%; in ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate differiscono in misura non superiore al 10% di quella corretta;
- la responsabilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i sindaci ed i liquidatori (reato proprio).

ii. Falso in prospetto (art. 173 bis TUF)

Commette il reato chi, nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche d'acquisto o di scambio, espone false informazioni od occulta dati o notizie in modo tale da indurre in errore i destinatari del prospetto (1° comma) ed è una fattispecie delittuosa nell'eventualità che il danno si verifichi (2° comma).

Si precisa che:

- deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto (dolo generico);
- la condotta deve essere idonea ad indurre in inganno i destinatari del prospetto;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto (dolo specifico).

Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta incriminata.

Il reato si configura come delitto o contravvenzione a seconda che la condotta abbia o meno causato danni patrimoniali ai destinatari del prospetto.

iii. Falsità nelle relazioni o nelle comunicazioni della Società di Revisione (art. 2624 c.c.)

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, concernenti la situazione economica patrimoniale o finanziaria della società al fine di conseguire per sé o per gli altri un ingiusto profitto.

La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.

Soggetti attivi sono i responsabili della Società di Revisione (reato proprio) ma anche i componenti del Consiglio di Amministrazione di Telespazio S.p.A. nonché i dipendenti che possono essere coinvolti a titolo di concorso nel reato. E', infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del responsabile della società di revisione.

iv. Impedito controllo (art. 2625 c.c.)

Il reato consiste nell'ostacolare o impedire lo svolgimento delle attività di controllo e/o di revisione - legalmente attribuite ai soci, ad organi sociali o a Società di Revisione - attraverso l'occultamento di documenti od altri idonei artifici.

Il reato, imputabile esclusivamente agli amministratori, è punito più gravemente se la condotta ha causato un danno.

v. Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Il reato si realizza attraverso riduzioni di capitale sociale, fusioni con altre società o scissioni attuate in violazione delle disposizioni di legge e che cagionino danno ai creditori (reato di evento).

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

vi. Illecita influenza sull'assemblea (art.2636 c.c.)

Il reato si attua quando con atti simulati o con frode si determina la maggioranza in assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Il reato può essere commesso da chiunque ("reato comune"), quindi anche da soggetti esterni alla società.

vii. Aggiotaggio (art. 2637 c.c.)

La realizzazione del reato avviene attraverso la diffusione di notizie false o attraverso operazioni o artifici che provochino una sensibile alterazione del prezzo di strumenti finanziari, quotati o meno, e/o idonei ad accrescere la fiducia del pubblico o di istituti finanziari nella stabilità patrimoniale.

Anche questo è un reato comune che può essere commesso da chiunque.

viii. Ostacolo all'esercizio delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Il reato può realizzarsi attraverso due distinte modalità entrambe finalizzate ad ostacolare l'attività di vigilanza delle autorità pubbliche preposte:

- attraverso comunicazioni alle autorità di vigilanza di fatti, sulla situazione economica, patrimoniale o finanziaria, non

corrispondenti al vero, ovvero con l'occultamento, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati;

- attraverso il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi modo.

In entrambe le modalità descritte i soggetti attivi nella realizzazione del reato sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

ix. Abuso di informazioni privilegiate (art. 184 TUF)

Il reato può realizzarsi attraverso tre distinte modalità da chiunque, essendo in possesso di informazioni privilegiate in ragione del suo incarico:

- acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari, utilizzando le informazioni medesime;
- comunica le informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
- raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nel punto i.

In tutte le modalità descritte i soggetti attivi nella realizzazione del reato sono gli amministratori, i direttori generali, i sindaci e i liquidatori e tutti coloro che intrattengono con l'Ente rapporti professionali e/o funzionali.

x. Manipolazione del mercato (art. 185 TUF)

Il reato può realizzarsi da chiunque diffonda notizie false o ponga in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

I soggetti attivi nella realizzazione del reato sono gli amministratori, i direttori generali, i sindaci e i liquidatori e tutti coloro che intrattengono con l'Ente rapporti professionali e/o funzionali.

B.2. ALTRI REATI

i. Reati contro la personalità individuale

Tale categoria di reati include, in particolare, i seguenti delitti:

- riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- tratta di persone (art. 601 c.p.);
- acquisto e alienazione di schiavi (art. 602 c.p.);

- reati connessi alla prostituzione minorile e allo sfruttamento della stessa (art. 600 bis c.p.);
- reati connessi alla pornografia minorile e allo sfruttamento della stessa (art. 600 ter c.p.);
- detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori (art. 600 quater c.p.);
- iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.);
- pornografia virtuale (art. 600 quater.I c.p.).

Ai sensi dell'art. 25 quinquies del d.lgs. 231/2001, sono comminate sanzioni interdittive (oltre a sanzioni pecuniarie) a carico delle società i cui amministratori o dipendenti (così come definiti nell'art. 5 del medesimo d.lgs. 231/2001) commettono, nell'interesse o a vantaggio delle società stesse, i delitti di cui agli artt. 600; 600 bis, primo comma; 600 ter, primo e secondo comma, anche se relativi al materiale pornografico di cui all'art. 600 quater.Iii; 600 quinquies; 601; 602, del codice penale.

ii. Reati transnazionali

Ai sensi dell'art. 3 della legge di autorizzazione alla ratifica della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale si considera reato transnazionale "il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- sia commesso in più di uno Stato;
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato".

Il reato in questione è aggravato se alla commissione dello stesso abbia dato il suo contributo un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato (la pena è aumentata da un terzo alla metà).

ⁱⁱ Parole inserite dall'art. 10 della legge 6 febbraio 2006, n. 38 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet".

In relazione alla responsabilità amministrativa degli Enti per i reati transnazionali, si applicheranno, in base all'art. 10 della legge di autorizzazione alla ratifica, le seguenti disposizioni:

- per i delitti previsti dagli artt. 416 (Associazione per delinquere) e 416 bis (Associazione di tipo mafioso) c.p., dall'art. 291 quater del testo unico di cui al D.P.R. 43/1973 (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri.), e dall'art. 74 del testo unico di cui al D.P.R. 309/1990 (Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope.), si applica all'Ente la sanzione amministrativa pecuniaria da quattrocento a mille quote; in caso di condanna, si applicano all'Ente le sanzioni interdittive previste dall'art. 9, comma 2, del d.lgs. 231/2001, per una durata non inferiore ad un anno. Se l'Ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nel comma 2, si applica all'Ente la sanzione amministrativa dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3, del d.lgs. 231/2001;
- per i reati concernenti il riciclaggio (artt 648 bis e 648 ter c.p.), si applica all'Ente la sanzione amministrativa pecuniaria da duecento a ottocento quote; si applicano all'Ente le sanzioni interdittive previste dall'articolo 9, comma 2, del d.lgs. 231/2001, per una durata non superiore a due anni.
- per i reati concernenti il traffico di migranti (art. 12, commi 3, 3 bis, 3 ter e 5, del d.lgs. 286/1998,) si applica all'Ente la sanzione amministrativa pecuniaria da duecento a mille quote; si applicano all'Ente le sanzioni interdittive previste dall'art. 9, comma 2, del d.lgs. 231/2001, per una durata non superiore a due anni.
- per i reati concernenti l'intralcio alla giustizia (artt 377 bis e 378 c.p.), si applica all'Ente la sanzione amministrativa pecuniaria fino a cinquecento quote.
- A tutti gli illeciti amministrativi previsti dall'art. 10 si applicano le disposizioni di cui al d.lgs. 231/2001".

B.3. PRINCIPALI AREE DI ATTIVITA' A RISCHIO DI COMMISSIONE DEI REATI

Le aree di attività considerate più specificatamente a rischio per Telespazio S.p.A., in relazione ai reati societari, sono le seguenti:

- 1) redazione del bilancio, relazione sulla gestione, bilancio consolidato e altre comunicazioni sociali;

- 2) operazioni societarie che in generale riguardano la sfera del patrimonio ed in particolare che possono incidere sull'integrità del capitale sociale;
- 3) ripartizione dei beni sociali da parte dei liquidatori di talune partecipate del Gruppo.
- 4) informative periodiche ai mercati finanziari (road show);
- 5) le attività soggette a vigilanza da parte delle autorità pubbliche;
- 6) informative e rapporti con gli organi di informazione e stampa.

Tenendo conto dell'appartenenza di Telespazio S.p.A. al Gruppo Finmeccanica è necessario considerare anche le seguenti attività:

- 7) salvaguardia del rapporto istituzionale di Finmeccanica con le autorità pubbliche di vigilanza garantendo che la comunicazione alla Capogruppo di informazioni di carattere economico, finanziario e patrimoniale del gruppo Telespazio sia completa, accurata e tempestiva;
- 8) gestione dei rapporti con gli organi di informazione e stampa. La diffusione di informazioni "price sensitive" per il Gruppo Telespazio potrebbe, indirettamente, comportare un'alterazione della quotazione dei titoli Finmeccanica.

Per quanto concerne i reati societari di "False comunicazioni sociali (art. 2621)" e "False comunicazioni sociali in danno dei soci o dei creditori (art. 2622) sono state altresì individuate le voci del Bilancio che possono alterare, in modo "sensibile", la rappresentazione della situazione economica, patrimoniale e finanziaria della società e del Gruppo e dunque essere rilevanti ai sensi degli articoli 2621 e 2622. I fattori considerati per l'individuazione di tali voci sono stati:

- materialità in Bilancio;
- margini di soggettività nella loro determinazione.

Le voci di Bilancio individuate sono le seguenti:

- Commesse in corso di lavorazione;
- Fondi di accantonamento per rischi;
- Partecipazioni.

Per gli "Altri reati", oltre alle aree a rischio reato sopra elencate per i reati societari e contro la Pubblica Amministrazione, è necessario considerare anche le aree afferenti l'utilizzo di internet, i servizi resi in

qualità di *service provider* e le aree di attività che prevedano contatti e permanenza all'estero.

La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal Codice Etico adottato da Telespazio S.p.A alla cui osservanza tutti gli amministratori e dipendenti della Società sono tenuti.

B.4. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

Destinatari della presente Parte Speciale "B" sono gli Amministratori, i Sindaci, il Direttore generale, i Dirigenti ed i loro Dipendenti in linea gerarchica che operino nelle aree di attività a rischio (di seguito i "Destinatari").

Ai Destinatari è fatto espresso obbligo di:

- 1) tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società e del Gruppo Telespazio;
- 2) tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, al fine di garantire la tutela del patrimonio degli investitori;
- 3) osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e di agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- 4) assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale prevista dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- 5) garantire che le informazioni di carattere economico, finanziario e patrimoniale da comunicare alle autorità pubbliche di vigilanza (ad esempio l'informativa legata alle società partecipate), siano anche a salvaguardia del rapporto istituzionale di Finmeccanica;

- 6) tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione.
- 7) osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne provochino una sensibile alterazione rispetto alla corrente situazione di mercato.
- 8) Agire nel più rigoroso rispetto di quanto previsto in ordine ai reati contro la personalità individuale, con particolare riferimento allo sfruttamento sessuale dei bambini ed alla pedopornografia anche a mezzo internet.

B.5. PRINCIPI DI ATTUAZIONE DEI COMPORAMENTI DESCRITTI

Di seguito sono descritte le modalità di attuazione dei principi sopra richiamati in relazione alle diverse tipologie di reati societari.

B.5.1. BILANCI ED ALTRE COMUNICAZIONI SOCIALI

Per la prevenzione dei reati di cui alle precedenti lettere 1) e 2) la redazione del bilancio annuale, relazione sulla gestione, relazione semestrale, bilancio consolidato e la scelta della Società di Revisione debbono essere realizzate in base a specifiche procedure aziendali.

Tali procedure debbono prevedere:

- l'elencazione dei dati e delle notizie che ciascun ente/funzione aziendale deve fornire, a quali altri enti/funzioni debbono essere trasmessi, i criteri per la loro elaborazione, la tempistica di consegna;
- la trasmissione dei dati ed informazioni alla funzione responsabile (Chief Financial Officer - CFO) per via informatica in modo che restino tracciati i vari passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- l'enunciazione dei criteri e le modalità per l'elaborazione e la trasmissione dei dati del bilancio consolidato da parte delle società del Gruppo soggette al consolidamento, specificando le responsabilità relative alle varie fasi del processo e le modalità di riconciliazione dei saldi infragruppo;
- la tempestiva trasmissione a tutti i membri del Consiglio di Amministrazione e del Collegio Sindacale e all'OdV della bozza del progetto di bilancio e della relazione della società di revisione, nonché un'idonea registrazione di tale trasmissione;

- riunioni tra la Società di Revisione, il Collegio Sindacale e l'OdV, prima della riunione del Consiglio di Amministrazione che delibererà sul bilancio.
- la sottoscrizione da parte dei responsabili delle funzioni coinvolte nei processi di formazione della bozza del progetto di bilancio o di altre comunicazioni sociali di una dichiarazione di veridicità, completezza e coerenza dei dati e delle informazioni trasmessi;
- la comunicazione all'OdV delle valutazioni che hanno condotto alla scelta della Società di Revisione;
- la comunicazione sistematica e tempestiva all'OdV di qualsiasi altro incarico, conferito o che si intenda conferire, alla Società di Revisione che sia aggiuntivo rispetto a quello della certificazione del bilancio.

Inoltre, nell'attività di predisposizione delle Comunicazioni indirizzate ai Soci, ed al Pubblico in generale, e, in particolare, ai fini della formazione del Bilancio, delle relazioni trimestrali, della relazione semestrale dovrà essere seguito il seguente procedimento:

il Responsabile di Chief Financial Officer (CFO) è tenuto a rilasciare un'apposita dichiarazione attestante:

- la veridicità, correttezza, precisione, e completezza dei dati e delle informazioni contenute nel bilancio o nei documenti contabili sopra indicati, e nei documenti connessi, nonché degli elementi informativi messi a disposizione dalla Società stessa;
- l'avvenuta raccolta delle dichiarazioni di veridicità correttezza, precisione e completezza da parte dei CFO delle Società controllate;
- l'insussistenza di elementi da cui poter desumere che le dichiarazioni ed i dati raccolti contengono elementi incompleti o inesatti;
- la predisposizione di un adeguato sistema di controllo teso a fornire una ragionevole certezza sui dati di bilancio;
- il rispetto delle procedure previste dal presente paragrafo;

la dichiarazione deve essere trasmessa in copia all'OdV.

B.5.2 ESERCIZIO DEI POTERI DI CONTROLLO SULLA GESTIONE SOCIALE.

Per la prevenzione dei reati di cui alle precedenti lettere iv. par. B.1., in attuazione del principio di comportamento enunciato al punto iv del precedente paragrafo B.4., le relative attività devono essere svolte nel rispetto delle regole di Governo Societario e delle procedure aziendali.

Queste debbono prevedere:

- la tempestiva trasmissione al Collegio Sindacale di tutti i documenti relativi ad argomenti posti all'ordine del giorno di Assemblee e Consigli di Amministrazione o sui quali il Collegio debba esprimere un parere;
- messa a disposizione del Collegio Sindacale e della Società di Revisione dei documenti sulla gestione della Società per le verifiche proprie dei due organismi;
- riunioni periodiche tra Collegio Sindacale, Società di revisione ed OdV per verificare l'osservanza delle regole e procedure aziendali in tema di normativa societaria da parte degli amministratori, del management e dei dipendenti.

B.5.3 TUTELA DEL CAPITALE SOCIALE.

Per la prevenzione dei reati di cui alle precedenti lettere v. par. B.1. tutte le operazioni sul capitale sociale della società, di destinazione di utili e riserve, di acquisto e cessione di partecipazioni e rami d'azienda, di fusione, scissione e scorporo, nonché tutte le operazioni, anche nell'ambito del gruppo, che possano potenzialmente ledere l'integrità del capitale sociale debbono essere realizzate in base a specifiche procedure aziendali e di gruppo all'uopo predisposte.

Queste debbono prevedere:

- l'assegnazione di responsabilità decisionali ed operative per le operazioni anzidette nonché i meccanismi di coordinamento tra le diverse funzioni aziendali coinvolte;
- l'informativa da parte del Management aziendale e la discussione delle operazioni anzidette in riunioni tra il Collegio Sindacale, la Società di Revisione e l'OdV;
- l'esplicita approvazione da parte del Consiglio di Amministrazione di Telespazio S.p.A.

B.5.4. PROSPETTI INFORMATIVI.

Per la prevenzione dei reati di cui alle precedenti lettere ii. par. B.1. la redazione, o compartecipazione alla redazione, di prospetti informativi deve essere effettuata in base a specifiche procedure aziendali.

Tali procedure debbono prevedere:

- la verifica della correttezza dei dati e delle informazioni tutte le volte che ve ne sia la possibilità;
- se i dati e/o informazioni utilizzati nel prospetto provengono da fonti esterne alla Società, l'acquisizione di un'attestazione di veridicità da parte dei soggetti esterni;

- l'individuazione di un responsabile per ciascuna operazione di redazione, o partecipazione alla redazione, di prospetto informativo;
- una tempestiva informativa all'OdV, da parte del responsabile dell'operazione, di ciascuna iniziativa che comporti la redazione o la partecipazione alla redazione di prospetti informativi, nonché della loro avvenuta pubblicazione.

Dovrà inoltre essere svolto, anteriormente all'avvio dei lavori per la predisposizione del prospetto, un idoneo programma di formazione di tutti i soggetti coinvolti nell'attività in questione, finalizzato a rendere edotti gli stessi della normativa vigente in materia, e delle fattispecie concrete integranti gli estremi del reato di falso in prospetto, nonché fornire un adeguato supporto ed informazione tecnica ai fini dello svolgimento delle attività di competenza.

B.5.5. ATTIVITÀ SOGGETTE A VIGILANZA.

Al fine di salvaguardare il rapporto istituzionale di Finmeccanica con le autorità pubbliche di vigilanza, le comunicazioni alla Capogruppo di fatti sulla situazione economica, patrimoniale o finanziaria del gruppo Telespazio devono essere effettuate in base a procedure che attribuiscono specifiche responsabilità in particolare per:

- le segnalazioni periodiche previste da leggi e regolamenti;
- la trasmissione di dati e documenti richiesti;

I principi su cui tali procedure trovano fondamento sono:

- qualità e tempestività delle comunicazioni;
- attendibilità delle comunicazioni che devono essere supportate da un sistema informativo affidabile e da controlli interni efficaci;
- adeguata formalizzazione delle procedure in oggetto;

nel corso delle attività ispettive messa a disposizione con tempestività e completezza della documentazione richiesta e massima disponibilità e collaborazione all'espletamento degli accertamenti.

Tutte le comunicazioni e l'informativa trasmessa a Finmeccanica per le attività soggette a vigilanza devono anche essere tenute a disposizione dell'OdV per le verifiche interne periodiche.

B.5.6. GESTIONE RAPPORTI CON LE SOCIETÀ DI REVISIONE.

Nella gestione di tali rapporti, si dovranno osservare le seguenti disposizioni:

- identificazione del personale all'interno della funzione CFO preposto alla trasmissione della documentazione alla Società di Revisione

- possibilità per il Responsabile della Società di Revisione di prendere contatto con l'OdV per verificare congiuntamente situazioni che possano presentare aspetti di criticità in relazione alle ipotesi di reato considerate; anche l'OdV può ravvisare la necessità di prendere contatto con la Società di Revisione per gli stessi motivi;
- divieto di attribuire alla Società di Revisione o ad altre Società appartenenti allo stesso Gruppo, incarichi di consulenza
- necessità di una preventiva autorizzazione da parte del C.d.A. per l'attribuzione alla stessa società di revisione di qualunque incarico, comunque ricompreso nelle attività di revisione contabile, ma diverso dall'incarico conferito ai sensi dell'art. 155 d.lgs n. 58/1998
- preventiva informazione all'OdV in ordine ad ogni proposta di incarico di cui al punto precedente;
- divieto di stipula di contratti di lavoro autonomo o subordinato nei confronti dei dipendenti delle società che effettuano la revisione contabile obbligatoria per i 36 mesi successivi a:
 - la scadenza del contratto tra Telespazio SpA e la stessa Società di Revisione, ovvero:
 - il termine del rapporto contrattuale tra il Dipendente e la Società di Revisione.

B.6. COMPITI DELL'ORGANISMO DI VIGILANZA

I compiti dell'OdV sono i seguenti:

- 1) per quanto riguarda il bilancio e le altre comunicazioni sociali, in ragione del fatto che il bilancio di Telespazio S.p.A. è certificato da una società di revisione, i compiti dell'OdV si limitano a:
 - monitoraggio dell'efficacia delle procedure interne e delle regole di governo societario per la prevenzione dei reati di false comunicazioni sociali;
 - esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;
 - verifica dell'effettiva indipendenza della società di revisione.
- 2) per quanto riguarda le altre attività a rischio:
 - verifiche periodiche sul rispetto delle procedure interne e delle regole di governo societario;

- verifiche periodiche sulle comunicazioni alla Capogruppo di fatti sulla situazione economica, patrimoniale o finanziaria soggetti a vigilanza;
- monitoraggio sull'efficacia delle verifiche atte a prevenire la commissione di reati;
- esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

L'OdV deve riportare i risultati della propria attività di vigilanza e controllo in materia di reati societari con cadenza semestrale al Collegio Sindacale.

PARTE SPECIALE "C"

Reati in materia di salute e sicurezza sul lavoro

C.1. LA TIPOLOGIA DEI REATI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO. (ART. 25 –SEPTIES DEL DECRETO)

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-septies del Decreto.

i. Omicidio colposo (art. 589 c.p.)

La fattispecie in esame si realizza quando si cagiona per colpa la morte di una persona con violazione delle norme per la prevenzione degli infortuni sul lavoro.

ii. Lesioni colpose gravi o gravissime (art. 590, comma 3 c.p.)

La fattispecie in esame si realizza quando si cagiona ad altri per colpa una lesione personale grave o gravissima con violazione delle norme per la prevenzione degli infortuni sul lavoro.

Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale, è perseguibile d'ufficio.

Ai sensi dell'art. 583 c.p., la lesione personale è:

- grave:
 - se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
 - se il fatto produce l'indebolimento permanente di un senso o di un organo;

- gravissima se dal fatto deriva:
 - una malattia certamente o probabilmente insanabile;
 - la perdita di un senso;
 - la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;
 - la deformazione, ovvero lo sfregio permanente del viso.

C.2. PRINCIPALI AREE DI ATTIVITÀ A RISCHIO DI COMMISSIONE DEI REATI

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui all'art. 25-septies del Decreto, le aree a rischio, che rappresentano le fasi del sistema di gestione della sicurezza, di seguito elencate:

- 1) **Pianificazione:** si tratta delle attività di pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro volte a fissare obiettivi coerenti con la politica aziendale, stabilire i processi necessari al raggiungimento degli obiettivi, definire e assegnare risorse.
- 2) **Attuazione e funzionamento:** si tratta delle attività volta a definire strutture organizzative e responsabilità, modalità di formazione, consultazione e comunicazione, modalità di gestione del sistema documentale, di controllo dei documenti e dei dati, le modalità di controllo operativo, la gestione delle emergenze. In particolare:
 - sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro;
 - individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro;
 - attività di informazione in tema di salute, sicurezza e igiene sul lavoro;
 - attività di formazione in tema di salute, sicurezza e igiene sul lavoro;
 - rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
 - gestione degli asset aziendali con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro.
- 3) **Controllo e azioni correttive:** si tratta delle attività volte a implementare modalità di misura e monitoraggio delle prestazioni, la registrazione e il monitoraggio degli infortuni, incidenti, non conformità, azioni correttive e preventive, modalità di gestione delle registrazioni, modalità di esecuzione audit periodici.
- 4) **Riesame della direzione:** si tratta delle attività di riesame periodico del Vertice Aziendale al fine di valutare se il sistema di gestione della salute e sicurezza è stato completamente realizzato e

se è sufficiente alla realizzazione della politica e degli obiettivi dell'azienda.

Le aree a rischio reato così identificate hanno costituito il punto di riferimento nella definizione delle procedure di controllo da implementare ai fini dell'adeguamento dell'attuale sistema di controlli interno.

La Società ha articolato la propria organizzazione aziendale per la sicurezza e la salute sui luoghi di lavoro con le figure di seguito indicate:

- Datore di Lavoro;
- Delegati del Datore di Lavoro;
- Responsabile del Servizio di Prevenzione e Protezione;
- Servizio Prevenzione e Protezione;
- Medico Competente;
- Rappresentante dei Lavoratori per la Sicurezza;
- Incaricati Emergenze.

C.3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITA' A RISCHIO

La presente Parte Speciale si riferisce a comportamenti posti in essere da Amministratori, Dirigenti e Dipendenti ("Esponenti Aziendali") operanti nelle aree di attività a rischio nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i "Destinatari").

La presente Parte Speciale prevede l'esplicito divieto per gli Esponenti Aziendali, in via diretta, e per i Collaboratori esterni e Partner, tramite apposite clausole contrattuali, di:

- 1) porre in essere, collaborare o dare causa al verificarsi di comportamenti tali che, considerati individualmente o collettivamente, realizzino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-septies del d.lgs. 231/2001);
- 2) violare i principi e le procedure aziendali previste nella presente Parte Speciale.

C.4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

Il sistema dei controlli, adottato dalla Società prevede, con riferimento alle singole aree a rischio individuate, una serie di protocolli di controllo di seguito descritti.

- 1) Per la **pianificazione del sistema di gestione della salute e sicurezza del lavoratore** sono stabiliti i seguenti protocolli di controllo:
 - **Politica ed Obiettivi.** Esistenza di un documento formalizzato di Politica che definisca gli indirizzi e gli obiettivi generali in tema di salute e sicurezza che l'azienda stabilisce di raggiungere e che:
 - sia formalmente approvato dall'Alta Direzione aziendale;
 - contenga almeno l'impegno ad essere conforme con le vigenti leggi in materia di salute e sicurezza applicabili e con gli altri requisiti sottoscritti;
 - sia adeguatamente diffuso ai dipendenti ed alle parti interessate (individui o gruppi interessati, coinvolti o influenzati dalle prestazioni di salute e sicurezza sul lavoro di una organizzazione);
 - sia periodicamente riesaminato per assicurare che gli obiettivi in esso indicati siano idonei a mitigare i rischi presenti nell'organizzazione e appropriati (es. ai nuovi regolamenti e leggi).
 - **Piani Annuali e pluriennali.** Esistenza di un Piano degli Investimenti in materia di salute e sicurezza sul lavoro, approvato dagli organi societari delegati:
 - che contenga una chiara individuazione delle scadenze, responsabilità e disponibilità delle risorse necessarie per l'attuazione (finanziarie, umane, logistiche, di equipaggiamento);
 - che sia adeguatamente comunicato all'organizzazione in modo che il personale ne abbia una sufficiente comprensione.
 - **Prescrizioni legali ed altre.** Esistenza di una normativa aziendale che definisca criteri e modalità da adottarsi per:
 - l'aggiornamento riguardo la legislazione rilevante e le altre prescrizioni applicabili in tema di salute e sicurezza;

- l'individuazione di dove tali prescrizioni si applicano (area aziendale) e le modalità di diffusione delle stesse.
- 2) Per l' **attuazione e il funzionamento del sistema di gestione della salute e sicurezza del lavoratore** sono stabiliti i seguenti protocolli di controllo:
- **Norme e documentazione del sistema.** Esistenza di normative aziendali che disciplinino ruoli, responsabilità nella gestione della documentazione relativa al sistema di gestione della salute e sicurezza (es. Manuale, Procedure, Istruzioni di lavoro) in coerenza con la Politica e le linee guida aziendali. In particolare le suddette normative riportano anche le modalità di gestione ed archiviazione e conservazione della documentazione prodotta (es: modalità di archiviazione/protocollazione a garanzia di un adeguato livello di tracciabilità /verificabilità).
 - **Organizzazione e Responsabilità – Datore di Lavoro.** Esistenza di disposizioni organizzative per l'individuazione della figura datoriale che tengano conto della struttura organizzativa della Società e del settore di attività produttiva.
 - **Organizzazione e Responsabilità – RSPP/ASPP/Medico Competente/RLS/Incaricati Emergenze.** Esistenza di disposizioni organizzative relative alla designazione del Responsabile del Servizio di Prevenzione e Protezione (RSPP), degli Addetti del SPP, del Medico Competente, del Responsabile dei Lavoratori per la Sicurezza (RLS) e degli Incaricati delle Emergenze che:
 - definiscano i requisiti specifici coerentemente alle disposizioni di legge in materia;
 - prevedano la tracciabilità delle verifiche svolte in ordine al possesso dei requisiti specifici previsti dalla normativa in materia;
 - prevedano lo svolgimento dell'assessment sul personale per comprenderne le capacità e le disponibilità temporali al fine di ricoprire tali specifici ruoli;
 - prevedano la tracciabilità della formale accettazione dell'incarico.

- **Organizzazione e Responsabilità - sicurezza nei cantieri temporanei o mobili**¹⁸. Ove previsto dalla normativa vigente¹⁹, esistenza di norme aziendali che:
 - disciplinino le modalità di individuazione ed assegnazione dell'incarico di Coordinatore in materia di salute e sicurezza per la progettazione dell'opera e di Coordinatore in materia di sicurezza e di salute durante la realizzazione dell'opera, tenendo conto dei requisiti professionali previsti dalle norme di legge;
 - prevedano la tracciabilità dell'assessment dei requisiti e dell'accettazione dell'incarico da parte dei Coordinatori.

- **Sistema di deleghe di funzioni**. Esistenza di un sistema di deleghe di funzioni predisposte secondo i seguenti principi di elaborazione giurisprudenziale:
 - effettività - sussistenza e compresenza di autonomia decisionale e finanziaria del delegato²⁰;
 - idoneità tecnico professionale ed esperienza del delegato²¹;
 - vigilanza sull'attività del delegato, non acquiescenza, non ingerenza²²;
 - certezza, specificità e consapevolezza²³.

- **Individuazione e valutazione dei rischi – Ruoli e responsabilità**. Esistenza di una procedura aziendale che identifichi ruoli, responsabilità e modalità per lo svolgimento, approvazione ed aggiornamento della valutazione globale e

¹⁸ Qualunque luogo in cui si effettuano lavori edili o di ingegneria civile, il cui l'elenco è riportato nell'allegato X al d.lgs.81/2008.

¹⁹ Datore di Lavoro committente di un appalto come specificato all'art.89 lett.b) del d.lgs. 81/2008.

²⁰ Esistenza di un sistema formalizzato di deleghe in materia di salute e sicurezza e di una norma aziendale che garantisca la verifica della tracciabilità e della permanenza delle deleghe, che indichi chiaramente la possibilità o meno per il delegato di sub-delegare funzioni in materia di salute e sicurezza e preveda tracciabilità dei criteri in base ai quali viene determinata la coerenza tra funzioni delegate e poteri decisionali e di spesa assegnati.

²¹ Esistenza di una norma aziendale che definisca procedure di controllo circa la permanenza in capo al delegato dei requisiti tecnico-professionali, un piano periodico di aggiornamento e sviluppo tecnico professionale del delegato ed un sistema di valutazione periodico delle sue capacità tecnico-professionali.

²² Esistenza di un flusso informativo formalizzato continuo/periodico tra delegante e delegato e di un'attività di vigilanza formalizzata.

²³ Esistenza di un sistema formalizzato di deleghe in materia di salute e sicurezza in cui sia chiaramente identificato l'ambito di operatività e di norme aziendali che prevedano la tracciabilità dell'accettazione espressa della delega da parte dei delegati/subdelegati.

documentata di tutti i rischi presenti nell'ambito dell'azienda. In particolare tale norma:

- identifica ruoli, autorità, requisiti di competenza e necessità di addestramento del personale responsabile per condurre l'identificazione dei pericoli, l'identificazione del rischio ed il controllo del rischio;
 - identifica le responsabilità per la verifica, l'approvazione e l'aggiornamento dei contenuti del Documento di Valutazione dei Rischi (DVR);
 - identifica modalità e criteri per la revisione in tempi o periodi determinati dei processi di identificazione dei pericoli e valutazione del rischio;
 - prevede, laddove necessario, la tracciabilità dell'avvenuto coinvolgimento del Medico Competente nel processo di identificazione dei pericoli e valutazione dei rischi;
 - prevede la valutazione delle diverse tipologie di sorgenti di rischio: pericoli ordinari o generici, ergonomici, specifici, di processo e organizzativi e una individuazione di aree omogenee in termini di pericolo all'interno dell'azienda;
 - prevede l'individuazione delle mansioni rappresentative dei lavoratori;
 - prevede il censimento e la caratterizzazione degli agenti chimici e delle attrezzature e macchine presenti;
 - prevede esplicita definizione dei criteri di valutazione adottati per le diverse categorie di rischio nel rispetto della normativa e prescrizioni vigenti.
- **Presenza del Documento di Valutazione dei Rischi (DVR).** Esistenza del documento di relazione sulla Valutazione dei Rischi redatto secondo le disposizioni definite e che contenga almeno:
- il procedimento di valutazione, con la specifica dei criteri adottati;
 - l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione;
 - il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.
- **Controllo operativo – affidamento compiti e mansioni.** Esistenza di una norma aziendale che individui i criteri e le

modalità definite per l'affidamento delle mansioni ai lavoratori da parte del Datore di Lavoro. In particolare tale norma:

- definisce i criteri di affidamento delle mansioni ai lavoratori in base alle capacità e alle condizioni degli stessi in rapporto alla loro salute e alla sicurezza, e a quanto emerso dai risultati degli accertamenti sanitari eseguiti;
- definisce le misure organizzative per la partecipazione del Medico Competente e del RSPP nella definizione di ruoli e responsabilità dei lavoratori;
- prevede la tracciabilità delle attività di assessment svolte a tale scopo (es. definizione di check list mirate quali elenchi dei compiti critici e/o processi a impatto sulla salute e sicurezza).

- **Controllo operativo – Dispositivi di protezione individuale (DPI).** Esistenza di una norma aziendale per la gestione, distribuzione ed il mantenimento in efficienza dei Dispositivi di Protezione Individuali. In particolare tale norma:

- definisce modalità per la verifica dei necessari requisiti quali resistenza, idoneità e mantenimento in buon stato di conservazione ed efficienza dei DPI;
- prevede la tracciabilità delle attività di consegna e verifica della funzionalità dei DPI (es. check list mirate quali elenchi dei dispositivi di protezione individuale da consegnare, condivisi con il responsabile del Servizio di Prevenzione e Protezione).

- **Gestione delle emergenze.** Esistenza di una norma aziendale per la gestione delle emergenze atta a mitigare gli effetti sulla salute della popolazione e sull'ambiente esterno. In particolare tale norma prevede:

- l'individuazione delle misure per il controllo di situazioni di rischio in caso di emergenza;
- l'indicazioni sulle modalità di abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato;
- le modalità di intervento dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei lavoratori in caso di pericolo grave ed immediato e di pronto soccorso;
- l'individuazione dei provvedimenti per evitare rischi per la salute della popolazione o deterioramento dell'ambiente esterno;

- le indicazioni sulle modalità e sulla tempistica/frequenza di svolgimento delle prove di emergenza.
- **Gestione del rischio incendio.** Esistenza di una norma aziendale che definisca le misure necessarie per la prevenzione incendi. In particolare tale norma contiene:
 - il monitoraggio delle attività da svolgersi al fine della richiesta di rilascio e rinnovo del CPI;
 - indicazioni sulle modalità di informazione ai lavoratori sulle norme di comportamento da attuarsi in caso di incendio;
 - indicazioni sulle modalità di tenuta ed aggiornamento del registro incendio.
- **Consultazione e comunicazione.**
 - Esistenza di un calendario che preveda riunioni periodiche di tutte le figure competenti per la verifica della situazione nella gestione delle tematiche riguardanti salute e sicurezza e di una adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione.
 - Esistenza di una norma aziendale che disciplini la diffusione delle informazioni relative alla salute e sicurezza. In particolare tale norma disciplina:
 - l'informativa periodica del datore di lavoro verso i lavoratori;
 - l'informativa al Medico Competente, laddove necessario, relativamente ai processi e rischi connessi all'attività produttiva.
- **Formazione, sensibilizzazione e competenze.** Esistenza di una norma aziendale che regolamenti il processo di formazione. In particolare tale norma:
 - definisce modalità di erogazione della formazione di ciascun lavoratore su: rischi dell'impresa, misure di prevenzione e protezione, rischi specifici e norme di sicurezza, caratteristiche delle sostanze pericolose (schede di sicurezza e norme di buona pratica operativa), procedure di emergenza, nominativi e ruoli del RSPP e del medico competente, laddove applicabile istruzioni d'uso delle attrezzature di lavoro e dei dispositivi di protezione individuale;
 - definisce i criteri di erogazione della formazione di ciascun lavoratore (es. all'assunzione, trasferimento o cambiamento di

mansioni, introduzione di nuove attrezzature, tecnologie, sostanze pericolose);

- con riferimento ai soggetti coinvolti nella gestione delle tematiche della salute e della sicurezza definisce l'identificazione dell'ambito, i contenuti e le modalità della formazione in dipendenza del ruolo assunto all'interno della struttura organizzativa (Rappresentanti dei Lavoratori per la Sicurezza, Addetti al Servizio di Prevenzione e Protezione, Squadre di Emergenze e Pronto Soccorso);
 - definisce i tempi di erogazione della formazione ai lavoratori sulla base delle modalità e dei criteri definiti (definizione di un Piano di Formazione su base annuale).
- **Rapporti con fornitori e contrattisti – informazione e coordinamento.** Esistenza di una norma aziendale che definisca:
- modalità e contenuti dell'informazione che deve essere fornita alle imprese esterne riguardo l'insieme delle norme e prescrizioni che un'impresa appaltatrice aggiudicataria di un ordine deve conoscere ed impegnarsi a rispettare ed a far rispettare ai propri dipendenti;
 - ruoli, responsabilità e modalità di elaborazione del Documento di Valutazione dei Rischi che indichi le misure da adottare per eliminare i rischi dovuti alle interferenze tra i lavoratori nel caso di diverse imprese coinvolte nell'esecuzione di un'opera.
- **Rapporti con fornitori e contrattisti – qualifica.** Esistenza di una norma aziendale che definisca modalità di qualifica dei fornitori. In particolare tale norma tiene conto:
- dei risultati della verifica dei requisiti tecnico-professionali degli appaltatori prevista ai sensi dell'art.90, comma 9, del d.lgs.81/08;
 - della rispondenza di quanto eventualmente fornito con le specifiche di acquisto e le migliori tecnologie disponibili in tema di tutela della salute e della sicurezza.
- **Rapporti con fornitori e contrattisti – clausole contrattuali.** Esistenza di clausole contrattuali standard riguardanti i costi della sicurezza nei contratti di somministrazione, di appalto e di subappalto.
- **Gestione degli asset.** Esistenza di norme aziendali che individuino le attività di manutenzione/ispezione degli asset

aziendali affinché ne sia sempre garantita l'integrità ed adeguatezza. In particolare tali norme prevedono:

- periodiche verifiche di adeguatezza e integrità degli asset e di conformità ai requisiti normativi applicabili;
- la pianificazione, effettuazione e verifica delle attività di ispezione e manutenzione tramite personale qualificato e idoneo.

3) Per il controllo e le azioni correttive sono stabiliti i seguenti protocolli di controllo:

- **Misura e monitoraggio delle prestazioni – infortuni.** Esistenza di una norma aziendale che indichi:
 - ruoli, responsabilità e modalità di rilevazione, registrazione, investigazione interna degli infortuni;
 - ruoli, responsabilità e modalità di tracciabilità ed investigazione degli incidenti occorsi²⁴ e dei "mancati incidenti"²⁵;
 - modalità di comunicazione degli infortuni/incidenti occorsi dai responsabili operativi al datore di lavoro e al responsabile del servizio di prevenzione e protezione.

- **Misura e monitoraggio delle prestazioni – altri dati (diversi da infortuni e incidenti).** Esistenza di norme aziendali che definiscano ruoli, responsabilità e modalità di registrazione e monitoraggio (anche attraverso l'uso di indicatori) per:
 - i dati riguardanti la sorveglianza sanitaria;
 - i dati riguardanti la sicurezza degli impianti (apparecchi di sollevamento e ascensori, impianti elettrici, attrezzature a pressione, serbatoi interrati, apparecchiature laser, macchine);
 - i dati riguardanti le sostanze ed i preparati pericolosi utilizzati in azienda (schede di sicurezza).

- **Misura e monitoraggio delle prestazioni – cause/controversie.** Esistenza di norme aziendali che definiscano ruoli, responsabilità e modalità di monitoraggio delle controversie/contenzioso pendenti relativi agli infortuni occorsi

²⁴ Eventi che hanno provocato un danno (se il danno prodotto riguarda l'integrità fisica di una persona si parla di infortunio)

²⁵ Incidenti che pur caratterizzati da un elevato potenziale di rischio, non hanno provocato nessun danno, o soltanto un danno marginale.

sui luoghi di lavoro al fine di identificare le aree a maggior rischio infortuni.

- **Audit.** Esistenza di una norma aziendale che disciplini ruoli, responsabilità e modalità operative riguardo le attività di audit e verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza. In particolare tale norma definisce:
 - la tempistica per la programmazione delle attività (Piano di Audit formalizzato);
 - le competenze necessarie per il personale coinvolto nelle attività di audit nel rispetto del principio dell'indipendenza dell'auditor rispetto all'attività che deve essere auditata;
 - le modalità di registrazione degli audit;
 - le modalità di individuazione e l'applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di gestione della salute e sicurezza in azienda o dalla normativa e prescrizioni applicabili;
 - le modalità di verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;
 - le modalità di comunicazione dei risultati dell'audit all'Alta Direzione aziendale.

 - **Reporting.** Esistenza di una norma aziendale che disciplini ruoli, responsabilità e modalità operative delle attività di reporting verso l'Organismo di Vigilanza e l'Alta Direzione.
- 4) Per il **riesame della direzione** sono stabiliti i seguenti protocolli di controllo:
- **Conduzione del processo di riesame.** Esistenza di una norma aziendale che definisca ruoli, responsabilità e modalità di conduzione del processo di riesame effettuato dall'Alta Direzione aziendale in relazione all'efficacia e all'efficienza del sistema di gestione della salute e sicurezza in azienda. Tale norma prevede la tracciabilità dello svolgimento delle seguenti attività:
 - l'analisi degli eventuali scostamenti tra i risultati ottenuti e gli obiettivi programmati;
 - l'analisi dei risultati degli Audit;
 - l'analisi dei risultati del monitoraggio della performance del sistema di gestione della salute e sicurezza (infortuni, altri dati);

- lo stato di avanzamento di eventuali azioni di miglioramento definite nel precedente Riesame;
- l'individuazione degli obiettivi di miglioramento per il periodo successivo e la necessità di eventuali modifiche ad elementi del sistema di gestione della salute e sicurezza in azienda.

C.5. COMPITI DELL'ODV

Il compiti dell'OdV sono i seguenti:

- 1) monitoraggio delle procedure interne per la prevenzione dei reati in materia di salute e sicurezza.

Tale compito sarà svolto anche tenendo conto dei seguenti flussi informativi:

- comunicazioni a cura del RSPP di ogni modifica e/o aggiornamento del Documento di Valutazione dei Rischi;
 - verbali relativi alle riunioni periodiche di prevenzione e protezione dai rischi (art.35 d.lgs. n.81/2008), a cura del RSPP;
 - ogni aggiornamento legato a modifiche delle responsabilità ad oggi conferite ai sensi del d.lgs.81/2008, comunicate dalla funzione Risorse Umane, Organizzazione e Information Technology;
 - eventuali segnalazioni, provenienti dagli organi di controllo o da qualsiasi dipendente, concernenti sia carenze o inadeguatezze dei luoghi e delle attrezzature di lavoro, ovvero dei Dispositivi di Protezione Individuale messi a disposizione dalla società, sia ogni altra situazione di pericolo connesso alla salute e sicurezza sul lavoro.
- 2) verificare periodicamente, con il supporto delle altre funzioni competenti, l'esistenza di clausole contrattuali standard riguardanti i costi della sicurezza nei contratti di somministrazione, di appalto e di subappalto;
 - 3) audizione del RSPP, con cadenza semestrale, sulle attività di competenza e sugli aspetti legati, in generale, alla pianificazione delle norme antinfortunistiche e sulla tutela dell'igiene e della sicurezza sul lavoro.

PARTE SPECIALE "D"

**Ricettazione, riciclaggio, impiego di denaro, beni o utilità di
provenienza illecita**

D.1. LA TIPOLOGIA DEI REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 25 –OCTIES DEL DECRETO)

L'art. 63, terzo comma, del d.lgs. 21 novembre 2007, n. 231 ha introdotto, nel novero dei reati presupposto della responsabilità amministrativa ex d.lgs. 231 del 2001, l'art. 25-octies prevedendo sanzioni pecuniarie e interdittive a carico dell'ente con riferimento ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (reati di cui agli artt. 648, 648-bis e 648-ter del codice penale).

L'art. 64, co. 1, lett. f), della medesima norma ha inoltre abrogato i commi 5 e 6 dell'art. 10 della l. n. 146/2006, di contrasto al crimine organizzato transnazionale che già prevedevano, a carico dell'ente, la responsabilità e le sanzioni ex d.lgs. 231 del 2001 per i reati di riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (artt. 648-bis e 648-ter c.p.), se caratterizzati dagli elementi della transnazionalità, secondo la definizione contenuta nell'art. 3 della stessa legge 146/2006.

Ne consegue che, ai sensi dell'art. 25-octies del d.lgs. 231 del 2001, l'ente è ora punibile per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un interesse o vantaggio per l'ente medesimo. Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-octies del Decreto.

i. Ricettazione (art. 648 c.p.)

L'art. 648 c.p. incrimina chi "fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare".

Per acquisto dovrebbe intendersi l'effetto di un attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente consegue il possesso del bene.

Il termine ricevere starebbe ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.

Per occultamento dovrebbe intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto.

La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione, da non intendersi in senso civilistico (come precisato dalla giurisprudenza), tra l'autore del reato principale e il terzo acquirente.

L'ultimo comma dell'art. 648 c.p. estende la punibilità "anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto".

Lo scopo dell'incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell'evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.

ii. Riciclaggio (art. 648-bis c.p.)

Tale reato consiste nel fatto di chiunque "fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa". Il delitto in esame sussiste anche quando l'autore del delitto da cui il denaro o le cose provengono, sia non imputabile o non punibile, o quando manchi una condizione di procedibilità riferita a tale delitto. È necessario che antecedentemente ad esso sia stato commesso un delitto non colposo al quale, però, il riciclatore non abbia partecipato a titolo di concorso.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale ed è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

La disposizione è applicabile anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto. È rilevante il fatto di chi ponga ostacoli alla identificazione dei beni suddetti dopo che essi sono stati sostituiti o trasferiti.

iii. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

È il reato commesso da "chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 c.p. (Ricettazione) e 648-bis c.p. (Riciclaggio), impiega in attività economiche o finanziarie denaro o beni o altre utilità provenienti da delitto".

Anche in questa fattispecie, è prevista la circostanza aggravante dell'esercizio di un'attività professionale ed è esteso ai soggetti l'ultimo comma dell'art. 648, ma la pena è diminuita se il fatto è di particolare tenuità.

Il riferimento specifico al termine "impiegare", di accezione più ampia rispetto a "investire" che suppone un impiego finalizzato a particolari obiettivi, esprime il significato di "usare comunque". Il richiamo al concetto di "attività" per indicare il settore di investimento (economia o finanza) consente viceversa di escludere gli impieghi di denaro od altre utilità che abbiano carattere occasionale o sporadico.

La specificità del reato rispetto a quello di riciclaggio risiede nella finalità di far perdere le tracce della provenienza illecita di denaro, beni o altre utilità, perseguita mediante l'impiego di dette risorse in attività economiche o finanziarie.

Il legislatore ha inteso punire quelle attività mediate che, a differenza del riciclaggio, non sostituiscono immediatamente i beni provenienti da delitto, ma che comunque contribuiscono alla "ripulitura" dei capitali illeciti.

D.2. PRINCIPALI AREE DI ATTIVITA' A RISCHIO DI COMMISSIONE DEI REATI

Le analisi svolte hanno permesso di individuare, in relazione al rischio di commissione dei reati di cui all'art. 25-octies del Decreto, come area a rischio l'Amministrazione, Finanza e Controllo con riferimento alla "Gestione delle transazioni finanziarie".

D.3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del Modello che, a qualunque titolo, siano coinvolti nell'aree a rischio, rispetto ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

In via generale, a tali soggetti è richiesto:

- 1) di garantire che ogni operazione o transazione sia correttamente e tempestivamente registrata nel sistema di contabilità aziendale secondo i criteri indicati dalla legge e sulla base dei principi contabili applicabili; ogni operazione o transazione deve essere autorizzata, verificabile, legittima, coerente e congrua;

- 2) di effettuare pagamenti nell'interesse della Società solo in presenza di adeguata documentazione di supporto.

E' fatto divieto di ricevere o accettare la promessa di pagamenti in contanti, in alcun modo e in alcuna circostanza, o correre il rischio di essere implicati in vicende relative al riciclaggio di denaro proveniente da attività illecite o criminali.

D.4. PRINCIPI DI ATTUAZIONE DEI COMPORAMENTI DESCRITTI

Il sistema dei controlli, adottato dalla Società prevede, per l'area a rischio Amministrazione, Finanza e Controllo con riferimento alla "Gestione delle transazioni finanziarie", una serie di protocolli di controllo di seguito descritti:

- 1) **Regolamentazione:** il processo in oggetto deve essere regolamentato da apposita documentazione organizzativa interna che disciplini la gestione dei flussi finanziari. Nell'ambito di tale processo devono essere definiti ruoli e responsabilità dei soggetti incaricati a gestire le diverse fasi, nonché i protocolli di prevenzione che da questi devono essere applicati. In particolare, il processo deve essere descritto distinguendo i flussi finanziari in entrata e quelli in uscita. Inoltre, devono essere previsti i seguenti protocolli di prevenzione:
- i controlli eseguiti in sede di apertura/modifica di anagrafica fornitori/clienti a sistema finalizzati ad assicurare che vi sia sempre piena corrispondenza tra il nome del fornitore/cliente e l'intestazione del conto su cui far pervenire/da cui accettare il pagamento;
 - possono essere disposti/accettati solo pagamenti/incassi nei confronti/da parte di soggetti presenti in anagrafica;
 - non è consentito effettuare/ricevere pagamenti su conti cifrati;
 - non è consentito utilizzare contante o altro strumento finanziario al portatore, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché utilizzare conto correnti o libretti di risparmio in forma anonima o con intestazione fittizia;
 - non possono essere utilizzati Istituti di credito privi di insediamenti fisici (Istituti virtuali);
 - devono essere rispettate le soglie ed i limiti definiti per i pagamenti.

- 2) **Tracciabilità:** il processo deve prevedere che tutte le fasi di gestione dei flussi finanziari siano documentate e tracciabili.
- 3) **Separazione dei compiti:** il processo deve essere condotto in accordo con il principio di separazione dei compiti fra le funzioni coinvolte nelle attività autorizzative, esecutive e di controllo.
- 4) **Procure e deleghe:** il processo deve prevedere che le attività debbano essere svolte nel rispetto di quanto previsto dallo Statuto della Società, dal sistema interno di procure per l'attribuzione dei poteri di rappresentanza e firma sociale e dal sistema interno di deleghe allo svolgimento delle attività di competenza.

D.5. COMPITI DELL'ODV

E' compito dell'OdV:

- 1) verificare periodicamente, con il supporto delle altre funzioni competenti:
 - il sistema delle procure in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di firma conferiti;
 - le soglie di importo previste per i pagamenti;
- 2) il monitoraggio dell'efficacia delle procedure interne per la prevenzione dei reati di ricettazione, riciclaggio e impiego di beni, denaro o utilità di provenienza illecita, in particolare per quanto attiene alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni, alla sede legale della società controparte (ad es. paradisi fiscali), agli Istituti di credito utilizzati (es. sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese).

Tali compiti saranno svolti anche tenendo conto delle eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente.

PARTE SPECIALE "E"

Delitti informatici e trattamento illecito dei dati

E.1. LA TIPOLOGIA DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (ART. 24-BIS DEL DECRETO)

La legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero" ha ampliato ulteriormente le fattispecie di reato che possono generare la responsabilità della società. L'art. 7 del predetto provvedimento ha introdotto nel d.lgs.231/2001 l'art. 24-bis "Delitti informatici e trattamento illecito di dati".

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 24-bis del Decreto.

i. Documenti informatici (art. 491 -bis c.p.)

"Se alcune delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applica le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private".

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- **Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)**
Commette tale reato il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero.
- **Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)**
Commette tale reato il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempite le condizioni richieste per la loro validità.
- **Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)**

Commette tale reato il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale.

- **Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)**

Commette tale reato il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità.

- **Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)**

Commette tale reato il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità.

- **Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)**

Commette tale reato chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità.

- **Falsità materiale commessa da privato (art. 482 c.p.)**

Commette tale reato il privato che realizza la condotta prevista dagli articoli 476, 477 e 478.

- **Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.)**

Commette tale reato chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità.

- **Falsità in registri e notificazioni (art. 484 c.p.)**

Commette tale reato chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie

operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni.

- **Falsità in scrittura privata (art. 485 c.p.)**

Commette tale reato chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera.

Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

- **Falsità in foglio firmato in bianco. Atto privato (art. 486 c.p.)**

Commette tale reato chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato.

Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.

- **Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.)**

Commette tale reato il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato.

- **Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)**

Tale fattispecie si applica ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti.

- **Uso di atto falso (art. 489 c.p.)**

Commette tale reato chiunque senza essere concorso nella falsità, fa uso di un atto falso.

Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno".

- **Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)**

Commette tale reato chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri.
 - **Copie autentiche che tengono luogo degli originali mancanti (art. 492 c.p.)**

Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti".
 - **Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)**

L'art. 493 c.p. prevede che le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.
- ii. Accesso abusivo a un sistema informatico o telematico (art. 615 -ter codice penale)**
- L'art. 615-ter punisce chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
- Il legislatore prevede sanzioni più elevate se:
- il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
 - il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
 - dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
- E', inoltre, previsto un aggravamento della sanzione qualora i fatti sopra descritti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

iii. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 -quater codice penale)

L'art. 615-quater sanziona chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Sanzioni più gravi sono previste se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema.

iv. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 -quinqies codice penale)

L'art. 615-quinqies considera il fenomeno della diffusione dei c.d. virus.

La norma punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

v. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 -quater del codice penale)

L'art. 617-quater (così come il successivo art. 617-quinqies) è una norma volta a tutelare la sicurezza e la genuinità delle comunicazioni informatiche e telematiche.

La fattispecie punisce:

- chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

- chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni informatiche o telematiche intercettate.

Sanzioni più elevate sono previste se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi esercita anche abusivamente la professione di investigatore privato.

vi. Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 -quinqies del codice penale)

L'art. 617-quinqies punisce l'installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Sanzioni più elevate sono previste se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi esercita anche abusivamente la professione di investigatore privato.

vii. Danneggiamento di informazioni, dati e programmi informatici (art. 635 -bis del codice penale)

La fattispecie si realizza quando chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Sanzioni più gravi sono previste se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

viii. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635 -ter del codice penale)

La fattispecie si realizza quando chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Sanzioni più elevate sono previste se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

È, inoltre, previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

ix. Danneggiamento di sistemi informatici e telematici (art. 635 -quater del codice penale)

L'art. 635-quater punisce chiunque, mediante le condotte di cui al sopra citato articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

È previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

x. Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 -quinqües del codice penale)

La norma prevede sanzioni nel caso in cui il fatto previsto dal precedente articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Sanzioni più gravi sono previste se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

È, inoltre, previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

xi. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 -quinqües del codice penale)

L'art. 640-quinquies punisce la condotta posta in essere dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

E.2. PRINCIPALI AREE DI ATTIVITA' A RISCHIO DI COMMISSIONE DEI REATI

Le analisi svolte hanno permesso di individuare, in relazione al rischio di commissione dei delitti informatici e trattamento illecito dei dati di cui all'art.24-bis del Decreto, come aree a rischio:

- Risorse Umane, Organizzazione e Information Technology (che include il Security Officer);
- Linee di Ingegneria;
- Operazioni.

con riferimento alle seguenti singole attività:

- 1) Gestione dei profili utente e del processo di autenticazione.
- 2) Gestione e protezione della postazione di lavoro.
- 3) Gestione degli accessi da e verso l'esterno.
- 4) Gestione e protezione delle reti.
- 5) Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD).
- 6) Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.).
- 7) Produzione e/o vendita di apparecchiature, dispositivi o programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti: acquisizione, sviluppo e manutenzione di apparecchiature, dispositivi o programmi informatici destinanti al mercato ed erogazione di servizi, per i clienti, inerenti la gestione degli stessi.

E.3. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del Modello che, a qualunque titolo, siano coinvolti

nell'aree a rischio, rispetto ai delitti informatici e trattamento illecito dei beni. In via generale, a tali soggetti è vietato:

- 1) porre in essere, collaborare o dare causa al verificarsi di comportamenti tali che, considerati individualmente o collettivamente, realizzino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del d.lgs. 231/2001);
- 2) violare i principi e le procedure aziendali previste nella presente Parte Speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;
- 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;
- 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;
- 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;
- 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;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- 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;
- 3) segnalare alle funzioni competenti il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla funzione competente l'originale della denuncia all'Autorità di Pubblica Sicurezza;
- 4) evitare di introdurre e/o conservare in Società (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;
- 5) evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società 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 Personal Computer (PC);
- 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;
- 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 della Società solo prodotti ufficialmente acquisiti dalla Società 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 della Società;
- 15) osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

E.4. PRINCIPI DI ATTUAZIONE DEI COMPORTAMENTI DESCRITTI

Il sistema dei controlli adottato dalla Società prevede, con riferimento alle aree a rischio individuate, una serie di protocolli di controllo di seguito descritti:

- 1) **Politiche di sicurezza.** Deve essere formalizzata una politica in materia di sicurezza del sistema informativo che preveda, fra l'altro:
 - le modalità di comunicazione anche a terzi;
 - le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi.
- 2) **Organizzazione della sicurezza per gli utenti interni.** Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.
- 3) **Organizzazione della sicurezza per gli utenti esterni.** Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di

prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

- 4) **Classificazione e controllo dei beni.** Deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità per l'identificazione e la classificazione degli assets aziendali (ivi inclusi dati e informazioni).

- 5) **Sicurezza fisica e ambientale.** Deve essere adottato e attuato uno strumento normativo che disponga l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature.

- 6) **Gestione delle comunicazioni e dell'operatività.** Deve essere adottato e attuato uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. In particolare, tale strumento normativo deve assicurare:
 - il corretto e sicuro funzionamento degli elaboratori di informazioni;
 - la protezione da software pericoloso;
 - il backup di informazioni e software;
 - la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
 - gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
 - una gestione organica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
 - il controllo sui cambiamenti agli elaboratori e ai sistemi;
 - la gestione di dispositivi rimovibili.

- 7) **Controllo degli accessi.** Deve essere adottato e attuato uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo deve prevedere:
 - l'autenticazione degli utenti tramite codice identificativo e password o altro sistema di autenticazione sicura;

- le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
 - una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
 - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
 - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
 - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
 - la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
 - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
 - la custodia dei dispositivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati.
- 8) **Gestione degli incidenti e dei problemi di sicurezza informatica:** Deve essere adottato e attuato uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo deve prevedere:
- appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;
 - l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;
 - la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
 - l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;
 - appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
 - l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;

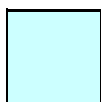
- l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
 - la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
 - la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.
- 9) **Audit.** Deve essere adottato e attuato uno strumento normativo che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.
- 10) **Risorse umane e sicurezza.** Deve essere adottato e attuato uno strumento normativo che preveda:
- la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
 - specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
 - l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
 - la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.
- 11) **Crittografia.** Deve essere adottato e attuato uno strumento normativo che preveda l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche.
- 12) **Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi.** Deve essere adottato e attuato uno strumento normativo che definisca:

- l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- la confidenzialità, autenticità e integrità delle informazioni;

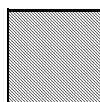
Di seguito si riporta una tabella riepilogativa dei protocolli di controllo suddetti applicabili alle singole aree a rischio.

PROTOCOLLI DI CONTROLLO	AREE A RISCHIO						
	1. Gestione dei profili utente e del processo di autenticazione	2. Gestione e protezione della postazione di lavoro	3. Gestione degli accessi da e verso l'esterno	4. Gestione e protezione delle reti	5. Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD)	6. Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.)	7. Produzione e/o vendita di apparecchiature, dispositivi o programmi informatici e di servizi di installazione e manutenzione di hardware, software, reti.
Politiche di sicurezza							
Organizzazione della sicurezza per gli utenti interni							
Organizzazione della sicurezza per gli utenti esterni							
Classificazione e controllo dei beni							
Sicurezza fisica ed ambientale							
Gestione delle comunicazioni e dell'operatività							
Controllo degli accessi							
Gestione degli incidenti e dei problemi di sicurezza informatica							
Audit							
Risorse umane e sicurezza							
Crittografia							
Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi							

Leggenda:



Applicabile



Non applicabile

E.5. COMPITI DELL'ODV

E' compito dell'OdV monitorare l'efficacia delle procedure interne per la prevenzione dei delitti informatici e trattamento illecito dei dati;

Tale compito sarà svolto anche tenendo conto dei seguenti flussi informativi:

- 1) ogni aggiornamento legato a modifiche delle responsabilità e dei ruoli a oggi conferiti in materia di sicurezza informatica, comunicate dalla funzione Risorse Umane, Organizzazione e Information Technology;
- 2) eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente.