MODELLO DI ORGANIZZAZIONE E GESTIONE *EX* D.LGS. 231/01

DI

SIIT S.C.P.A.

PARTE GENERALE

Adottato dal Consiglio di Gestione in data 19/04/2023

INDICE

1. Il Decreto Legislativo 8 giugno 2001, n. 231, in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica 4
1.1 La Responsabilità Amministrativa delle Persone Giuridiche 4
1.2 Le Persone soggette al D.Lgs. n. 231 del 2001 4
1.3 I Reati Presupposto 5
1.4 Le Sanzioni previste nel Decreto 7
1.5 Delitti tentati 11
1.5.1 Le Condotte Esimenti 11
1.6 Le Linee Guida 12
2. Il presente Modello 14
2.1 SIIT S.c.p.A.: profilo e storia aziendale. 14
2.2 Il presente Modello 14
2.2.1 Le finalità del Modello 14
2.2.2 La costruzione del Modello 15
2.2.3 Il concetto di rischio accettabile 15
2.2.4 La struttura del Modello ed i Reati Presupposto rilevanti ai fini della sua costruzione 16
2.2.5 L'adozione del Modello 17
2.3 I documenti connessi al Modello 17
2.4 Gestione delle risorse finanziarie 17
2.5 Diffusione del Modello 18
2.5.1 Destinatari 18
2.5.2 Formazione ed Informazione del Personale 18
2.5.3 Informazione ai Terzi e diffusione del Modello 19
3. Elementi del modello di *governance* e dell'assetto organizzativo generale di SIIT S.c.p.A. 19
3.1 Il Modello di *governance* della Società 19
3.2 Il sistema di controllo interno di SIIT S.c.p.A. 20
3.3 Principi generali di controllo in tutte le Aree a Rischio Reato 20
4. L'Organismo di Vigilanza 21
4.1 Caratteristiche dell'Organismo di Vigilanza 21
4.1.1 Autonomia ed indipendenza 21
4.1.2 Professionalità 22
4.1.3 Continuità d'azione 22
4.2 Individuazione dell'Organismo di Vigilanza 22
4.3 Durata dell'incarico e cause di cessazione 23
4.4 Casi di ineleggibilità e di decadenza 23
4.5 Funzioni, compiti e poteri dell'Organismo di Vigilanza 24
4.6 Risorse dell'Organismo di Vigilanza 25
4.7 Flussi informativi dell'Organismo di Vigilanza 25
4.7.1 Obblighi di informazione nei confronti dell'Organismo di Vigilanza 25
4.7.2 Segnalazioni nei confronti dell'Organismo di Vigilanza ai sensi dell'art. 6 comma 2 bis lettera a) del D.Lgs. 231/01 26
4.7.3 Gestione dei flussi e delle segnalazioni 26
4.7.4 Obblighi di informazione propri dell'Organismo di Vigilanza 27
5. Sistema Sanzionatorio per mancata osservanza del presente Modello e delle norme-disposizioni ivi richiamate 28
5.1 Principi generali 28
5.2 Definizione di "Violazione" ai fini dell'operatività del presente Sistema Sanzionatorio 29
5.3 Sistema disciplinare 29
5.3.1 Personale dipendente in posizione non dirigenziale 29
5.3.2 Dirigenti 30
5.3.3 Consiglieri 30

5.3.4 Revisori 30
5.3.5 Terzi: collaboratori e consulenti esterni 31

1. Il Decreto Legislativo 8 giugno 2001, n. 231, in materia di responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica

1.1 La Responsabilità Amministrativa delle Persone Giuridiche

Il Decreto Legislativo 8 giugno 2001, n. 231, in attuazione della Legge Delega 29 settembre 2000, n. 300, ha introdotto in Italia la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (di seguito, per brevità, anche "**D.Lgs. n. 231 del 2001**" o il "**Decreto**"), che si inserisce in un ampio processo legislativo di lotta alla corruzione ed adegua la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune Convenzioni Internazionali precedentemente sottoscritte dall'Italia.

Il D.Lgs. n. 231 del 2001 stabilisce, pertanto, un regime di responsabilità amministrativa (equiparabile sostanzialmente alla responsabilità penale), a carico delle persone giuridiche[1] (di seguito, per brevità, il/gli "**Ente/Enti**"), che va ad aggiungersi alla responsabilità della persona fisica (meglio individuata di seguito) autrice materiale del reato e che mira a coinvolgere, nella punizione dello stesso, gli Enti nel cui interesse o vantaggio tale reato è stato compiuto. Tale responsabilità amministrativa sussiste unicamente per i reati tassativamente elencati nel medesimo D.Lgs. n. 231 del 2001.

L'articolo 4 del Decreto precisa, inoltre, che in alcuni casi ed alle condizioni previste dagli articoli 7, 8, 9 e 10 del Codice Penale, sussiste la responsabilità amministrativa degli Enti che hanno sede principale nel territorio dello Stato per i reati commessi all'estero dalle persone fisiche (come di seguito meglio individuate) a condizione che nei confronti di tali Enti non proceda lo Stato del luogo in cui è stato commesso il fatto criminoso.

1.2 Le Persone soggette al D.Lgs. n. 231 del 2001

I soggetti che, commettendo un reato nell'interesse o a vantaggio dell'Ente, ne possono determinare la responsabilità sono di seguito elencati:

(i) persone fisiche che rivestono posizioni di vertice (rappresentanza, amministrazione o direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale o persone che esercitano, di fatto, la gestione

[1] L'art.1 del D.Lgs. n. 231 del 2001 ha delimitato l'ambito dei soggetti destinatari della normativa agli *"enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica"*. Alla luce di ciò, la normativa si applica nei confronti degli:

- enti a soggettività privata, ovvero agli enti dotati di personalità giuridica ed associazioni "anche prive" di personalità giuridica;
- enti a soggettività pubblica, ovvero gli enti dotati di soggettività pubblica, ma privi di poteri pubblici (c.d. "enti pubblici economici");
- enti a soggettività mista pubblica/privata (c.d. "società miste").

Sono invece esclusi dal novero dei soggetti destinatari: lo Stato, gli enti pubblici territoriali (Regioni, Province, Comuni e Comunità montane), gli enti pubblici non economici e, in generale, tutti gli enti che svolgano funzioni di rilievo costituzionale (Camera dei deputati, Senato della Repubblica, Corte costituzionale, Segretariato generale della Presidenza della Repubblica, C.S.M., etc.).

ed il controllo: di seguito, per brevità, i "**Soggetti Apicali**");

(ii) persone fisiche sottoposte alla direzione o vigilanza da parte di uno dei Soggetti Apicali (di seguito, per brevità, i "**Soggetti Sottoposti**").

A questo proposito, giova rilevare che non è necessario che i Soggetti Sottoposti abbiano con l'Ente un rapporto di lavoro subordinato, dovendosi ricomprendere in tale nozione anche "*quei prestatori di lavoro che, pur non essendo <dipendenti> dell'ente, abbiano con esso un rapporto tale da far ritenere sussistere un obbligo di vigilanza da parte dei vertici dell'ente medesimo: si pensi, ad esempio, agli agenti, ai partners in operazioni di joint-venture, ai c.d. parasubordinati in genere, ai distributori, fornitori, consulenti, collaboratori*"[2].

Infatti, secondo l'indirizzo dottrinale prevalente, assumono rilevanza ai fini della responsabilità amministrativa dell'ente quelle situazioni in cui un incarico particolare sia affidato a collaboratori esterni, tenuti ad eseguirlo sotto la direzione o il controllo di Soggetti Apicali.

È comunque opportuno ribadire che l'Ente non risponde, per espressa previsione legislativa (articolo 5, comma 2, del Decreto), se i predetti soggetti hanno agito nell'interesse esclusivo proprio o di terzi. In ogni caso, il loro comportamento deve essere riferibile a quel rapporto "organico" per il quale gli atti della persona fisica possono essere imputati all'Ente.

1.3 I Reati Presupposto

Il Decreto richiama le seguenti fattispecie di reato (di seguito, per brevità, anche, i "**Reati Presupposto**"):

(i) reati contro la Pubblica Amministrazione e/o in danno dell'Unione europea, di cui agli articoli 24 e 25 del D.Lgs. n. 231 del 2001), introdotti dal Decreto e successivamente modificati dalla L. 190 del 6 novembre 2012 – come modificata dalla Legge 69 del 2015 -, dalla L. 3 del 9 gennaio 2019[3], nonché dal D. Lgs. 14 luglio 2020, n. 75[4]; nello specifico trattasi dei delitti di indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24 del Decreto), nonché delitti di peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25 del Decreto);

(ii) delitti informatici e trattamento illecito dei dati, introdotti dall'articolo 7 della Legge 18 marzo 2008, n. 48, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo

[2] Così testualmente: Circolare Assonime, in data 19 novembre 2002, n. 68.

[3] Legge 69/2015 *"Disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio"* pubblicata su Gazzetta Ufficiale n. 124 del 30/05/2015.
Legge 9 gennaio 2019, n. 3 recante "*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici"* pubblicata su Gazzetta Ufficiale n. 13 del 16/01/2019.

[4] D. Lgs. 75/2020 "*Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*".

24-*bis*, ed ulteriormente ampliati, da ultimo, con il D.L. n. 105 del 2019;

(iii) delitti di criminalità organizzata, introdotti dall'articolo 2, comma 29, della Legge 15 luglio 2009, n. 94[5] che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 24-*ter*;

(iv) peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (Art. 25, D.Lgs. n. 231/2001), modificato dalla L. n. 190/2012, dalla L. 3/2019 e dal D.Lgs. n. 75/2020;

(v) delitti in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, introdotti dall'articolo 6 della Legge 23 novembre 2001, n. 409, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*bis*, successivamente integrato dall'articolo 17, comma 7, lett. a), della Legge 23 luglio 2009, n. 99;

(vi) delitti contro l'industria e il commercio, introdotti dall'articolo 17, comma 7, lett. b), della Legge 23 luglio 2009, n. 99, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*bis* 1;

(vii) reati societari, introdotti dal Decreto Legislativo 11 aprile 2002, n. 61, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*ter*, successivamente modificato e integrato dalla Legge n. 262 del 28 dicembre 2005, dalla Legge n. 190 del 6 novembre 2012, dalla Legge 69 del 2015[6], nonché dal D.Lgs. 38 del 15 marzo 2017;

(viii) delitti con finalità di terrorismo o di eversione dell'ordine democratico, introdotti dalla Legge 14 gennaio 2003, n. 7, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*quater*;

(ix) pratiche di mutilazione degli organi genitali femminili, introdotti dalla Legge 9 gennaio 2006, n. 7, che ha inserito nel D.Lgs. n. 231 del 2001 l'art. 25-*quater*.1;

(x) delitti contro la personalità individuale, introdotti dalla Legge 11 agosto 2003, n. 228, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*quinquies*, successivamente modificato e integrato dalla Legge 38 del 6 febbraio 2006, dal D.Lgs. 39 del 4 marzo 2014, nonché dalla Legge 199 del 29 ottobre 2016;

(xi) reati di abuso di mercato, previsti dalla Legge 18 aprile 2005, n. 62, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*sexies* e, all'interno del TUF, l'articolo 187-*quinquies* "*Responsabilità dell'ente*";

(xii) reati di omicidio colposo o lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro, introdotti dalla Legge 3 agosto 2007, n. 123, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*septies*, successivamente modificato dal D.Lgs. 81 del 9 aprile 2008;

(xiii) reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, introdotti dal Decreto Legislativo 21 novembre 2007, n. 231, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*octies*, successivamente integrato dalla Legge 186 del 15 dicembre 2014 - che introduce la fattispecie di autoriciclaggio (art. 648-ter.1 c.p.) - nonché modificato dal D.Lgs. 90 del 25 maggio 2017;

(xiv) delitti in materia di violazione del diritto d'autore, introdotti dall'articolo 15, comma 7, lett. c), della Legge 23 luglio 2009, n. 99, che ha inserito nel D.Lgs. n.

[5] Legge 15 luglio 2009, n. 94 recante "*Disposizioni in materia di sicurezza pubblica*".

[6] Legge 69/2015 *"Disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio"* pubblicata su Gazzetta Ufficiale n. 124 del 30/05/2015.

231 del 2001 l'articolo 25-*novies*;

(xv) delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dall'art. 4 della Legge 3 agosto 2009, n. 116, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*decies*[7], successivamente modificato dal D. Lgs. 121 del 7 luglio 2011;

(xvi) reati ambientali, introdotti dal D.Lgs. 7 luglio 2011, n. 121, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*undecies* [8] modificato dalla Legge 68 del 2015;

(xvii) reati transnazionali, introdotti dalla Legge 16 marzo 2006, n. 146, "*Legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale*";

(xviii) delitto di impiego di cittadini di Paesi terzi di cui il soggiorno è irregolare, introdotto dal Decreto Legislativo 16 luglio 2012, n. 109, recante l'"*Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare*", che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*duodecies,* successivamente integrato dal D.Lgs. 17 ottobre 2017, n. 161 con l'applicazione delle relative sanzioni pecuniarie ed interdittive (art. 30, co. 4);

(xix) razzismo e xenofobia, introdotto dalla legge 20 novembre 2017, n. 167, recante "*Disposizioni per la completa attuazione della decisione quadro 2008/913/GAI sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale"* che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*terdecies,*

(xx) frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, introdotto dalla Legge 3 maggio 2019, n. 39 recante la "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulle manipolazioni sportive (fatta a Magglingen il 18 settembre 2014)"*, che ha inserito nel D.Lgs. n. 231 del 2001 l'art. 25-*quaterdecies*;

(xxi) reati tributari, introdotti dalla Legge di conversione del 26 ottobre 2019, n.157, di definitiva approvazione del D.L. 124/2019, intitolato "*Disposizioni urgenti in materia fiscale e per esigenze indifferibili"*, che ha inserito nel D.Lgs n. 231 del 2001 l'articolo 25-*quinquesdecies*, successivamente modificato e integrato dal D.Lgs. 75 del 14 luglio 2020;

(xxii) contrabbando (D.P.R. 23 gennaio 1973, n. 43), introdotto dal D.Lgs. 75 del 14 luglio 2020, che ha inserito nel D.Lgs. n. 231 del 2001 l'articolo 25-*sexiesdecies*.

1.4 Le Sanzioni previste nel Decreto

Il D.Lgs. n. 231 del 2001 prevede le seguenti tipologie di sanzioni applicabili agli enti destinatari della normativa:

(a) sanzioni amministrative pecuniarie;
(b) sanzioni interdittive;

[7] Originariamente 25-*novies* e così rinumerato dal D.Lgs. 121/2011.
[8] La norma che introduce i reati ambientali nel D.Lgs 231/2001 è stata modificata dalla Legge 68/2015 *"Disposizioni in materia di delitti contro l'ambiente*" pubblicata su Gazzetta Ufficiale n. 122 del 28/05/2015 che introduce i cosiddetti "ecoreati".

(c) confisca del prezzo o del profitto del reato;
(d) pubblicazione della sentenza.

(a) La sanzione amministrativa pecuniaria, disciplinata dagli articoli 10 e seguenti del Decreto, costituisce la sanzione "di base" di necessaria applicazione, del cui pagamento risponde l'Ente con il suo patrimonio o con il fondo comune.

Il Legislatore ha adottato un criterio innovativo di commisurazione della sanzione, attribuendo al Giudice l'obbligo di procedere a due diverse e successive operazioni di apprezzamento. Ciò comporta un maggiore adeguamento della sanzione alla gravità del fatto ed alle condizioni economiche dell'Ente.

La prima valutazione richiede al Giudice di determinare il numero delle quote (in ogni caso non inferiore a cento, né superiore a mille)[9] tenendo conto:
- della gravità del fatto;
- del grado di responsabilità dell'Ente;
- dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Nel corso della seconda valutazione, il Giudice determina, entro i valori minimi e massimi predeterminati in relazione agli illeciti sanzionati, il valore di ciascuna quota, da un minimo di Euro 258,00 ad un massimo di Euro 1.549,00. Tale importo è fissato "*sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione*" (articoli 10 e 11, comma 2, D.Lgs. n. 231 del 2001).

Come affermato al punto 5.1. della Relazione al Decreto, "*Quanto alle modalità di accertamento delle condizioni economiche e patrimoniali dell'ente, il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazione le dimensioni dell'ente e la sua posizione sul mercato.* (…) *Il giudice non potrà fare a meno di calarsi, con l'ausilio di consulenti, nella realtà dell'impresa, dove potrà attingere anche le informazioni relative allo stato di solidità economica, finanziaria e patrimoniale dell'ente*".

L'articolo 12, D.Lgs. n. 231 del 2001, prevede una serie di casi in cui la sanzione pecuniaria viene ridotta. Essi sono schematicamente riassunti nella seguente tabella, con indicazione della riduzione apportata e dei presupposti per l'applicazione della riduzione stessa.

Riduzione	Presupposti
1/2	• L'autore del reato ha commesso il fatto nel

[9] Con riferimento ai reati di *market abuse*, il secondo comma dell'articolo 25-*sexies* del D.Lgs. n. 231 del 2001 prevede che: "S*e in seguito alla commissione dei reati di cui al comma 1, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto*".

Riduzione	Presupposti
(e non può comunque essere superiore ad Euro 103.291,00)	prevalente interesse proprio o di terzi *e* l'Ente non ne ha ricavato un vantaggio o ne ha ricavato un vantaggio minimo; *ovvero* • il danno patrimoniale cagionato è di particolare tenuità.
da 1/3 a ½	[Prima della dichiarazione di apertura del dibattimento di primo grado] • L'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *ovvero* • è stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.
da 1/2 a 2/3	[Prima della dichiarazione di apertura del dibattimento di primo grado] • L'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *e* • è stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

(b) Le seguenti **sanzioni interdittive** sono previste dal Decreto e si applicano solo in relazione ai reati per i quali sono espressamente previste:

- interdizione dall'esercizio dell'attività aziendale;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Perché le sanzioni interdittive possano essere comminate, è necessaria la sussistenza di almeno una delle condizioni di cui all'articolo 13, D.Lgs. n. 231 del 2001, ossia:

- "*l'ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative*"; ovvero

- "*in caso di reiterazione degli illeciti*"[10].

Inoltre, le sanzioni interdittive possono anche essere richieste dal Pubblico Ministero e applicate all'Ente dal Giudice in via cautelare, quando:

- sono presenti gravi indizi per ritenere la sussistenza della responsabilità dell'Ente per un illecito amministrativo dipendente da reato;
- emergono fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa specie di quello per cui si procede;
- l'Ente ha tratto un profitto di rilevante entità.

In ogni caso, non si procede all'applicazione delle sanzioni interdittive quando il reato è stato commesso nel prevalente interesse dell'autore o di terzi e l'Ente ne ha ricavato un vantaggio minimo o nullo, ovvero il danno patrimoniale cagionato è di particolare tenuità.

L'applicazione delle sanzioni interdittive è altresì esclusa dal fatto che l'Ente abbia posto in essere le condotte riparatrici previste dall'articolo 17, D.Lgs. n. 231 del 2001 e, più precisamente, quando concorrono le seguenti condizioni:

- "*l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso*";
- "*l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi*";
- "*l'ente ha messo a disposizione il profitto conseguito ai fini della confisca*".

Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni e la scelta della misura da applicare e della sua durata viene effettuata dal Giudice sulla base dei criteri in precedenza indicati per la commisurazione della sanzione pecuniaria, "*tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso*" (art. 14, D.Lgs. n. 231 del 2001).

Con riferimento ai soli reati di concussione, induzione indebita a dare o promettere utilità o corruzione, le sanzioni interdittive, qualora previste con durata compresa tra tre mesi e due anni, possono essere ridotte[11] nell'ipotesi in cui l'ente si adoperi affinché:
- l'attività delittuosa non sia portata a conseguenze ulteriori;
- siano assicurate le prove dei reati e l'individuazione dei responsabili;
- sia garantito il sequestro delle somme o di altre utilità trasferite;
- siano eliminate le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi.

Il Legislatore si è, poi, preoccupato di precisare che l'interdizione dell'attività ha natura

[10] Ai sensi dell'articolo 20 del D.Lgs. n. 231 del 2001, "*si ha reiterazione quando l'ente, già condannato in via definitiva almeno una volta per un illecito dipendente da reato, ne commette un altro nei cinque anni successivi alla condanna definitiva*".
[11] L'introduzione del beneficio della riduzione delle sanzioni interdittive si è avuta ad opera della Legge 9 gennaio 2019, n. 3, c.d. "Legge Anticorruzione".

residuale rispetto alle altre sanzioni interdittive.

(c) Ai sensi dell'articolo 19, D.Lgs. n. 231 del 2001, è sempre disposta, con la sentenza di condanna, la **confisca** - anche per equivalente - del prezzo (denaro o altra utilità economica data o promessa per indurre o determinare un altro soggetto a commettere il reato) o del profitto (utilità economica immediata ricavata) del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede.

(d) La **pubblicazione della sentenza di condanna** in uno o più giornali, per estratto o per intero, può essere disposta dal Giudice, unitamente all'affissione nel comune dove l'Ente ha la sede principale, quando è applicata una sanzione interdittiva. La pubblicazione è eseguita a cura della Cancelleria del Giudice competente e a spese dell'Ente.

1.5 Delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei reati presupposto del Decreto, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (articolo 26 del Decreto).

1.5.1 Le Condotte Esimenti

Gli articoli 6 e 7 del D.Lgs. n. 231 del 2001, prevedono forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i reati commessi nell'interesse o a vantaggio dello stesso sia da Soggetti Apicali, sia da Soggetti Sottoposti (come definiti al precedente paragrafo).

In particolare, nel caso di reati commessi da Soggetti Apicali, l'articolo 6 del Decreto prevede l'esonero qualora l'Ente stesso dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello verificatosi (di seguito, per brevità, il "**Modello**");
b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di curarne l'aggiornamento è stato affidato ad un organismo dell'Ente (di seguito, per brevità, l'"**Organismo di Vigilanza**" o l'"**OdV**"), dotato di autonomi poteri di iniziativa e controllo;
c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il Modello;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per quanto concerne i Soggetti Sottoposti, l'articolo 7 del Decreto prevede l'esonero della

responsabilità nel caso in cui l'Ente abbia adottato ed efficacemente attuato, prima della commissione del reato, un Modello idoneo a prevenire reati della specie di quello verificatosi.

L'esonero della responsabilità dell'Ente non è tuttavia determinato dalla mera adozione del Modello, bensì dalla sua efficace attuazione da realizzarsi attraverso l'implementazione di tutti i protocolli ed i controlli necessari a limitare il rischio di commissione dei reati che l'Organismo intende scongiurare. In particolare, con riferimento alle caratteristiche del Modello, il Decreto prevede espressamente, all'articolo 6, comma 2, le seguenti fasi propedeutiche ad una corretta implementazione del Modello stesso:

a) individuazione delle attività nel cui ambito esiste la possibilità che siano commessi reati;
b) previsione di specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
c) individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
d) previsione di obblighi di informazione nei confronti dell'Organismo di Vigilanza;
e) introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

1.6 Le Linee Guida

Su espressa indicazione del Legislatore delegato, i Modelli possono essere adottati sulla base di codici di comportamento redatti da associazioni rappresentative di categoria che siano stati comunicati al Ministero della Giustizia il quale, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sull'idoneità dei modelli a prevenire i reati.

La predisposizione del presente Modello è ispirata alle principali Linee Guida per la costruzione dei Modelli di organizzazione gestione e controllo *ex* D.Lgs. n. 231 del 2001, *in primis* quelle di Confindustria approvate originariamente in data 7 marzo 2002 e successivamente aggiornate (di seguito, per brevità, definite anche le "**Linee Guida**").

Il percorso indicato dalle Linee Guida 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 dai consulenti, 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 dalle Linee Guida di Confindustria sono, per quanto concerne la prevenzione dei reati dolosi:

- il Codice Comportamento (o di comportamento);
- il sistema organizzativo;
- le procedure manuali ed informatiche;
- i poteri autorizzativi e di firma;
- il sistema di controllo e gestione;
- la comunicazione al personale e sua formazione.

Con riferimento ai reati colposi (reati in materia di salute e sicurezza sul lavoro e la maggior parte dei reati ambientali), le componenti più rilevanti individuate da Confindustria sono:

- il Codice Comportamento (o di comportamento) con riferimento ai reati considerati;
- la struttura organizzativa,
- la formazione e addestramento,
- la comunicazione e coinvolgimento,
- la gestione operativa,
- il sistema di monitoraggio della sicurezza.

Il sistema di controllo 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 dei protocolli previsti dal Modello;
- individuazione di un Organismo di Vigilanza 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 reato”, di fornire informazioni all’Organismo di Vigilanza, sia su base strutturata (informativa periodica in attuazione del Modello stesso), sia per segnalare anomalie o atipicità riscontrate nell’ambito delle informazioni disponibili.

2. Il presente Modello

2.1 SIIT S.c.p.A.: profilo e storia aziendale.

SIIT S.c.p.A. è una società consortile per azioni costituita nel 2005 per sostenere ed accrescere competenze e competitività nel settore dell'innovazioni tecnologica regionale. La Società non persegue fini di lucro e rappresenta un sistema integrato tra grande industria, piccola e media impresa, Università di Genova, istituzioni pubbliche, di ricerca e finanziarie.
La Società pone particolare attenzione allo sviluppo di attività di ricerca industriale e di trasferimento tecnologico.
Gli obiettivi della Società sono finalizzati prioritariamente allo sviluppo cooperativo tra soggetti Industriali ed Enti di Ricerca per lo svolgimento e la realizzazione di attività di ricerca industriale e trasferimento tecnologico finalizzate a favorire la competitività regionale in coerenza con le Smart Specialization Strategies della Regione Liguria.
SIIT a partire dalla sua costituzione ha indirizzato la propria attività verso obiettivi ben delineati di sei piattaforme tematiche, di seguito riportate:

- Sicurezza;
- ITS/Mobilità, Trasporti e Logistica;
- Sistemi di Automazione;
- Organizzazioni complesse;
- Tecnologie Abilitanti;
- Servizi collegati.

Rientrano inoltre nell'ambito operativo di SIIT anche le attività di formazione, l'internazionalizzazione, l'indirizzo e la gestione dei laboratori di ricerca.
In particolare, oltre alle azioni dedicate ad attività di ricerca applicata, trasferimento tecnologico e prototipazione, nell'ottica di favorire la continua aggregazione sistemica tra grande, piccola e media industria e mondo della ricerca, sono significative le attività di informazioni, consulenza, formazione specialistica ed aggiornamento professionale per Enti ed Imprese.

2.2 Il presente Modello

2.2.1 Le finalità del Modello

SIIT S.c.p.A., nell'ambito del più ampio percorso di rafforzamento della propria *governance* aziendale e a fronte delle novità legislative e di modifiche organizzative endogene, ha ritenuto di procedere alla implementazione del Modello.

Il presente Modello, predisposto dalla Società sulla base dell'individuazione delle aree di possibile rischio nelle attività al cui interno si ritiene più alta la possibilità che siano commessi i reati, si propone come finalità quelle di:

- predisporre un sistema di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi alle proprie attività;
- rendere tutti coloro che operano in nome e per conto della Società, ed in particolare

quelli impegnati nelle "aree di attività a rischio", consapevoli di poter incorrere, in caso di violazione delle disposizioni in esso 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 con la Società che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale;
- confermare che la Società non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità e che, in ogni caso, tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi cui è ispirata l'attività imprenditoriale della Società.

2.2.2 La costruzione del Modello

Sulla base delle indicazioni contenute nelle Linee Guida di riferimento, la costruzione del Modello (e la successiva redazione del presente documento) si è articolata nelle fasi di seguito descritte:

(i) esame preliminare del contesto dell'ente attraverso l'analisi della documentazione societaria rilevante e lo svolgimento di interviste con i responsabili della Società informati sulla struttura e le attività della stessa, al fine di definire l'organizzazione e le attività eseguite dalle varie unità organizzative/funzioni aziendali, nonché i processi aziendali nei quali le attività sono articolate e la loro concreta ed effettiva attuazione;
(ii) individuazione delle aree di attività e dei processi aziendali "a rischio" operata sulla base del sopra citato esame preliminare del contesto dell'ente (di seguito, per brevità, cumulativamente indicate come le "**Aree a Rischio Reato**");
(iii) definizione in via di ipotesi delle principali possibili modalità di commissione dei Reati Presupposto all'interno delle singole Aree a Rischio Reato;
(iv) rilevazione ed individuazione del sistema di controllo dell'ente finalizzato a prevenire la commissione dei Reati Presupposto.

2.2.3 Il concetto di rischio accettabile

Nella predisposizione di un Modello di organizzazione e gestione, quale il presente, non può essere trascurato il concetto di rischio accettabile. È, infatti, imprescindibile stabilire, ai fini del rispetto delle previsioni introdotte dal D.Lgs. n. 231 del 2001, una soglia che consenta di limitare la quantità e qualità degli strumenti di prevenzione che devono essere adottati al fine di impedire la commissione del reato. Con specifico riferimento al meccanismo sanzionatorio introdotto dal Decreto, la soglia di accettabilità è rappresentata dall'efficace implementazione di un adeguato sistema preventivo che sia tale da non poter essere aggirato se non intenzionalmente, con conseguente prova, ai fini dell'esclusione della responsabilità amministrativa dell'ente, del fatto che le persone che hanno

commesso il reato hanno agito eludendo fraudolentemente il Modello ed i controlli adottati dalla Società.

2.2.4 La struttura del Modello ed i Reati Presupposto rilevanti ai fini della sua costruzione

La Società ha inteso predisporre un Modello che tenesse conto della propria peculiare realtà aziendale, in coerenza con il proprio sistema di governo e in grado di valorizzare i controlli e gli organismi esistenti.

Il Modello, pertanto, rappresenta un insieme coerente di principi, regole e disposizioni che:

- incidono sul funzionamento interno della Società e sulle modalità con le quali la stessa si rapporta con l'esterno;
- regolano la diligente gestione di un sistema di controllo delle Aree a Rischio Reato, finalizzato a prevenire la commissione, o la tentata commissione, dei reati richiamati dal Decreto.

In particolare, il Modello di SIIT S.c.p.A. . è costituito da:

- una "**Parte Generale**", che contiene i principi cardine del Modello stesso;
- una "**Parte Speciale**", contenente la descrizione delle norme di comportamento generali implementate dalla Società per ogni categoria di Reato Presupposto, con una sezione di dettaglio strutturata per processo e contenente l'indicazione delle Aree a Rischio Reato individuate in relazione ai Reati Presupposto rilevanti e la descrizione dei controlli preventivi implementati al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/01 ritenuti rilevanti per la Società.

A seguito della valutazione dell'attività in concreto svolta da SIIT S.c.p.A. e della sua storia, sono state dalla Società considerate teoricamente rilevanti le seguenti fattispecie di reato:

- **Reati contro la Pubblica Amministrazione e/o in danno dell'Unione europea** (Artt. 24 e 25 del Decreto);
- **Delitti informatici e trattamento illecito dei dati** (Art. 24-*bis* del Decreto);
- **Delitti di criminalità organizzata** (Art. 24-*ter* del Decreto);
- **Reati di Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** (Art. 25-*bis* del Decreto);
- **Delitti contro l'industria e il commercio** (Art. 25-*bis* 1 del Decreto);
- **Reati societari** (Art.25-*ter* del Decreto);
- **Delitti con finalità di terrorismo o eversione dell'ordine democratico** (Art. 25-*quater* del Decreto);
- **Delitti contro la personalità individuale** (Art. 25-*quinquies*);
- **Reati in materia di salute e sicurezza sul lavoro** (Art.25-*septies*);
- **Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (Art.25-*octies* del Decreto);

- **Delitti in materia di violazione del diritto d'autore** (Art.25-nonies del Decreto);
- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria** (Art. 25-*decies* del Decreto);
- **Reati Ambientali** (Art. 25-*undecies* del Decreto);
- **Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare** (Art. 25-*duodecies* del Decreto);
- **Reati tributari** (Art. 25-*quinquesdecies* del Decreto);
- **Reati transnazionali** (Legge 6 marzo 2006, n. 146).

In ogni caso, i principi etici su cui si fonda il Modello della Società e la sua struttura di *governance* sono finalizzati a prevenire in linea generale anche quelle fattispecie di reato che non trovano disciplina specifica nelle Parti Speciali del presente Modello.

2.2.5 L'adozione del Modello

L'adozione del presente Modello è demandata dal Decreto stesso alla competenza dell'organo dirigente (ed in particolare al Consiglio di Gestione), al quale è altresì attribuito il compito di integrare il presente Modello con ulteriori Parti Speciali relative ad altre tipologie di Reati Presupposto di nuova introduzione nel D.Lgs. n. 231 del 2001.

2.3 I documenti connessi al Modello

Formano parte integrante e sostanziale del Modello i seguenti documenti:

- Codice di Condotta contenente l'insieme dei diritti, doveri e responsabilità di SIIT S.c.p.A. nei confronti dei destinatari del Modello stesso (di seguito, per brevità, **"Codice Comportamento**");
- sistema di procedure, di protocolli e di prassi e controlli interni aventi quale finalità quella di garantire un'adeguata trasparenza e conoscibilità dei processi decisionali e finanziari, nonché dei comportamenti che devono essere tenuti dai destinatari del presente Modello operanti nelle Aree a Rischio Reato (di seguito, per brevità, il sistema delle deleghe e procure, le procedure, i protocolli ed i controlli interni sopra citati verranno cumulativamente definiti le "**Procedure**").

Ne consegue che con il termine Modello deve intendersi non solo il presente documento, ma altresì tutti gli ulteriori documenti e le Procedure che verranno successivamente adottati secondo quanto previsto nello stesso e che perseguiranno le finalità ivi indicate.

2.4 Gestione delle risorse finanziarie

Fermo restando quanto indicato al precedente paragrafo, tenuto conto che - ai sensi dell'articolo 6, lettera c) del D.Lgs. n. 231 del 2001 - tra le esigenze cui il Modello deve

rispondere vi è anche l'individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati, la Società ha adottato specifici protocolli contenenti i principi ed i comportamenti da seguire nell'ambito della gestione di tali risorse.

2.5 Diffusione del Modello

2.5.1 Destinatari

Il presente Modello tiene conto della particolare realtà imprenditoriale di SIIT S.c.p.A. e rappresenta un valido strumento di sensibilizzazione ed informazione dei Soggetti Apicali e dei Soggetti Sottoposti (di seguito, per brevità, i "**Destinatari**").

Tutto ciò affinché i Destinatari seguano, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti in linea con i valori Comportamento-sociali cui si ispira la Società nel perseguimento del proprio oggetto sociale e tali, comunque, da prevenire il rischio di commissione dei reati previsti dal Decreto.

In ogni caso, le funzioni aziendali competenti assicurano il recepimento nelle Procedure della Società dei principi e delle norme di comportamento contenuti nel Modello e nel Codice Comportamento di SIIT S.c.p.A.

2.5.2 Formazione ed Informazione del Personale

È obiettivo della Società garantire una corretta conoscenza da parte dei Destinatari circa il contenuto del Decreto e gli obblighi derivanti dal medesimo.

Ai fini dell'efficace attuazione del presente Modello, la formazione e l'informativa verso i Destinatari sono gestite dalla Funzione competente in materia di gestione delle Risorse Umane in stretto coordinamento con l'Organismo di Vigilanza e con le altre funzioni aziendali di volta in volta coinvolte nella applicazione del Modello.

Le principali modalità di svolgimento delle attività di formazione/informazione necessarie anche ai fini del rispetto delle disposizioni contenute nel Decreto, attengono la specifica informativa all'atto dell'assunzione e le ulteriori attività ritenute necessarie al fine di garantire la corretta applicazione delle disposizioni previste nel Decreto. In particolare è prevista:

- una comunicazione iniziale. A tale proposito, l'adozione del presente Modello è comunicata a tutte le risorse presenti in Società. Ai nuovi assunti viene consegnato il Codice Comportamento ed il Modello - Parte Generale di SIIT S.c.p.A.. Agli stessi, viene inoltre fatto sottoscrivere un modulo con il quale prendono atto che il Modello è disponibile nella *intranet* aziendale e si impegnano ad osservare i contenuti della normativa citata. Inoltre, ai Soggetti Apicali e/o Sottoposti che operano nelle Aree a Rischio Reato, viene data informativa della/e Parte/i Speciale/i che riguarda/no

l'Area di riferimento;
- una specifica attività di formazione. Tale attività di formazione "continua" è obbligatoria e sviluppata attraverso strumenti e procedure informatiche (*e-mail* di aggiornamento, *intranet* aziendale, strumenti di autovalutazione ecc.), nonché incontri e seminari di formazione ed aggiornamento periodici. Tale attività è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società.

Al fine di garantire l'effettiva diffusione del Modello e l'informazione del personale con riferimento ai contenuti del Decreto ed agli obblighi derivanti dall'attuazione del medesimo, è istituita una specifica sezione della *intranet* aziendale (nella quale sono presenti e disponibili tutti i documenti che compongono il Modello) dedicata all'argomento e aggiornata, di volta in volta, dalla funzione interna di riferimento in coordinamento o su indicazione dell'Organismo di Vigilanza.

2.5.3 Informazione ai Terzi e diffusione del Modello

La Società prevede altresì la diffusione del Modello alle persone che intrattengono con la Stessa rapporti di collaborazione senza vincolo di subordinazione, rapporti di consulenza, rapporti di agenzia, rapporti di rappresentanza commerciale ed altri rapporti che si concretizzino in una prestazione professionale, non a carattere subordinato, sia continuativa sia occasionale (ivi inclusi i soggetti che agiscono per i fornitori e i *partners*, anche sotto forma di associazione temporanea di imprese, nonché *joint-venture*) (di seguito, per brevità, i "**Terzi**").

In particolare, le funzioni aziendali, di volta in volta coinvolte, forniscono ai soggetti Terzi in generale e alle società di *service* con cui entrano in contatto, idonea informativa in relazione all'adozione da parte di SIIT S.c.p.A. del Modello ai sensi del D.Lgs. n. 231 del 2001. La Società invita, inoltre, i Terzi a prendere visione dei contenuti del Codice Comportamento e della Parte Generale del Modello presenti sul sito *internet* della stessa.

Nei rispettivi testi contrattuali sono inserite specifiche clausole dirette ad informare i Terzi dell'adozione del Modello da parte di SIIT S.c.p.A., di cui gli stessi dichiarano di aver preso visione e di aver conoscenza delle conseguenze derivanti dal mancato rispetto dei precetti contenuti nella Parte Generale del Modello, nel Codice Comportamento nonché si obbligano a non commettere e a far sì che i propri apicali o sottoposti si astengano dal commettere alcuno dei Reati Presupposto.

3. Elementi del modello di *governance* e dell'assetto organizzativo generale di SIIT S.c.p.A. .

3.1 Il Modello di *governance* della Società

SIIT S.c.p.A. è una società consortile per azioni, che non persegue fini di lucro e che ha adottato un sistema di gestione duale.
La Società è amministrata dal Consiglio di Gestione composto da 3 (tre) componenti, incluso il Presidente del Consiglio di Gestione.

I consiglieri durano in carica per il periodo stabilito all'atto della loro nomina, comunque non superiore a 3 (tre) esercizi e sono rieleggibili. Essi scadono alla data dell'assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della loro carica. Il venire meno della sussistenza dei requisiti di legge costituisce causa di immediata decadenza dell'amministratore.

Al Consiglio di Gestione spetta comunque il potere di controllo e di avocare a sé le operazioni rientranti nella delega, oltre che il potere di revocare le deleghe.
Gli eventuali organi e soggetti delegati sono tenuti a riferire al consiglio di gestione ed al Consiglio di Sorveglianza con cadenza periodica.

Il Consiglio di Gestione è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, con facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione ed il raggiungimento dello scopo sociale.

Il Consiglio Sorveglianza, come organo di controllo, è composto da 26 (ventisei) membri ai quali si aggiunge il revisore legale, nominato ed incaricato del controllo contabile della Società.

3.2 Il sistema di controllo interno di SIIT S.c.p.A. .

SIIT S.c.p.A. ha adottato i seguenti strumenti di carattere generale, diretti a programmare la formazione e l'attuazione delle decisioni della Società (anche in relazione ai reati da prevenire):

- i principi etici ai quali la Società si ispira, anche sulla base di quanto stabilito nel Codice Comportamento;
- il sistema di deleghe e procure;
- la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale aziendale ed organizzativa;
- il sistema di controllo interno e quindi la struttura delle procedure aziendali;
- le procedure afferenti il sistema amministrativo, contabile e di *reporting*;
- le comunicazioni e le circolari aziendali dirette al personale;
- la formazione obbligatoria, adeguata e differenziata di tutto il personale;
- il sistema sanzionatorio di cui ai CCNL applicabili;
- il "*corpus*" normativo e regolamentare nazionale e straniero qualora applicabile.

3.3 Principi generali di controllo in tutte le Aree a Rischio Reato

In aggiunta ai controlli specifici descritti in ciascuna Sezione della Parte Speciale del presente Modello, la Società ha implementato specifici controlli generali applicabili in tutte le Aree a Rischio Reato.

Si tratta, nello specifico, dei seguenti controlli:

- **Trasparenza**: ogni operazione/transazione/azione deve essere giustificabile, verificabile, coerente e congruente;

- **Separazione delle funzioni/Poteri**: nessuno può gestire in autonomia un intero processo e può essere dotato di poteri illimitati; i poteri autorizzativi e di firma devono essere definiti in modo coerente con le responsabilità organizzative assegnate;

- **Adeguatezza delle norme interne**: l'insieme delle norme dell'ente deve essere coerente con l'operatività svolta ed il livello di complessità organizzativa e tale da garantire i controlli necessari a prevenire la commissione dei reati previsti dal Decreto;

- **Tracciabilità/Documentabilità**: ogni operazione/transazione/azione, nonché la relativa attività di verifica e controllo devono essere documentate e la documentazione deve essere adeguatamente archiviata.

4. L'Organismo di Vigilanza

4.1 Caratteristiche dell'Organismo di Vigilanza

Secondo le disposizioni del D.Lgs. n. 231 del 2001 (articoli 6 e 7), nonché le indicazioni contenute nelle Linee Guida di Confindustria, le caratteristiche dell'Organismo di Vigilanza, tali da assicurare un'effettiva ed efficace attuazione del Modello, devono essere:

(a) autonomia ed indipendenza;
(b) professionalità;
(c) continuità d'azione.

4.1.1 Autonomia ed indipendenza

I requisiti di autonomia ed indipendenza sono fondamentali affinché l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo e, dunque, non subisca condizionamenti o interferenze da parte dell'organo dirigente.

Tali requisiti si possono ottenere garantendo all'Organismo di Vigilanza la posizione gerarchica più elevata possibile, e prevedendo un'attività di *reporting* ai vertici aziendali.

Ai fini dell'indipendenza è inoltre indispensabile che all'OdV non siano attribuiti compiti operativi, che ne comprometterebbero l'obiettività di giudizio con riferimento a verifiche sui comportamenti e sull'effettività del Modello.

4.1.2 Professionalità

L'OdV deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio[12].

4.1.3 Continuità d'azione

L'Organismo di Vigilanza deve:

- svolgere in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine;
- essere una struttura riferibile alla Società, in modo da garantire la dovuta continuità nell'attività di vigilanza.

Per assicurare l'effettiva sussistenza dei requisiti descritti in precedenza, è opportuno che tali soggetti posseggano, oltre alle competenze professionali descritte, i requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito (es. onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi dell'ente e con il vertice, etc.).

4.2 Individuazione dell'Organismo di Vigilanza

Il Consiglio di Gestione di SIIT S.c.p.A. ha nominato quale Organismo di Vigilanza della Società un organo monocratico composto da un membro, individuato in un professionista esterno di adeguato profilo.

Tale organismo garantisce l'autonomia dell'iniziativa di controllo da ogni forma di interferenza e/o di condizionamento da parte di qualunque componente dell'organizzazione, assicurando al contempo sufficiente continuità d'azione e, nel complesso, permette di soddisfare il requisito della professionalità in relazione alle diverse categorie di Reati Presupposto.

Con la medesima delibera che ha nominato l'OdV, il Consiglio di Gestione della Società ha fissato il compenso spettante a tale organo per l'incarico assegnatogli, nonché le risorse necessarie per l'espletamento delle proprie attribuzioni, come meglio dettagliate nel prosieguo del documento.

L'Organismo di Vigilanza provvede a dotarsi di un proprio regolamento interno, nonché

[12] Ci si riferisce, tra l'altro, a: tecniche di analisi e valutazione dei rischi; misure per il loro contenimento (procedure organizzative, meccanismi di contrapposizione dei compiti, etc.); *flow charting* di procedure e processi per l'individuazione dei punti di debolezza, tecniche di intervista e di elaborazione dei questionari; metodologie per l'individuazione di frodi; etc. L'Organismo di Vigilanza deve avere competenze di tipo ispettivo (per accertare come si sia potuto verificare un reato della specie in esame e chi lo abbia commesso); competenze di tipo consulenziale (per adottare – all'atto del disegno del Modello e delle successive modifiche – le misure più idonee a prevenire, con ragionevole certezza, la commissione dei reati medesimi) o, ancora, correntemente per verificare che i comportamenti quotidiani rispettino effettivamente quelli codificati) e competenze giuridiche. Il D.Lgs. n. 231 del 2001 è una disciplina penale ed avendo l'attività dell'Organismo di Vigilanza lo scopo di prevenire la realizzazione dei reati è dunque essenziale la conoscenza della struttura e delle modalità realizzative dei reati (che potrà essere assicurata mediante l'utilizzo delle risorse aziendali, ovvero della consulenza esterna).

a stabilire ed aggiornare il piano delle attività da svolgere annualmente.

4.3 Durata dell'incarico e cause di cessazione

L'Organismo di Vigilanza resta in carica per la durata indicata nell'atto di nomina e può essere rinnovato.

La cessazione dall'incarico dell'OdV può avvenire per una delle seguenti cause:
- scadenza dell'incarico;
- revoca dell'Organismo da parte del Consiglio di Gestione;
- rinuncia del componente, formalizzata mediante apposita comunicazione scritta inviata al Consiglio di Gestione e al Consiglio di Sorveglianza;
- sopraggiungere di una delle cause di decadenza di cui al successivo paragrafo.

La revoca dell'OdV può essere disposta solo per giusta causa e tali devono intendersi, a titolo esemplificativo, le seguenti ipotesi:
- il caso in cui il componente sia coinvolto in un processo penale avente ad oggetto la commissione di un delitto;
- il caso in cui sia riscontrata la violazione degli obblighi di riservatezza previsti a carico dell'OdV;
- una grave negligenza nell'espletamento dei compiti connessi all'incarico;
- il possibile coinvolgimento della Società in un procedimento, penale o civile, che sia connesso ad un'omessa o insufficiente vigilanza, anche colposa.

La revoca è disposta con delibera del Consiglio di Gestione, previo parere vincolante del Consiglio di Sorveglianza della Società.

In caso di scadenza, revoca o rinuncia, il Consiglio di Gestione nomina senza indugio il nuovo componente dell'OdV, mentre il componente uscente rimane in carica fino alla sua sostituzione.

4.4 Casi di ineleggibilità e di decadenza

Costituiscono motivi di ineleggibilità e/o di decadenza del componente dell'OdV:
a) l'interdizione, l'inabilitazione, il fallimento o, comunque, la condanna penale, anche non passata in giudicato, per uno dei reati previsti dal Decreto o, comunque, ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;
b) l'esistenza di relazioni di parentela, coniugio o affinità entro il quarto grado con i membri del Consiglio di Gestione o del Consiglio di Sorveglianza, o con i soggetti esterni incaricati della revisione;
c) l'esistenza di rapporti di natura patrimoniale tra il componente e la Società tali da compromettere l'indipendenza del componente stesso.

Qualora, nel corso dell'incarico, dovesse sopraggiungere una causa di decadenza, il componente l'Organismo di Vigilanza è tenuto ad informare immediatamente il Consiglio di Gestione.

4.5 Funzioni, compiti e poteri dell'Organismo di Vigilanza

In conformità alle indicazioni fornite dal Decreto e dalle Linee Guida, la funzione dell'Organismo di Vigilanza consiste, in generale, nel:

1. vigilare sull'effettiva applicazione del Modello in relazione alle diverse tipologie di reati presi in considerazione dallo stesso;
2. verificare l'efficacia del Modello e la sua reale capacità di prevenire la commissione dei reati in questione;
3. individuare e proporre al Consiglio di Gestione aggiornamenti e modifiche del Modello stesso in relazione alla mutata normativa o alle mutate necessità o condizioni aziendali;
4. verificare che le proposte di aggiornamento e modifica formulate dal Consiglio di Gestione siano state effettivamente recepite nel Modello.

Nell'ambito della funzione sopra descritta, spettano all'OdV i seguenti compiti:

a. verificare periodicamente la mappa delle Aree a Rischio Reato e l'adeguatezza dei punti di controllo al fine di consentire il loro adeguamento ai mutamenti dell'attività e/o della struttura aziendale. A questo scopo, i destinatari del Modello, così come meglio descritti nelle parti speciali dello stesso, devono segnalare all'OdV le eventuali situazioni in grado di esporre la Società al rischio di reato. Tutte le comunicazioni devono essere redatte in forma scritta e trasmesse all'apposito indirizzo di posta elettronica attivato dall'OdV;
b. effettuare periodicamente, sulla base del piano di attività dell'OdV previamente stabilito, verifiche ed ispezioni mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle Aree a Rischio Reato;
c. raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni di cui al successivo paragrafo) rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV;
d. condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello portate all'attenzione dell'OdV da specifiche segnalazioni o emerse nel corso dell'attività di vigilanza dello stesso;
e. verificare che gli elementi previsti nel Modello per le diverse tipologie di reati (clausole *standard*, procedure e relativi controlli, sistema delle deleghe, etc.) vengano effettivamente adottati ed implementati e siano rispondenti alle esigenze di osservanza del D.Lgs. n. 231 del 2001, provvedendo, in caso contrario, a proporre azioni correttive ed aggiornamenti degli stessi.

Per lo svolgimento delle funzioni e dei compiti sopra indicati, vengono attribuiti all'OdV i seguenti poteri:

1. accedere in modo ampio e capillare ai vari documenti aziendali ed, in particolare, a quelli riguardanti i rapporti di natura contrattuale e non instaurati dalla Società con terzi;
2. avvalersi del supporto e della cooperazione delle varie strutture aziendali e degli organi dell'ente che possano essere interessati, o comunque coinvolti, nelle attività di controllo;
3. conferire specifici incarichi di consulenza ed assistenza a professionisti anche esterni alla Società.

4.6 Risorse dell'Organismo di Vigilanza

Il Consiglio di Gestione assegna all'OdV le risorse umane e finanziarie ritenute opportune ai fini dello svolgimento dell'incarico assegnato. In particolare, all'Organismo di Vigilanza sono attribuiti autonomi poteri di spesa, nonché la facoltà di stipulare, modificare e/o risolvere incarichi professionali a soggetti terzi in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico.

4.7 Flussi informativi dell'Organismo di Vigilanza

4.7.1 Obblighi di informazione nei confronti dell'Organismo di Vigilanza

Al fine di agevolare l'attività di vigilanza sull'efficacia del Modello, l'OdV deve essere informato, mediante apposite segnalazioni da parte dei Destinatari (e, ove del caso, dei Terzi) in merito ad eventi che potrebbero comportare la responsabilità di SIIT S.c.p.A. . ai sensi del D.Lgs. n. 231 del 2001.

I flussi informativi verso l'OdV si distinguono in informazioni di carattere generale ed informazioni specifiche obbligatorie.

Nel primo caso valgono le seguenti prescrizioni:

- i Destinatari sono tenuti a segnalare all'OdV le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei reati o a pratiche non in linea con le procedure e le norme di comportamento emanate o che verranno emanate da SIIT S.c.p.A.;
- i Terzi sono tenuti ad effettuare le segnalazioni relative alla commissione, o alla ragionevole convinzione di commissione, dei reati nei limiti e secondo le modalità previste contrattualmente;
- i Terzi sono tenuti ad effettuare le eventuali segnalazioni direttamente all'OdV.

Oltre alle segnalazioni relative alle violazioni di carattere generale sopra descritte, devono essere obbligatoriamente e tempestivamente trasmesse all'OdV le informazioni concernenti:

- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da

qualsiasi altra autorità, inerenti lo svolgimento di indagini che vedano coinvolta SIIT S.c.p.A. od i componenti degli organi sociali;
- i rapporti eventualmente predisposti dai responsabili di altri organi (ad esempio, Consiglio di Sorveglianza nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza del D.Lgs. n. 231 del 2001;
- le notizie relative a procedimenti disciplinari nonché ad eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di reati o violazione delle regole di comportamento o procedurali del Modello;
- le commissioni di inchiesta o relazioni/comunicazioni interne da cui emerga la responsabilità per le ipotesi di reato di cui al D.Lgs. n. 231 del 2001;
- i cambiamenti organizzativi;
- gli aggiornamenti del sistema delle deleghe e dei poteri;
- le operazioni particolarmente significative svolte nell'ambito delle Aree a Rischio Reato;
- i mutamenti nelle Aree a Rischio Reato o potenzialmente a rischio;
- le eventuali comunicazioni del Consiglio di Sorveglianza in merito ad aspetti che possono indicare carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società;
- la dichiarazione di veridicità e completezza delle informazioni contenute nelle comunicazioni sociali;
- la copia dei verbali delle riunioni del Consiglio di Gestione, del Consiglio di Sorveglianza.

4.7.2 Segnalazioni nei confronti dell'Organismo di Vigilanza ai sensi dell'art. 6 comma 2 bis lettera a) del D.Lgs. 231/01

In relazione alle segnalazioni previste ai sensi dell'art. 6 comma 2 *bis* lettera a) del D.Lgs. 231/01, SIIT S.c.p.A. ha individuato nell'OdV l'organo deputato alla ricezione.
Pertanto le segnalazioni *ex* art. 6 comma 2 *bis* lettera a) a tutela dell'integrità dell'Ente, potranno essere indirizzate dai Destinatari del presente Modello (come definiti nel par. 3.2) all'OdV, attraverso i canali e secondo le modalità specificate nei paragrafi seguenti.
Le segnalazioni potranno avere ad oggetto condotte illecite che abbiano attinenza ai reati presupposto previsti a norma del D. Lgs. 231/01 ovvero violazioni correlate al Modello adottato da SIIT S.c.p.A..
In particolare potranno essere presentate:
- segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del D. Lgs. 231/01 e fondate su elementi di fatto precisi e concordanti;
- segnalazioni di violazioni del Modello adottato da SIIT S.c.p.A., di cui siano venuti a conoscenza in ragione delle funzioni svolte.

4.7.3 Gestione dei flussi e delle segnalazioni

- SIIT S.c.p.A. ha adottato i seguenti specifici canali informativi dedicati al fine di gestire i flussi verso l'OdV, nonché le segnalazioni rientranti nelle ipotesi disciplinate dall'art. 6 comma 2 *bis* del D.Lgs. 231/01. A riguardo è stata istituita una casella di posta elettronica certificata dedicata esclusivamente all'OdV avente l'indirizzo segnalazioni.siit@legalmail.it,

al fine di:

- assicurare la segretezza nella direzione dei flussi comunicati all'OdV ovvero al Legale Rappresentante/Datore di lavoro e facilitarne il flusso;
- garantire la riservatezza dell'identità del segnalante anche nelle attività di gestione delle comunicazioni (con specifico riguardo alle segnalazioni di cui all'art. 6 comma 2 bis lettera a) del D. Lgs. 231/01).

L'OdV valuta le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine può ascoltare l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere. In ogni caso, i segnalanti saranno garantiti da qualsiasi forma di ritorsione o penalizzazione e ad essi sarà assicurata la massima riservatezza, fatti salvi gli obblighi di legge e le esigenze di tutela della Società o delle persone accusate erroneamente o in malafede.
E' fatto divieto di porre in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione (c.d. "misure di tutela del segnalante").

In particolare, l'OdV valuta le segnalazioni ricevute con discrezionalità e responsabilità, secondo quanto indicato all'interno del proprio Regolamento.

4.7.4 Obblighi di informazione propri dell'Organismo di Vigilanza

Premesso che la responsabilità di adottare ed efficacemente implementare il Modello permane in capo al Consiglio di Gestione della Società, l'OdV riferisce in merito all'attuazione del Modello e al verificarsi di eventuali criticità.

In particolare, l'Organismo di Vigilanza ha la responsabilità nei confronti del Consiglio di Gestione di:
- comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere al fine di adempiere ai compiti assegnati;
- comunicare periodicamente lo stato di avanzamento del programma unitamente alle eventuali modifiche apportate allo stesso;
- comunicare tempestivamente eventuali problematiche connesse alle attività, laddove

rilevanti;
- relazionare, con cadenza almeno semestrale, in merito all'attuazione del Modello.

L'OdV sarà tenuto a relazionare periodicamente il Consiglio Gestione ed il Consiglio di Sorveglianza in merito all'esecuzione delle proprie attività.

L'Organismo potrà richiedere di essere convocato dai suddetti organi per riferire in merito al funzionamento del Modello o a situazioni specifiche. Gli incontri con gli organi dell'ente cui l'OdV riferisce devono essere verbalizzati. Copia di tali verbali sarà custodita dall'OdV e dagli organi di volta in volta coinvolti.

Fermo restando quanto sopra, l'Organismo di Vigilanza potrà, inoltre, comunicare, valutando le singole circostanze:

(i) i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'OdV ottenga dai responsabili dei processi un piano delle azioni, con relativa tempistica, per l'implementazione delle attività suscettibili di miglioramento nonché il risultato di tale implementazione;

(ii) segnalare al Consiglio di Gestione e al Consiglio di Sorveglianza comportamenti/azioni non in linea con il Modello al fine di:
   a) acquisire dal Consiglio di Gestione tutti gli elementi per effettuare eventuali comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
   b) dare indicazioni per la rimozione delle carenze onde evitare il ripetersi dell'accadimento.

L'Organismo, infine, ha l'obbligo di informare immediatamente il Consiglio di Sorveglianza qualora la violazione riguardi i componenti del Consiglio di Gestione.

5. Sistema Sanzionatorio per mancata osservanza del presente Modello e delle norme-disposizioni ivi richiamate

5.1 Principi generali

SIIT S.c.p.A. prende atto e dichiara che la l'adozione di un adeguato sistema sanzionatorio per la violazione delle norme contenute nel Modello, nei relativi Allegati e nelle Procedure è condizione essenziale per assicurare l'effettività del Modello stesso.

Al riguardo, infatti, lo stesso articolo 6 comma 2, lettera e), del Decreto prevede che i modelli di organizzazione e gestione devono *"introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello"*.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello e dalle

Procedure sono assunte dalla Società in piena autonomia e indipendentemente dalla tipologia di illeciti di cui al D.Lgs. n. 231 del 2001 che le violazioni in questione possano determinare.
Più precisamente, la mancata osservanza delle norme contenute nel Modello e nelle Procedure lede, infatti, di per sé sola, il rapporto di fiducia in essere con la Società e comporta azioni disciplinari a prescindere dall'eventuale instaurazione di un giudizio penale nei casi in cui la violazione costituisca reato. Ciò anche nel rispetto dei principi di tempestività e immediatezza della contestazione disciplinare e della irrogazione delle sanzioni, in ottemperanza alle norme di legge vigenti.

Le sanzioni devono spaziare da misure conservative, per le infrazioni più tenui, a provvedimenti idonei a recidere il rapporto tra l'agente e l'ente, nel caso di violazioni più gravi. Il potere disciplinare deve sempre conformarsi ai principi di proporzione (sanzione commisurata alla violazione) e contradditorio (coinvolgimento del soggetto interessato).

SIIT S.c.p.a. prevede di adottare a riguardo il sistema sanzionatorio di cui al C.C.N.L. di riferimento

È possibile prevedere inoltre meccanismi premiali riservati a quanti cooperano al fine dell'efficace attuazione del Modello. Spesso, infatti, quando si intende promuovere il rispetto delle regole, la prospettazione dei vantaggi derivanti dalla loro osservanza può risultare più efficace della minaccia di conseguenze negative per la loro violazione.

5.2 Definizione di "Violazione" ai fini dell'operatività del presente Sistema Sanzionatorio

A titolo meramente generale ed esemplificativo, costituisce "**Violazione**" del presente Modello e delle relative Procedure:

- la messa in atto di azioni o comportamenti, non conformi alla legge e alle prescrizioni contenute nel Modello stesso e nelle relative Procedure, che comportino una situazione di mero rischio di commissione di uno dei reati contemplati dal D.Lgs. n. 231 del 2001;
- l'omissione di azioni o comportamenti prescritti nel Modello e nelle relative Procedure che comportino una situazione di mero rischio di commissione di uno dei reati contemplati dal D.Lgs. n. 231 del 2001;
- ai sensi dell'art. 6 comma 2 bis del D.Lgs. 231 del 2001, la messa in atto di azioni o comportamenti inosservanti delle specifiche "misure di tutela del segnalante", nonché, la messa in atto di azioni o comportamenti, realizzati con dolo o colpa grave, volti alla presentazione di segnalazioni che si rivelino, poi, infondate.

5.3 Sistema disciplinare

5.3.1 Personale dipendente in posizione non dirigenziale

I comportamenti tenuti dai lavoratori dipendenti in violazione delle norme contenute nel

presente Modello e nelle Procedure Aziendali sono definiti come *illeciti disciplinari*.

Con riferimento alla tipologia di sanzioni irrogabili nei riguardi di detti lavoratori dipendenti, esse rientrano tra quelle previste dai Contratti Collettivi Nazionali di Lavoro (di seguito, per brevità, i "**CCNL**"), nel rispetto delle procedure previste dall'articolo 7 della Legge n. 300 del 1970 (di seguito, per brevità, lo "**Statuto dei lavoratori**") ed eventuali normative speciali applicabili.

La Violazione da parte del personale dipendente, ai sensi del precedente paragrafo del presente Modello, può dar luogo, secondo la gravità della Violazione stessa, a provvedimenti, che vengono stabiliti in applicazione dei principi di proporzionalità, nonché dei criteri di correlazione tra infrazione sanzione e, comunque, nel rispetto della forma e delle modalità previste dalla normativa vigente.

Fatto, in ogni caso, salvo quanto indicato nel Sistema Disciplinare eventualmente introdotto in SIIT S.c.p.A., le sanzioni irrogabili nei riguardi dei dipendenti rientrano tra quelle previste dal CCNL di riferimento.

Il sistema disciplinare viene costantemente monitorato dall'Organismo di Vigilanza.

5.3.2 Dirigenti

In caso di: (a) Violazione ai sensi di quanto sopracitato, o (b) adozione, nell'espletamento di attività nelle Aree a Rischio Reato, di un comportamento non conforme alle prescrizioni dei documenti sopra citati, da parte del personale inquadrato come dirigente, si provvederà ad applicare nei confronti dei responsabili le misure disciplinari più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti.

5.3.3 Consiglieri

Nel caso di Violazione delle regole sopradescritte da parte di uno o più dei Consiglieri di SIIT S.c.p.A., l'Organismo di Vigilanza informerà senza indugio l'intero Consiglio di Gestione ed il Consiglio di Sorveglianza della Società per le opportune valutazioni e provvedimenti.

Nell'ipotesi in cui sia stato disposto il rinvio a giudizio di uno o più dei Consiglieri, presunti autori del reato da cui deriva la responsabilità amministrativa della Società, il Presidente del Consiglio di Gestione di SIIT S.c.p.A. (o, in sua vece, un Consigliere delegato) dovrà procedere alla convocazione del Consiglio per deliberare in merito alla revoca del mandato.

5.3.4 Revisori

Nel caso di Violazione delle regole di cui al precedente paragrafo, da parte di uno o più Revisori Legali, l'Organismo di Vigilanza informa il Consiglio di Gestione affinché lo

stesso venga convocato ed affinché siano adottati gli opportuni provvedimenti.

5.3.5 Terzi: collaboratori e consulenti esterni

Nel caso di Violazione delle regole di cui al precedente paragrafo, da parte di collaboratori o consulenti esterni, o, più in generale, di Terzi, la Società, a seconda della gravità della violazione: (i) richiamerà gli interessati al rigoroso rispetto delle disposizioni ivi previste; o (ii) avrà titolo, in funzione delle diverse tipologie contrattuali, di recedere dal rapporto in essere per giusta causa ovvero di risolvere il contratto per inadempimento dei soggetti poc'anzi indicati.

A tal fine, SIIT S.c.p.A. ha previsto l'inserimento di apposite clausole nei contratti con i medesimi che prevedano: (**a**) l'informativa ai Terzi dell'adozione del Modello e del Codice Comportamento da parte di SIIT S.c.p.A., di cui gli stessi dichiarano di aver preso visione, impegnandosi a rispettarne i contenuti e a non porre in essere comportamenti che possano determinare una violazione della legge, del Modello o la commissione di alcuno dei Reati Presupposto; (**b**) il diritto per la Società di recedere dal rapporto o risolvere il contratto (con o senza l'applicazione di penali), in caso di inottemperanza a tali obblighi.

PARTE SPECIALE

PRINCIPI DI CONTROLLO GENERALI E SPECIFICI PER LE AREE A RISCHIO

SIIT S.C.P.A.

INDICE

PREMESSA 4

LA STRUTTURA DELLA PARTE SPECIALE 4

1. Reati contro la pubblica amministrazione e/o in danno dell'unione europea (artt. 24-25 d.lgs. 231/01) 5
2. Delitti informatici e trattamento illecito di dati (art.24-bis d.lgs.231/01) 7
3. Delitti di criminalità organizzata, induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorita' giudiziaria e reati transnazionali (artt. 24-ter e 25-decies d.lgs. 231/01, l.146/2006) 9
4. Delitti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis d.lgs. 231/01) 10
5. Delitti contro l'industria ed il commercio (art. 25-bis 1 d.lgs. 231/01) 11
6. Reati societari (art. 25-ter d.lgs. 231/01) 12
7. Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater d.lgs. 231/01) 15
8. Delitti contro la personalità individuale (art.25-quinquies d.lgs. 231/01) 16
9. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (art. 25-septies d.lgs. 231/01) 17
10. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonche' autoriciclaggio (art. 25-octies d.lgs. 231/01) 30
11. Delitti in materia di violazione del diritto d'autore (art. 25-novies d.lgs. 231/01) 31
12. Impiego di cittadini di paesi terzi il cui soggiorno e' irregolare (art. 25-duodecies d.lgs. 231/01) 33
13. Reati tributari (art. 25-quinquiesdecies d.lgs. 231/01) 33
14. Contrabbando (art.25-sexiesdecies, d.lgs. 231/2001) 35

SEZIONE DI DETTAGLIO 37

LE AREE A RISCHIO-REATO 38

NORME DI COMPORTAMENTO PARTICOLARE NELLE SINGOLE AREE A RISCHIO-REATO 39

Area a rischio n. 1: Amministrazione, contabilità e bilancio 39
a) Attività Sensibili 39
b) Funzioni aziendali /unità organizzative e figure coinvolte 39
c) Fattispecie di reato potenzialmente applicabili 39
d) Controlli Preventivi 42
Area a rischio n. 2: Gestione delle attività di ricerca e sviluppo 45

a) Attività Sensibili 45
b) Funzioni aziendali /unità organizzative e figure coinvolte 45
c) Fattispecie di reato potenzialmente applicabili 45
d) Controlli Preventivi 46
AREA A RISCHIO N° 3 : AFFARI LEGALI E SOCIETARI 49
a) Attività Sensibili 49
b) Funzioni aziendali /unità organizzative e figure coinvolte 49
c) Fattispecie di reato potenzialmente applicabili 49
d) Controlli Preventivi 50
Area a rischio n. 4: Gestione delle risorse umane 51
a) Attività Sensibili 51
b) Funzioni aziendali /unità organizzative e figure coinvolte 51
c) Fattispecie di reato potenzialmente applicabili 52
d) Controlli Preventivi 53
Area a rischio n. 5: Gestione della salute e sicurezza sul lavoro 55
a) Attività Sensibili 55
b) Funzioni aziendali/unità organizzative e figure coinvolte 55
c) Fattispecie di reato potenzialmente applicabili 56
d) Controlli Preventivi 57
Area a rischio n. 6: Gestione degli acquisti 59
a) Attività Sensibili 59
b) Funzioni aziendali /unità organizzative e figure coinvolte 59
c) Fattispecie di reato potenzialmente applicabili 59
d) Controlli Preventivi 61

PREMESSA

LA STRUTTURA DELLA PARTE SPECIALE

SIIT S.c.p.A.(di seguito anche solo "**SIIT S.c.p.A.**" o "**la Società**" ha adottato una struttura del Modello che prevede, oltre alla Parte Generale, anche una Parte Speciale contenente una descrizione delle norme di comportamento generali implementate dalla Società per ogni categoria di Reato Presupposto, unitamente ad una sezione di dettaglio, strutturata per processo, contenente l'indicazione delle Aree a Rischio Reato individuate in relazione ai Reati Presupposto rilevanti e la descrizione dei controlli preventivi implementati al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/01 (in seguito anche il "**D.Lgs. 231/2001**" ovvero "**il Decreto**") ritenuti rilevanti per la Società (si veda *infra* "*Sezione di dettaglio*").

Le norme di comportamento generali implementate dalla Società devono essere osservate dai Destinatari del Modello in relazione ai Reati Presupposto rilevanti previsti dal Decreto 231 nei seguenti articoli:

- 24 e 25 (reati contro la Pubblica Amministrazione e/o in danno dell'Unione europea);
- 24-*bis* (delitti informatici);
- 24-*ter* (delitti di criminalità organizzata, avendo riguardo anche alla criminalità internazionale ai sensi della L. 146/06);
- 25-*bis* (falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, limitatamente alle fattispecie di cui agli artt. 473 e 474 c.p.) e 25-*bis*.1 (delitti contro l'industria e il commercio);
- 25-*ter* (reati societari);
- 25-*quater* (delitti con finalità di terrorismo o di eversione dell'ordine democratico);
- 25-*quinquies* (delitti contro la personalità individuale, limitatamente alla fattispecie di cui all'art. 603-*bis* c.p.);
- 25-*septies* (omicidio colposo o lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro);
- 25-*octies* (reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio);
- 25-*novies* (delitti in violazione del diritto d'autore);
- 25-*decies* (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria);
- 25-*duodecies* (impiego di cittadini di Paesi terzi il cui soggiorno è irregolare);
- 25-*quinquiesdecies* (reati tributari);
- 25-*sexiesdecies* (contrabbando).

1. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E/O IN DANNO DELL'UNIONE EUROPEA (ARTT. 24-25 D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Reati contro la Pubblica Amministrazione ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e di Condotta e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;
b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A tal proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

1) tenere rapporti con la Pubblica Amministrazione, nonché Istituzioni, Organismi/Uffici dell'Unione Europea, se non da parte dei soggetti a ciò deputati secondo i mansionari della società o eventuali deleghe o procure opportunamente conferite;
2) porre in essere qualsiasi situazione di conflitto di interesse nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle ipotesi di reato ai sensi degli articoli 24 e 25 del D.Lgs. n. 231 del 2001;
3) accordare o corrispondere somme di denaro o altra utilità in favore di pubblici ufficiali o incaricati di pubblico servizio, o a loro parenti, appartenenti alla Pubblica Amministrazione, agli Enti Pubblici e/o ai soggetti ad essi assimilati dello Stato italiano, dell'Unione Europea e di altri Organismi comunitari, nonché degli Stati esteri, salvo che si tratti di doni o utilità d'uso di modico valore e/o che abbiano un valore simbolico e/o che rientrino nella normale cortesia d'affari;
4) sottostare alla illecita richiesta del pubblico ufficiale o dell'incaricato di pubblico servizio che, con abuso della sua qualità e dei suoi poteri, induce taluno (il soggetto che opera in SIIT S.c.p.A.) a dare o promettere indebitamente a sé o ad altri a lui vicini, denaro o altra utilità;

5) fare promesse di qualsivoglia genere e specie (assunzione, *stage*, etc.) o accordare vantaggi di qualsiasi natura a favore di pubblici ufficiali e/o incaricati di un pubblico servizio appartenenti alla Pubblica Amministrazione, agli Enti Pubblici e/o ai soggetti ad essi assimilati dello Stato Italiano, dell'Unione Europea e di altri Organismi comunitari, nonché degli Stati esteri, o comunque a beneficio di altri individui o entità giuridiche comunque riconducibili alla sfera di interesse dei soggetti sopra indicati;
6) effettuare prestazioni in favore di terzi in genere non direttamente correlate e corrispondenti a quanto contrattualmente pattuito con tali soggetti;
7) accordare e corrispondere agli assegnatari di incarichi di natura professionale somme non adeguatamente proporzionate all'attività svolta, anche in considerazione delle condizioni di mercato;
8) effettuare pagamenti a soggetti diversi dalla controparte contrattuale;
9) in occasione di una trattativa d'affari, richiesta o rapporto con la Pubblica Amministrazione nonché Istituzioni, Organismi/Uffici dell'Unione Europea, influenzare impropriamente le decisioni della controparte, comprese quelle dei funzionari che trattano o prendono decisioni per conto della Pubblica Amministrazione, nonché Istituzioni, Organismi/Uffici dell'Unione Europea e/o assecondare condizionamenti e pressioni volti a determinare decisioni di SIIT S.c.p.A. non in linea con i dettami dello Statuto, delle disposizioni normative interne, del Codice Comportamento e del presente Modello;
10) farsi rappresentare, nei rapporti con la Pubblica Amministrazione nonché Istituzioni, Organismi/Uffici dell'Unione Europea, da un consulente o da altro soggetto terzo non adeguatamente e formalmente autorizzato, ed in ogni caso nell'ipotesi in cui si possano creare situazioni di conflitti di interesse;
11) fornire, redigere o consegnare ai pubblici ufficiali e/o agli incaricati di un pubblico servizio appartenenti alla Pubblica Amministrazione, agli Enti Pubblici e/o ai soggetti ad essi assimilati dello Stato Italiano, dell'Unione Europea (o altri Organismi comunitari) e degli Stati esteri dichiarazioni, dati o documenti in genere aventi contenuti inesatti, errati, incompleti, lacunosi e/o falsi, al fine di ottenere certificazioni, permessi, autorizzazioni e/o licenze di qualsivoglia genere o specie, o conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
12) fornire, redigere, esibire o consegnare ai pubblici ufficiali o incaricati di pubblico servizio (nazionali, comunitari o esteri) dichiarazioni, dati, informazioni o documenti in genere aventi contenuti volutamente artefatti, inesatti, errati, incompleti, lacunosi e/o falsi, nell'ambito di qualsivoglia attività di natura imprenditoriale svolta dalla Società.

A tal fine è necessario:

- effettuare dichiarazioni a organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, contenenti solo elementi autentici e accurati;
- adottare un comportamento improntato ai principi di integrità, onestà, trasparenza e buona fede in relazione a qualsiasi attività da intraprendersi nell'ambito di ogni attività aziendale;
- garantire il rispetto dei principi di correttezza, trasparenza e buona fede in qualsiasi rapporto professionale che si intraprenda con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- effettuare dichiarazioni a organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, contenenti solo elementi autentici e accurati;
- definire per iscritto qualsiasi tipo di accordo con consulenti e collaboratori in modo da rendere evidenti i termini dell'accordo stesso – con particolare riguardo alla tipologia di incarico/transazione e alle condizioni economiche sottostanti.

2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART.24-BIS D.LGS.231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti informatici e trattamento illecito di dati individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;
b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A questo proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

1) introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;

2) accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati di SIIT S.c.p.A., o a parti di esse, non possedendo le credenziali di accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;
3) distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di pubblica utilità;
4) introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
5) alterare, mediante l'utilizzo di firma elettronica o comunque in qualsiasi modo, documenti informatici;
6) produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o alterati;
7) intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
8) utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio, *virus, worm, trojan, spyware, dialer, keylogger, rootkit*) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
9) detenere, procurarsi, riprodurre e/o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
10) procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
11) rimuovere il software antivirus installato sugli strumenti informatici in dotazione agli utenti.

Le funzioni/unità organizzative aziendali e, in particolare, coloro i quali rivestono posizioni rilevanti nell'utilizzo e nell'amministrazione dei sistemi informatici, devono ispirare la loro azione ai seguenti principi generali:

- *Riservatezza* - garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- *Integrità* - garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- *Disponibilità* - garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

3. DELITTI DI CRIMINALITÀ ORGANIZZATA, INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA E REATI TRANSNAZIONALI (ARTT. 24-TER E 25-DECIES D.LGS. 231/01, L.146/2006)

Nell'espletamento delle proprie funzioni, oltre alle regole di cui al presente Modello, i Destinatari devono, in generale, conoscere e rispettare le norme inerenti la prevenzione dei reati in oggetto.

In particolare, ai Destinatari è fatto espresso divieto di:

1) porre in essere, collaborare o dare causa alla realizzazione di comportamenti, considerati individualmente o collettivamente, tali da integrare, in maniera diretta o indiretta, le fattispecie di reato previste dagli articoli oggetto di analisi;
2) utilizzare, anche occasionalmente, SIIT S.c.p.A. o una sua unità organizzativa allo scopo di consentire o agevolare la commissione di uno o più dei reati oggetto di analisi nella presente Sezione;
3) porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo;
4) effettuare prestazioni in favore di terzi che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
5) riconoscere compensi in favore di terzi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
6) ricevere compensi per forniture o prestazioni inesistenti o che esulano dalla ordinaria attività d'impresa;
7) fornire, direttamente o indirettamente, fondi a favore di soggetti che perseguono, direttamente o in qualità di prestanome, finalità di criminalità organizzata (anche transnazionale), agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche;
8) usare violenza o minaccia nei confronti di un soggetto chiamato a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale affinché lo stesso soggetto non renda dichiarazioni o renda dichiarazioni mendaci;
9) promettere di offrire denaro o altra utilità ad un soggetto chiamato a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale affinché lo stesso soggetto non renda dichiarazioni o renda dichiarazioni mendaci;

10) influire in qualsiasi modo sulla volontà di rispondere di soggetti chiamati a rendere dichiarazioni innanzi l'Autorità Giudiziaria determinandoli a rendere dichiarazioni mendaci ovvero inducendoli ad avvalersi della facoltà di non rispondere

Alla luce di quanto sopra, al fine di prevenire la commissione dei reati previsti all'art. 24-*ter* del D.Lgs. n. 231 del 2001e ritenuti rilevanti per SIIT S.c.p.A., quest'ultima adotta norme di comportamento improntate a:

1) verificare che qualunque transazione finanziaria presupponga la previa conoscenza del beneficiario, quantomeno diretto, della relativa somma di denaro;
2) verificare l'attendibilità commerciale e professionale dei fornitori ed eventuali *partner* commerciali/finanziari;
3) verificare che i dati raccolti relativamente ai rapporti con terzi siano completi ed aggiornati sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del profilo;
4) verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari ed ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
5) adottare adeguati programmi di formazione del personale.

Tutte le funzioni/unità organizzative aziendali interessate dalle attività potenzialmente rilevanti per i reati di cui alla presente sezione dovranno riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

4. DELITTI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (ART. 25-BIS D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti di falsità in monete individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;

b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A questo proposito, a titolo meramente esemplificativo e non esaustivo, ai Destinatari del Modello è fatto divieto in particolare di:

1) porre in essere qualsiasi operazione o attività che possa configurarsi come reato di falsità in monete, carte di pubblico credito, valori di bollo e in strumenti o segni di riconoscimento;
2) manipolare, alterandoli, monete, carte di pubblico credito e valori di bollo;
3) introdurre nello Stato e utilizzare, nelle operazioni di incasso e pagamento, denaro contante e carte di pubblico credito contraffatti e/o alterati;
4) acquistare e/o utilizzare valori di bollo contraffatti e/o alterati.

5. DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO (ART. 25-BIS 1 D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti di falsità in strumenti o segni di riconoscimento e contro l'industria ed il commercio individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;
b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A questo proposito, a titolo meramente esemplificativo e non esaustivo, ai Destinatari del Modello è fatto divieto in particolare di:

1) compiere atti di concorrenza con violenza o minaccia nei confronti di società concorrenti;
2) consegnare all'acquirente finale un prodotto diverso per origine, provenienza, qualità o quantità rispetto a quello concordato;

3) mettere in vendita o comunque contribuire a mettere in commercio prodotti industriali con nomi, marchi o segni distintivi atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dei prodotti medesimi;
4) contribuire a fabbricare o adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale in titolarità di terzi;
5) introdurre nel territorio dello Stato, detenere per la vendita e mettere comunque in circolazione beni realizzati usurpando un titolo di proprietà industriale in titolarità di terzi;
6) introdurre nel territorio dello Stato, detenere per la vendita e mettere comunque in circolazione prodotti con le indicazioni geografiche contraffatte.

È fatto altresì obbligo di:

1) svolgere con la massima diligenza e accuratezza tutte le necessarie ricerche di anteriorità relative al marchio, brevetto, segno distintivo, disegno o modello che intendono utilizzare e/o mettere in commercio, al fine di verificare la sussistenza di eventuali diritti di privativa di terzi;
2) ottenere dai rispettivi titolari e/o licenzianti dei relativi diritti di utilizzo sui marchi, brevetti, segni distintivi, disegni o modelli in questione, specifiche dichiarazioni volte ad attestare le seguenti principali circostanze:
   (a) essere i legittimi titolari dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
   (b) garantire che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o di concessione in uso non violino alcun diritto di proprietà industriale in capo a terzi;
   (c) impegnarsi a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio di natura patrimoniale e non, le potesse derivare, per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.
3) verificare la conformità della merce eventualmente consegnata al cliente rispetto a quanto concordato con lo stesso.

6. REATI SOCIETARI (ART. 25-TER D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Reati Societari individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;

b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A tal proposito, a titolo meramente esemplificativo e non esaustivo, i Destinatari del Modello, sono tenuti, in particolare, a:

1) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione, assicurando un pieno rispetto delle norme di legge e regolamentari, nello svolgimento di tutte le attività finalizzate all'acquisizione, elaborazione, gestione e comunicazione dei dati e delle informazioni destinate a consentire un fondato giudizio sulla situazione patrimoniale, economica e finanziaria di SIIT S.c.p.A.

   A questo proposito, ai Destinatari è fatto divieto in particolare di:
   - fornire, redigere o trasmettere dati o documenti inesatti, errati, incompleti, lacunosi e/o non rispondenti alla realtà, tali da configurare una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;
   - alterare o, comunque, riportare in modo non corretto i dati e le informazioni destinati alla predisposizione e stesura dei documenti societari di natura patrimoniale, economica e finanziaria;
   - illustrare dati ed informazioni in modo tale da fornire una rappresentazione non corretta e veritiera sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione delle relative attività;
2) osservare rigorosamente tutte le norme poste a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere.

   A questo proposito, ai Destinatari è fatto divieto in particolare di:
   - restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
   - ripartire utili o acconti su utili non effettivamente conseguiti o da destinare per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
   - effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;

3) mettere a disposizione dei soci e degli altri organi sociali tutta la documentazione sulla gestione di SIIT S.c.p.A. necessaria ad effettuare le attività di controllo legalmente attribuite agli stessi.

   A questo proposito, ai Destinatari è fatto particolare divieto di:

   - porre in essere comportamenti che impediscano materialmente, o comunque ostacolino, lo svolgimento dell'attività di controllo da parte dei soci e degli altri organi di controllo, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti;

4) garantire il regolare funzionamento ed andamento della Società e degli organi sociali, agevolando ed assicurando tutte le forme di controllo interno sulla gestione sociale previste dalla legge nonché favorendo la libera formazione ed assunzione delle decisioni della Società.

   A questo proposito, ai Destinatari è fatto particolare divieto di:

   - tenere condotte che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte degli Organi deputati al controllo e dei soci;
   - porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

5) mettere a disposizione dei soggetti che svolgono le attività di controllo contabile i documenti sulla gestione della Società, onde consentire a tali organismi di espletare le necessarie verifiche;

6) rispettare ed osservare rigorosamente tutte le previsioni di legge a tutela dell'integrità e dell'effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

7) attenersi alle precise regole di comportamento indicate nelle procedure di riferimento nella conclusione di contratti con altre società private astenendosi dal dare o promettere denaro o altra utilità per sé o per altri, così da non indurre gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili, i sindaci e i liquidatori ovvero i soggetti sottoposti alla direzione o alla vigilanza di uno di essi a violare gli obblighi inerenti il loro ufficio ovvero gli obblighi di fedeltà, con conseguente nocumento per la società per cui prestano attività lavorativa.

   In ordine a tale punto, è fatto espresso divieto a coloro che rappresentano la Società nel corso di trattative con aziende private, di dare o promettere denaro o altra utilità direttamente ai soggetti che rappresentano la controparte contrattuale ovvero - per loro tramite - ad altri soggetti, al fine di far loro violare gli obblighi inerenti l'ufficio da loro ricoperto ovvero i più generali obblighi di fedeltà rispetto

all'organizzazione da loro rappresentata, determinandoli a concludere contratti ovvero ad assumere iniziative che cagionino nocumento all'organizzazione per la quale lavorano.

7. DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (ART. 25-QUATER D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti con Finalità di Terrorismo o di Eversione dell'Ordine Democratico individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari del presente Modello sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare, considerati individualmente o collettivamente, in maniera diretta o indiretta, le fattispecie di reato previste dall'art. 25-*quater* del Decreto;
- astenersi dall'utilizzare, anche occasionalmente, SIIT S.c.p.A. o una sua Funzione Aziendale allo scopo di consentire o agevolare la commissione di uno o più Delitti con Finalità di Terrorismo o di Eversione dell'Ordine Democratico;
- astenersi dal fornire, direttamente o indirettamente, fondi a favore di soggetti che intendono porre in essere uno o più Delitti con Finalità di Terrorismo o di Eversione dell'Ordine Democratico ovvero a favore di soggetti che perseguono, direttamente o in qualità di prestanome, finalità di terrorismo o eversione dell'ordine democratico, agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche. Vengono in considerazione i fondi e le risorse economiche erogate a favore di un soggetto o di un gruppo nella consapevolezza - o quantomeno con il ragionevole sospetto - che:
  - questo persegua finalità di terrorismo o eversione dell'ordine democratico;
  - il beneficiario dei fondi li destinerà a tali gruppi;
  - le risorse finanziarie saranno utilizzate per commettere attentati alla sicurezza dei trasporti e degli aeroporti, alla vita e all'incolumità di agenti diplomatici, sequestri di persona e/o circolazione di armi, anche nucleari;
- astenersi dall'effettuare prestazioni in favore di terzi che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- astenersi dal riconoscere compensi in favore di terzi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;

- astenersi dall'erogare liberalità a favore di enti e soggetti inseriti nelle Liste ONU e/o in tutte le Liste di riferimento in tema di prevenzione al terrorismo di qualsiasi matrice.

Alla luce di quanto sopra, al fine di prevenire la commissione dei reati previsti all'art. 25-*quater* del D.Lgs. n. 231 del 2001, la Società adotta norme di comportamento improntate a:

- verificare che qualunque transazione finanziaria presupponga la previa conoscenza del beneficiario, quantomeno diretto, della relativa somma di denaro;
- verificare l'attendibilità commerciale e professionale dei fornitori e di eventuali *partner* commerciali/finanziari;
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- espletare i controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti derivanti da operazioni infragruppo.
- adottare adeguati programmi di formazione del Personale.

Ferma restando la necessità di porre in essere le condotte di carattere generale sopra indicate con specifico riferimento ai Delitti con Finalità di Terrorismo o di Eversione dell'Ordine Democratico rilevanti per SIIT S.c.p.A. e individuati, la Società ha adottato e attuato specifiche Procedure applicabili anche alle fattispecie di reato di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

È fatto, infine, obbligo a tutti i Destinatari (come individuati nella Parte Generale del presente Modello) di riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità che dovessero emergere rispetto alla presente sezione.

8. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (ART.25-QUINQUIES D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti contro la personalità individuale, in particolar modo l'intermediazione illecita e sfruttamento del lavoro, i Destinatari sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;

b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A questo proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

1. gestire le risorse umane in violazione delle vigenti disposizioni in materia di diritto del lavoro (con particolare attenzione alle condizioni igienico-sanitarie, alla sicurezza, ai diritti sindacali, di associazione e rappresentanza, ai diritti dei minori e delle donne);
2. istituire rapporti contrattuali (connessi all'assunzione di incarichi o all'acquisto di beni e servizi, etc.) nei confronti di soggetti che non rispettino la normativa vigente in materia di lavoro, con particolare attenzione al lavoro minorile e a quanto disposto in tema di salute e sicurezza;
3. fornire, direttamente o indirettamente, fondi a favore di soggetti che intendono porre in essere uno o più reati contemplati all'interno dell'art. 25 *quinquies* ovvero a favore di soggetti che perseguono, direttamente o in qualità di prestanome, tali finalità, agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche;
4. effettuare prestazioni in favore di terzi che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
5. riconoscere compensi in favore di terzi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.

In aggiunta a quanto sopra previsto, è necessario precisare che:

a) qualunque transazione finanziaria deve presupporre la conoscenza del soggetto beneficiario, quantomeno diretto, della relativa somma di denaro;
b) le transazioni di rilevante valore devono essere concluse con le persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli ed accertamenti (es. referenze personali, etc.);
c) i dati raccolti relativamente ai rapporti con i clienti, i consulenti e i partner commerciali devono essere completi ed aggiornati sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del profilo.

9. OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E DELLA SICUREZZA SUL LAVORO (ART. 25-SEPTIES D.LGS. 231/01)

Premessa

All'esito di una concreta valutazione del "rischio-reato" presente all'interno di SIIT S.c.p.A., fatta alla luce ed in considerazione dei cosiddetti "reati presupposto" specificamente previsti dal D.Lgs. 8 giugno 2001, n. 231, sono state considerate concretamente rilevanti per la Società le fattispecie di reato previste dall'art. 25-septies del Decreto ovvero i reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (articolo 9 della legge 3 agosto 2007, n. 123) ed in particolare:

- **l'omicidio colposo** (art. 589, comma 2, c.p.);
- le **lesioni personali colpose gravi o gravissime** (art. 590, comma 3, c.p.)

Sono stati - quindi - stabiliti i protocolli cautelari, ovvero i comportamenti, le procedure e le istruzioni da osservare (standard di controllo) al fine di prevenire la commissione dei reati qui richiamati, in modo tale da assicurare un sistema aziendale in grado di garantire l'adempimento di tutti gli obblighi giuridici specificamente richiamati dall'art. 30 del D.Lgs. 9 aprile 2008, n. 81 (in seguito anche il "*D. Lgs. 81/2008*" ovvero il "*Testo Unico in materia di salute e sicurezza sul lavoro*").

Fattispecie

L'art. 9 della Legge 3 agosto 2007 n. 123, così come sostituito dall'art. 300 del D.Lgs. 81/2008, ha esteso l'ambito applicativo della responsabilità da reato degli enti ai delitti "*di cui agli articoli 589 e 590, terzo comma, c.p. commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*".

Con riferimento all'ipotesi di **omicidio colposo aggravato** si distingue:

1. ***oggetto giuridico***: la norma tutela la vita umana sanzionando i comportamenti che provochino la morte per colpa del reo con condotte che violino l'incolumità del lavoratore;
2. ***soggetto attivo***: il soggetto attivo del reato può essere "chiunque". Tuttavia il rimprovero per non aver tenuto quella condotta supposta come causa dell'evento è mosso a colui o coloro che, sulla base dell'accertato ruolo nell'organizzazione del luogo di lavoro interessato all'evento, si ritiene avrebbero dovuto adottare quella data misura protettiva o imporre l'osservanza di quella determinata misura, tanto per citare - in via esemplificativa - alcune delle omissioni più frequentemente indicate come causa degli eventi antinfortunistici. Quindi, il "chiunque" si trasforma di volta in volta in questo o quel soggetto, la cui posizione in quel determinato luogo di lavoro lo colloca tra quelle figure alle quali le fonti normative prevenzionali assegnano una funzione - con i correlati obblighi - di scelta, programmazione, attuazione, controllo delle diverse misure prevenzionali, legislativamente predefinite e presuntivamente ritenute idonee a prevenire l'evento infortunistico in questa o quella delle attività lavorative. La Società, al fine di rendere concretamente applicabili le regole prevenzionali, ha individuato,

all'interno della propria organizzazione imprenditoriale, i diversi ruoli e la ripartizione organizzativa degli stessi: solo così le "posizioni di garanzia" sono nelle condizioni di adempiere agli obblighi che tale posizione aggrega a sé, e la funzione di tutela dei terzi è sostanziale e non già un mero "parametro" di valutazione dell'eventuale responsabilità;

3. ***causalità***: ai sensi dell'art. 40, comma 1, del c.p. "*nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipendente l'esistenza del reato, non è conseguenza della sua azione od omissione*". Per poter stabilire, poi, che un determinato evento è conseguenza di una azione od omissione si deve ricorrere alla cosiddetta "condicio sine qua non", per cui, se si elimina la detta azione od omissione, viene meno anche l'evento. Ovviamente per poter affermare che una azione (od omissione) costituisce condizione necessaria di un evento bisogna ricorrere a nozioni scientifiche o anche statistiche che dimostrino che v'è consequenzialità tra quella condotta e quell'evento. Poiché è impossibile conoscere tutti gli aspetti dei fatti e tutti i profili della situazione storica, il giudizio sul nesso di causalità è, in fondo, un giudizio di "alta probabilità" o di probabilità logica o razionale credibilità circa la consequenzialità di un evento ad una condotta. In caso di omicidio colposo, il rapporto di causalità tra la condotta dell'imputato e l'evento non resta escluso per il solo fatto che tale condotta non sarebbe stata idonea a produrre l'evento stesso senza il concorso della condotta antigiuridica altrui, non essendo sufficiente un semplice concorso di colpa del lavoratore, ma occorrendo una di lui condotta dolosa ovvero la presenza di un rischio elettivo generato da un'attività non avente rapporto con lo svolgimento del lavoro o esorbitante dai limiti di esso;
4. ***elemento soggettivo***: il soggetto attivo del reato deve aver realizzato involontariamente, cioè per colpa, la morte del lavoratore. Il soggetto attivo versa in colpa quando la sua condotta violi le regole cautelari cioè le regole che impongono comportamenti, non realizzando i quali non è prevedibile che si realizzi l'evento dannoso, mentre, realizzandoli, tale evento è prevedibile ed evitabile. La condotta colposa può essere violatrice o di norme generiche e di prudenza, diligenza e perizia ovvero di norme specifiche (ad esempio quelle contenute nel D.Lgs. 81/2008) che impongono di agire o non agire. Queste norme specifiche sono fondate sulla conoscenza che certe azioni o certe omissioni possono determinare pericolo di danni ai beni protetti, come la vita dei lavoratori. Mentre i comportamenti doverosi sono valutati sulla base della migliore scienza per essere adeguati al progresso tecnologico (art. 18, comma 1° lett. z) del D.Lgs. 81/2008), la prevedibilità dell'evento o, per converso, la sua evitabilità vanno valutate tenendo presente il modello di "agente" formato per quella stessa condizione o professione del caso di specie. Le norme cautelari scritte non esauriscono tutta la prudenza, diligenza o perizia necessarie, cosicché il giudizio

negativo circa l'atteggiamento psicologico del soggetto agente può trovare fondamento, appunto, in valutazioni generiche del dovere di sicurezza; può infatti sussistere la colpa del soggetto attivo sulla base delle comuni nozioni generali di prudenza, diligenza e perizia.

Con riferimento invece alle ipotesi **di lesioni gravi o gravissime aggravate** si distingue:

1. ***oggetto giuridico:*** la norma tutela l'integrità fisica e fisico-psichica della persona, sanzionando i comportamenti che provochino una malattia penalmente rilevante. La lesione personale è grave:
- se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o una 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.

La lesione personale è 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;

2. ***soggetto attivo***: si tratta di un reato che può essere commesso da "*chiunque*"; per la particolare posizione dei soggetti investiti degli "*obblighi di garanzia*" in materia antinfortunistica vedi sub 2) del reato di omicidio colposo;
3. ***causalità***: nessuna peculiarità presenta la causalità rispetto a quella relativa al reato di omicidio colposo aggravato;
4. ***elemento soggettivo***: anche in questo caso nessuna peculiarità rispetto a quanto già descritto nel reato di omicidio colposo aggravato.

L'assetto organizzativo di SIIT S.c.p.A.

All'interno della Società la ripartizione delle funzioni, dei poteri e dei correlativi doveri in materia di salute e sicurezza sul lavoro (in seguito anche "*SSL*") è espressione di precise scelte organizzative, che hanno portato la Società ad individuare, all'interno del proprio assetto societario la persona che, in concreto, riveste la qualifica di "*datore di lavoro*" in materia di salute e sicurezza nei luoghi di lavoro, alla luce della definizione che ne viene data dall'art. 2, comma 1°, lett. b) del D.Lgs. 81/2008 e dei poteri allo stesso attribuiti.
Tenuto conto, poi, della natura, delle dimensioni della propria organizzazione e del tipo di attività svolta, SIIT S.c.p.A. ha previsto un'articolazione di funzioni in grado di assicurare le competenze tecniche ed i poteri necessari per la verifica, valutazione,

gestione e controllo del rischio, definendo formalmente - in coerenza con lo schema organizzativo e funzionale dell'azienda - le figure specifiche operanti in tale ambito (Responsabile del Servizio di Prevenzione e Protezione, Medico Competente, Rappresentante dei lavoratori per la salute, la sicurezza e l'Ambiente, ecc.).
In questo modo, la Società ha previsto una propria articolazione di funzioni atta ad assicurare la salvaguardia degli interessi protetti per il tramite della cooperazione di più soggetti che - sulla base della valorizzazione delle necessarie competenze differenziate - si dividono il lavoro ripartendosi i compiti, ai sensi di quanto puntualmente richiesto dal comma 3 dell'art. 30 del D.Lgs. 81/2008 in materia di salute e sicurezza sul lavoro.

Il sistema di gestione delle tematiche SSL istituito dalla Società ha l'intento di:

- garantire un ambiente di lavoro sicuro per i lavoratori che operano all'interno dell'azienda, tale da prevenire infortuni, malattie professionali e rischi per la Salute e la Sicurezza degli stessi;
- prevenire l'accadimento di incidenti rilevanti, con potenziali conseguenze all'interno ed all'esterno del sito produttivo;
- stabilire obiettivi di miglioramento continuo;
- tenere sotto controllo i processi e le attività dell'organizzazione che possono generare impatti sulla Salute e Sicurezza dei lavoratori;
- applicare, mantenere attive e migliorare le proprie prestazioni per la Salute e Sicurezza dei lavoratori;
- garantire da parte della Società la conformità alle prescrizioni legislative poste a tutela della Salute e Sicurezza sul lavoro, prevenendo – quindi – la tenuta di condotte colpose che possono essere la causa di eventi infortunistici, di malattie professionali o, ancora, di incidenti rilevanti;
- garantire un sistema organizzativo, gestionale e di controllo che costituisca un valido strumento per prevenire la commissione di possibili reati antinfortunistici a carico della Società *ex* art. 25-*septies* del D.Lgs. 231/2001.

Tutta l'azienda, sia ai livelli apicali che a quelli operativi, deve attenersi a questi principi, in particolare quando devono essere prese delle decisioni o fatte delle scelte e, in seguito, quando le stesse devono essere attuate.
La sicurezza nell'ambiente di lavoro si consegue – infatti - con la partecipazione attiva di tutti coloro che operano all'interno della Società i quali devono tenere, nella loro attività quotidiana, comportamenti che siano conformi alla legge e ai protocolli cautelari di cui al sistema di gestione delle tematiche SSL di SIIT S.c.p.A.
Come espressamente previsto dal comma 5 dell'art. 30 del D.Lgs. 81/2008, il Modello di organizzazione, gestione e controllo adottato da SIIT S.c.p.A. ed il suo sistema di gestione delle tematiche SSL si presumono conformi, per le parti corrispondenti, a quelli che sono i requisiti richiesti dall'articolo 30 sopra richiamato per l'adozione di un Modello di

organizzazione e gestione che sia idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche per i reati presupposto di cui all'art. 25-*septies* del D.Lgs. 231/2001.

Di seguito vengono riportati i principi di comportamento che si richiede vengano adottati da parte di tutto il personale nello svolgimento di tutte le attività aziendali. Tali regole di condotta sono finalizzate a limitare il più possibile il verificarsi dei reati previsti nel Decreto.
I principi di comportamento si applicano direttamente a chiunque sia tenuto, in via diretta od indiretta, all'osservanza delle norme antinfortunistiche. La normativa vigente individua i seguenti soggetti quali garanti *ex lege*, per quanto di rispettiva competenza, dell'obbligo di sicurezza: Datore di Lavoro, dirigenti, preposti, lavoratori.

In particolare, non sono delegabili da parte del Datore di Lavoro i seguenti obblighi previsti *ex* art. 17 del D.Lgs. 81/2008 (TUS):

a) la valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'art. 29, TUS;
b) la designazione del Responsabile del Servizio di Prevenzione e Protezione.

Fatta eccezione per quanto stabilito dall'art. 17, TUS attraverso lo strumento della delega di funzioni previsto dall'art. 16, TUS, il Datore di Lavoro può delegare, nel rispetto delle condizioni dettate dall'art.16[1], l'esecuzione degli obblighi di sicurezza a soggetti che siano dotati delle necessarie competenze. I soggetti delegati dal Datore di Lavoro possono

[1] Articolo 16, TUS, *Delega di funzioni*

1. La delega di funzioni da parte del Datore di Lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni:
   a) che essa risulti da atto scritto recante data certa;
   b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
   c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
   d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
   e) che la delega sia accettata dal delegato per iscritto.
2. La delega di funzioni di cui al comma 1 deve essere data adeguata e tempestiva pubblicità.
3. La delega di funzioni non esclude l'obbligo di vigilanza in capo al Datore di Lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. L'obbligo di cui al precedente periodo si intende assolto in caso di adozione ed efficace attuazione del modello di verifica di cui all'articolo 30, comma 4.

3-*bis* Il soggetto delegato può, a sua volta, previa intesa con il Datore di Lavoro delegare specifiche funzioni in materia di salute e sicurezza sul lavoro alle condizioni di cui ai commi 1 e 2. La delega di funzioni di cui al periodo precedente non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale sia stata conferita la delega di cui al presente comma non può, a sua volta, delegare le funzioni delegate.

a loro volta subdelegare l'esecuzione degli obblighi di sicurezza nei limiti previsti dall'art. 16, comma 3-*bis*, TUS.

Il Datore di Lavoro e i dirigenti sono tenuti all'adempimento degli obblighi previsti dall'articolo 18[2], TUS, nel quadro della più ampia previsione dell'art. 2087 c.c.,

[2] Articolo 18, TUS *Obblighi del Datore di Lavoro e del dirigente*

1. Il Datore di Lavoro, che esercita le attività di cui all'articolo 3, e i dirigenti, che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono:
   a) nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal presente decreto legislativo.
   b) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;
   c) nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;
   d) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;
   e) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
   f) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;
   g) inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richieder al medico competente l'osservanza degli obblighi previsti a suo carico nel presente decreto;
   g-*bis*) nei casi di sorveglianza sanitaria di cui all'articolo 41, comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro;
   h) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
   i) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
   l) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37;
   m) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
   n) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;
   o) consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), anche su supporto informatico come previsto dall'articolo 53, comma 5, nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r). Il documento è consultato esclusivamente in azienda.
   p) elaborare il documento di cui all'articolo 26, comma 3, anche su supporto informatico come previsto dall'articolo 53, comma 5, e, , su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza. Il documento è consultato esclusivamente in azienda.;
   q) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;
   r) comunicare in via telematica all'INAIL, o all'IPSEMA, nonché per il loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del

qualificata quale norma di chiusura del sistema con riferimento alla portata degli obblighi di sicurezza posti *ex lege* in capo al Datore di Lavoro.

---

certificato medico, ai fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza al lavoro superiore a tre giorni. L'obbligo di comunicazione degli infortuni che comportino un'assenza dal lavoro superiore a tre giorni si considera comunque assolto per mezzo della denuncia di cui all'articolo 53 del decreto del Presidente della Repubblica 30 giugno 1965, n. 1124;

s) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50;
t) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;
u) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del Datore di Lavoro;
v) nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'articolo 35;
z) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
aa) comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza; in fase di prima applicazione l'obbligo di cui alla presente lettera riguarda i nominativi dei rappresentanti dei lavoratori per la sicurezza già eletti o designati;
bb) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità;

1-*bis* L'obbligo di cui alla lettera r) del comma 1, relativo alla comunicazione a fini statistici e informativi dei dati relativi agli infortuni che comportano l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento, escluso quello dell'evento, decorre dalla scadenza del termine di sei mesi dall'adozione del decreto interministeriale di cui all'articolo 8, comma 4.

2. Il Datore di Lavoro fornisce al servizio di prevenzione e protezione ed al medico competente informazioni in merito a:
   a) la natura dei rischi;
   b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;
   c) la descrizione degli impianti e dei processi produttivi;
   d) i dati di cui al comma 1, lettera r), e quelli relativi alle malattie professionali;
   e) i provvedimenti adottati dagli organi di vigilanza.
3. Gli obblighi relativi agli interventi strutturali e di manutenzione necessari per assicurare, ai sensi del presente decreto legislativo, la sicurezza dei locali e degli edifici assegnati in uso a pubbliche amministrazioni o a pubblici uffici, ivi comprese le istituzioni scolastiche ed educative, restano a carico dell'amministrazione tenuta, per effetto di norme o convenzioni, alla loro fornitura e manutenzione. In tale caso gli obblighi previsti dal presente decreto legislativo, relativamente ai predetti interventi, si intendono assolti, da parte dei dirigenti o funzionari preposti agli uffici interessati, con la richiesta del loro adempimento all'amministrazione competente o al soggetto che ne ha l'obbligo giuridico.

3-*bis* Il Datore di Lavoro e i dirigenti sono tenuti altresì a vigilare in ordine all'adempimento degli obblighi di cui agli articoli 19, 20, 22, 23, 24 e 25 del presente decreto, ferma restando l'esclusiva responsabilità dei soggetti obbligati ai sensi dei medesimi articoli qualora la mancata attuazione dei predetti obblighi sia addebitabile unicamente agli stessi e non sia riscontrabile un difetto di vigilanza del Datore di Lavoro e dei dirigenti.

In particolare, il Datore di Lavoro e i dirigenti sono tenuti a vigilare sull'adempimento degli obblighi di sicurezza posti dalla normativa in capo a preposti, lavoratori, progettisti, fabbricanti, fornitori, installatori e medici competenti.
Gli obblighi di sicurezza posti dalla normativa vigente in capo a preposti e lavoratori sono compiutamente disciplinati rispettivamente dagli articoli 19[3] e 20[4] TUS.

[3] Articolo 19, TUS *Obblighi del preposto*

1. In riferimento alle attività indicate all'articolo 3, i preposti, secondo le loro attribuzioni e competenze, devono:
   a) sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di persistenza della inosservanza, informare i loro superiori diretti;
   b) verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
   c) richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
   d) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
   e) astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;
   f) segnalare tempestivamente al Datore di Lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
   g) frequentare appositi corsi di formazione secondo quanto previsto dall'articolo 37.

[4] Articolo 20, TUS *Obblighi dei lavoratori*

1. Ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal Datore di Lavoro.
2. I lavoratori devono in particolare:
   a) contribuire, insieme al Datore di Lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
   b) osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
   c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza;
   d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
   e) segnalare immediatamente al Datore di Lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché' qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
   f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
   g) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
   h) partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
   i) sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.
3. I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del Datore di Lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi.

In base al disposto dell'articolo 31, TUS il Datore di Lavoro organizza il servizio di prevenzione e protezione all'interno dell'azienda o dell'unità produttiva, o incarica persone o servizi esterni, in assenza di dipendenti che all'interno dell'azienda ovvero dell'unità produttiva, siano in possesso delle capacità e dei requisiti professionali di cui all'articolo 32, TUS.

PRINCIPI GENERALI

É fatto divieto, per tutti i Destinatari, di:

a) porre in essere comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, fattispecie di reato rientranti tra quelle sopra considerate (art. 25-*septies* del Decreto);
b) porre in essere comportamenti imprudenti, negligenti od imperiti che possano costituire un pericolo per la sicurezza all'interno dei luoghi di lavoro;
c) 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;
d) rifiutare di utilizzare dispositivi di protezione individuale o collettivi o svolgere attività lavorative in violazione delle disposizioni impartite dai responsabili per la sicurezza;
e) svolgere attività di lavoro e adoperare macchinari e strumentazioni senza aver preventivamente ricevuto adeguate istruzioni sulle modalità operative oppure senza aver precedentemente partecipato a corsi di formazione;
f) omettere la segnalazione della propria eventuale incapacità o inesperienza nell'uso di strumenti aziendali;
g) rifiutarsi di partecipare a corsi di formazione in materia di salute e sicurezza sul luogo di lavoro.

Sotto l'aspetto generale, nell'ambito dei suddetti comportamenti i soggetti aziendali preposti all'attuazione delle misure di sicurezza - ciascuno per le attività di sua competenza specificamente individuate - sono tenuti ad assicurare:

a) il rispetto degli *standard* tecnico-strutturali di legge relativi ad attrezzature, impianti e luoghi di lavoro;
b) l'attuazione delle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c) l'attuazione di modifiche di natura organizzativa finalizzate a far fronte a emergenze, primo soccorso, gestione degli appalti;
d) il corretto svolgimento delle riunioni periodiche di sicurezza e delle consultazioni dei rappresentanti dei lavoratori per la sicurezza;

e) le attività di sorveglianza sanitaria;
f) le attività di formazione e informazione del personale;
g) le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte del personale;
h) l'acquisizione della documentazione e delle certificazioni obbligatorie di legge;
i) le verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate.

Al fine di realizzare un sistema di gestione della sicurezza sul lavoro coerente, che integri al suo interno la tecnica, l'organizzazione e le condizioni del lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro, la Società provvede a predisporre:

1) idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui ai precedenti punti da a) ad i);
2) un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello, secondo i dettami stabiliti dalle normative vigenti;
3) un idoneo sistema di controllo sull'attuazione degli obiettivi prefissati in materia di sicurezza e del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Si prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni o omissioni, conformemente alla loro formazione ed alle istruzioni e ai mezzi forniti dal Datore di Lavoro ai fini sicurezza;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro ai fini sicurezza, dai dirigenti e dai soggetti preposti alla sicurezza ai fini della protezione collettiva ed individuale;
- utilizzare correttamente i macchinari e le apparecchiature, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a disposizione;
- segnalare immediatamente al Datore di Lavoro ai fini sicurezza, al Servizio di Prevenzione e Protezione ed agli altri soggetti coinvolti nel sistema di gestione della sicurezza le deficienze dei mezzi e dispositivi di cui ai punti che precedono, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi

direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;

- non rimuovere o modificare senza autorizzazione o comunque compromettere i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di propria competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- sottoporsi ai controlli sanitari previsti;
- contribuire, insieme al Datore di Lavoro, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

In generale tutti i Destinatari del Modello devono rispettare quanto definito al fine di preservare la sicurezza e la salute dei lavoratori e comunicare tempestivamente alle strutture interne competenti eventuali segnali di rischio e/o pericolo, incidenti (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e delle procedure aziendali.

REGOLE DI COMPORTAMENTO

É fatto divieto ai Destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare, presi individualmente o collettivamente, in maniera diretta o indiretta, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-*septies* del Decreto).

É fatto, altresì, divieto di porre in essere comportamenti in violazione dei principi e delle Procedure aziendali, ovvero di altre disposizioni aziendali in materia di salute e sicurezza dei luoghi di lavoro.

In particolare, con riferimento ai Terzi eventualmente coinvolti nelle attività:

- gli **appaltatori** devono: (i) garantire la propria idoneità tecnico-professionale con riferimento ai lavori da eseguire; (ii) recepire le informazioni fornite da SIIT S.c.p.A. in merito ai rischi presenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate dalla Società; (iii) cooperare e coordinarsi con SIIT S.c.p.A. per l'individuazione e l'attuazione delle misure di prevenzione e protezione e degli interventi necessari al fine di prevenire i rischi sul lavoro a cui sono esposti i soggetti coinvolti, anche indirettamente, nell'esecuzione dei lavori da eseguire in appalto o mediante contratto d'opera o di somministrazione;

- i **fornitori** devono vendere, noleggiare e concedere in uso esclusivamente strumenti ed attrezzature di lavoro, dispositivi di protezione individuali ed impianti che siano conformi alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro;
- gli **installatori**, infine, devono attenersi alle istruzioni fornite dai fabbricanti dei prodotti da installare, con particolare riferimento alle misure e agli adempimenti in materia di salute e sicurezza sul lavoro.

Infine, è fatto obbligo a tutti i Destinatari del presente Modello (come identificati nella Parte Generale) di segnalare prontamente all'OdV qualsiasi eventuale violazione delle disposizioni previste nel Modello di SIIT S.c.p.A. e della presente sezione.

10. RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO (ART. 25-OCTIES D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei reati oggetto di analisi, individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

a) astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare la fattispecie di reato considerate;
b) astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
c) riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

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

- ricevere, trasmettere, trasferire, vendere, acquistare o comunque movimentare, beni, denaro o altre utilità, nella consapevolezza o nel dubbio della loro provenienza illecita;
- violare le norme di legge esistenti circa le modalità di incasso e/o pagamento.

È, altresì, fatto obbligo in particolare di:

- tenere un comportamento corretto, trasparente e di collaborazione, nel rispetto delle norme di legge, in tutte attività inerenti all'operatività aziendale, ed in particolare nell'ambito delle attività sensibili – come di seguito definite - mantenendosi aggiornati sull'evoluzione normativa in materia;
- verificare l'attendibilità dei fornitori e di eventuali *partner* commerciali e finanziari, sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori);
- ispirarsi a criteri di trasparenza nell'esercizio dell'attività aziendale e nella scelta dei fornitori e di eventuali *partner* commerciali e finanziari, prestando la massima attenzione alle notizie riguardanti i soggetti terzi con i quali la Società ha rapporti di natura finanziaria o societaria che possano anche solo generare il sospetto della commissione di uno dei reati *de quo*;

- verificare la regolarità degli incassi/pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- utilizzare il bonifico bancario quale strumento privilegiato di incasso e di pagamento;
- assicurare la tracciabilità delle fasi del processo decisionale relativo ai rapporti finanziari e societari con soggetti terzi o società del gruppo;
- conservare la documentazione a supporto delle operazioni finanziarie e societarie, adottando tutte le misure di sicurezza necessarie;
- informare tempestivamente chi di dovere - nel rispetto delle disposizioni previste dalla regolamentazione interna - ogniqualvolta si è a conoscenza, si sospetta o si hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio.

11. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti in materia di violazione del diritto d'autore individuati e ritenuti rilevanti per SIIT S.c.p.A., i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;
- astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
- riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

A tal proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto ai Destinatari in particolare di:

1. caricare, senza autorizzazione, *software* sulle *workstation* fornite dalla Società;
2. riprodurre o distribuire abusivamente fonogrammi o videogrammi di opere musicali o audiovisive;

3. riprodurre, trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca dati senza aver preventivamente ottenuto la necessaria autorizzazione dal legittimo titolare del diritto d'autore e/o del diritto di sfruttamento economico della banca dati medesima.

Con riferimento all'acquisto o all'utilizzo da parte della Società di qualsivoglia bene suscettibile di tutela ai sensi della Legge sul Diritto d'Autore, è fatto altresì obbligo ai Destinatari di ottenere dai rispettivi titolari e/o licenzianti dei relativi diritti di utilizzo sui beni in questione, specifiche dichiarazioni volte ad attestare le seguenti principali circostanze:
(i) di essere i legittimi titolari dei diritti di sfruttamento economico sui beni oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
(ii) di garantire che i beni oggetto di cessione o di concessione in uso non violano alcun diritto di proprietà intellettuale in capo a terzi;
(iii) di impegnarsi a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio di natura patrimoniale e non, le potesse derivare, per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

12. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE (ART. 25-DUODECIES D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei Delitti di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;
- astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
- riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

In particolare, i Destinatari devono rispettare principi e norme di comportamento di seguito indicati:

- non instaurare alcun rapporto di lavoro con soggetti privi di permesso di soggiorno;
- verificare in via preventiva le informazioni disponibili su ogni possibile fornitore (incluse le informazioni economiche e relative alla reputazione) ed evitare di intraprendere o intrattenere relazioni d'affari con fornitori dei quali sia conosciuto o sospettato il coinvolgimento in attività illecite;
- non compiere altri atti diretti a procurare illegalmente l'ingresso di stranieri nel territorio dello Stato Italiano o di altro Stato.

13. REATI TRIBUTARI (ART. 25-QUINQUIESDECIES D.LGS. 231/01)

Al fine di prevenire ed impedire il verificarsi dei reati di natura tributaria, i Destinatari, come definiti nella Parte Generale del presente Modello, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Comportamento e dalle specifiche Procedure aziendali:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato considerate;

- astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati considerati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi;
- riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

Con specifico riferimento alla prevenzione dei reati tributari, a titolo meramente esemplificativo e non esaustivo, i Destinatari operanti nelle aree di attività a rischio reato sono tenuti a:

- redigere, fornire o trasmettere all'Amministrazione finanziaria documenti e/o dati corretti, completi, esatti e rispondenti alla realtà, tali da configurare una descrizione limpida della situazione fiscale e finanziaria della Società ai fini dell'esatto adempimento degli obblighi fiscali e tributari;
- mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione con l'Amministrazione finanziaria, assicurando il pieno rispetto delle norme di legge e regolamentari nello svolgimento di tutte le attività finalizzate all'acquisizione, elaborazione, gestione e comunicazione dei dati e delle informazioni destinate a consentire un fondato e veritiero giudizio ai fini fiscali sulla situazione patrimoniale, economica, finanziaria, fiscale e tributaria della Società. A questo proposito, ai Destinatari è fatto divieto, in particolare, di:
  - contabilizzare (o detenere al fine di prova nei confronti dell'Amministrazione finanziaria) ed utilizzare nelle dichiarazioni (relative alle imposte sui redditi e/o sul valore aggiunto) elementi passivi fittizi derivanti da fatture o altri documenti per operazioni oggettivamente/soggettivamente inesistenti, al fine di evadere le imposte sui redditi o sul valore aggiunto;
  - indicare nelle dichiarazioni elementi attivi inferiori a quelli effettivi o elementi passivi fittizi o crediti e ritenute fittizi, compiendo operazioni simulate oggettivamente o soggettivamente, ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'Amministrazione finanziaria, al fine di evadere le imposte sui redditi o sul valore aggiunto;
  - emettere o rilasciare fatture o altri documenti per operazioni oggettivamente/soggettivamente inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto;
  - alterare o comunque riportare in maniera inesatta i dati e le informazioni destinati alla predisposizione e stesura dei documenti di natura patrimoniale, economica, finanziaria e fiscale;
  - occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione – in modo da non consentire all'Amministrazione finanziaria la ricostruzione dei redditi o del volume d'affari – al fine di evadere le imposte sui redditi o sul valore aggiunto ovvero di

consentire l'evasione a terzi;

- indicare nelle dichiarazioni annuali relative alle imposte sui redditi o sul valore aggiunto elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro;
- omettere di presentare, essendovi obbligata la Società, una delle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto ovvero la dichiarazione di sostituto d'imposta, nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro;
- utilizzare indebitamente in compensazione crediti non spettanti ovvero crediti inesistenti al fine di non versare le somme dovute, nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro;

- non alienare simulatamente o non compiere altri atti fraudolenti sui beni / cespiti della Società o sui beni altrui, idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte;
- illustrare dati ed informazioni in modo tale da fornire una rappresentazione corretta e veritiera sulla situazione patrimoniale, economica, finanziaria e fiscale della Società;
- mettere a disposizione dei soci e degli altri organi sociali tutta la documentazione riguardante la gestione della Società e prodromica allo svolgimento di ogni e qualsivoglia attività di verifica e controllo legalmente e statutariamente attribuita ai predetti. A questo proposito, ai Destinatari è fatto particolare divieto di porre in essere comportamenti che impediscano materialmente o comunque ostacolino lo svolgimento dell'attività di controllo da parte dei soci e degli altri organi di controllo mediante l'occultamento o la distruzione di documenti ovvero mediante l'uso di altri mezzi fraudolenti.

14. CONTRABBANDO (ART.25-SEXIESDECIES, D.LGS. 231/2001)

La presente sezione, oltre agli specifici principi di controllo contenuti nella sezione per Aree a Rischio, richiama i principi generali di comportamento, alla cui osservanza sono tenuti tutti i Destinatari, e prevede l'espresso divieto a carico dei medesimi di porre in essere comportamenti:

- tali da integrare le fattispecie di reato di cui ai sensi dell'art. 25-sexiesdecies, ovvero tali da agevolarne la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate ai sensi dell'art. 25-sexiesdecies, possano potenzialmente

diventarlo;

- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi dal Modello, dal Codice di Condotta e dalla Practice.

Con specifico riferimento alla prevenzione dei reati di contrabbando ci cui al d.P.R. n. 43 del 23 gennaio 1973 e s.m.i., a titolo meramente esemplificativo e non esaustivo, i Destinatari operanti nelle aree di attività a rischio reato sono tenuti a:

- redigere, fornire o trasmettere alle Autorità doganali documenti e/o dati corretti, completi, esatti e rispondenti alla realtà, tali da configurare una descrizione veritiera delle merci in transito, anche ai fini dell'esatto adempimento dei diritti di confine (dazi doganali);
- mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione con le Autorità doganali, assicurando il pieno rispetto delle norme di legge e regolamentari nello svolgimento di tutte le attività finalizzate alla identificazione e alla tracciatura delle merci in transito e alla comunicazione dei dati e delle informazioni destinate a consentire l'esatto adempimento dei diritti di confine (dazi doganali).

A questo proposito, ai Destinatari è fatto divieto, in particolare, di:

- introdurre merci estere attraverso il confine di terra in violazione delle prescrizioni, dei divieti e delle limitazioni stabilite dalla legge (attraversamento della merce al di fuori dei punti stabiliti / delle linee doganali);
- scaricare o depositare merci estere nello spazio intermedio tra la frontiera e la più vicina dogana;
- nascondere merci estere sulla persona o nei bagagli o nei colli o nelle suppellettili o fra merci di altro genere od in qualunque mezzo di trasporto, per sottrarle alla visita doganale;
- asportare merci dagli spazi doganali senza aver pagato i diritti dovuti o senza averne garantito il pagamento;
- portare fuori del territorio doganale merci nazionali o nazionalizzate soggette a diritti di confine in violazione delle prescrizioni;
- nascondere merci nelle navi estere allo scopo di sottrarle alla visita doganale;
- gettare da un aeromobile in volo, nel territorio doganale, merci estere ovvero nasconderle nell'aeromobile stesso allo scopo di sottrarle alla visita doganale;
- dare, in tutto o in parte, a merci estere importate in franchigia e con riduzione dei diritti stessi una destinazione od un uso diverso da quello per il quale è stata concessa la franchigia o la riduzione;
- detenere, quali concessionari di un magazzino doganale di proprietà privata, merci estere per le quali non vi è stata la prescritta dichiarazione d'introduzione o che non risultano assunte in carico nei registri di deposito;

- sottoporre le merci a manipolazioni artificiose ovvero usare altri mezzi fraudolenti nelle operazioni di importazione o di esportazione temporanea o nelle operazioni di riesportazione e di reimportazione, allo scopo di sottrarle al pagamento di diritti che sarebbero dovuti;
- al di fuori delle predette casistiche - e più genericamente - sottrarre merci al pagamento dei diritti di confine dovuti.

SEZIONE DI DETTAGLIO

La presente sezione, strutturata per processo, contiene l'indicazione delle Aree a Rischio Reato individuate in relazione ai Reati Presupposto rilevanti e riporta, per ciascuna Area, le seguenti informazioni:

- le famiglie di reato applicabili ed i relativi reati presupposto astrattamente perpetrabili (per la descrizione dei reati presupposto e del relativo trattamento sanzionatorio *ex* Decreto 231, si rinvia al documento in Appendice al Modello);
- le relative attività sensibili ("**Attività Sensibili**"), ovvero quelle nel cui espletamento è connesso il rischio di commissione dei reati previsti dal D.Lgs. 231/01;
- le Strutture aziendali di SIIT S.c.p.A. coinvolte nelle Attività Sensibili e che, astrattamente, potrebbero commettere i Reati Presupposto previsti dal Decreto 231 nell'interesse o a vantaggio della Società, sebbene tale individuazione non debba considerarsi, in ogni caso, tassativa, atteso che ciascun soggetto aziendale potrebbe, in linea teorica, essere coinvolto a titolo di concorso. Si considerano sempre incluse, inoltre, le Funzioni competenti a diretto riporto delle Direzioni, nonché eventuali procuratori della Società ed i vertici aziendali, qualora siano coinvolti nelle aree a rischio reato in funzione delle previsioni del sistema di deleghe e procure vigente;
- i principali controlli preventivi in essere a presidio dei rischi di commissione reato.

Inoltre, sono state identificate anche le aree a rischio c.d. "strumentali", ossia quelle aree caratterizzate da particolari attività che possono assumere carattere di supporto (o, appunto, strumentale) rispetto alla commissione di determinati reati (ad es. contro la Pubblica Amministrazione: Corruzione e Istigazione alla corruzione).

Infine, trasversalmente a tutte le Aree a Rischio Reato, sono stati considerati rilevanti anche i seguenti principi generali di controllo:

- previsione di un sistema di deleghe e procure nonché di un sistema organizzativo (compiti, ruoli e responsabilità formalizzati);
- esistenza di specifici protocolli aziendali (ad esempio, procedure locali) che descrivono ruoli, responsabilità, attività, modalità operative e controlli;

- segregazione dei compiti tra:
  - chi richiede / chi autorizza e chi effettua i pagamenti;
  - chi esegue e chi controlla;
- tracciabilità e verificabilità *ex post* di ogni operazione relativa alle Attività Sensibili;
- archiviazione della documentazione, ivi incluse le scritture contabili, al fine di impedirne l'occultamento o la distruzione ovvero di garantire la tracciabilità del processo.

La presente sezione di dettaglio ha carattere riservato e non può essere comunicata a terzi in ragione delle informazioni ivi contenute.

LE AREE A RISCHIO-REATO

Nel corso dell'attività di analisi condotta nell'ambito delle diverse direzioni/funzioni aziendali, sono state individuate le seguenti **"Aree a Rischio-Reato"** (o semplicemente "**Aree a Rischio**") rispetto alle quali è stato ritenuto astrattamente sussistente e rilevante il rischio di commissione dei reati previsti dal D. Lgs 231/01:

1. Amministrazione, Contabilità e Bilancio;
2. Gestione delle Attività di Ricerca e Sviluppo;
3. Gestione Affari Legali e Societari;
4. Gestione delle Risorse Umane;
5. Gestione della Salute e Sicurezza sul Lavoro;
6. Gestione degli Acquisti.

Si riporta di seguito, per ciascuna "Area a Rischio", l'indicazione delle Attività Sensibili[5] che la compongono, dei ruoli aziendali coinvolti, delle fattispecie di reato astrattamente rilevanti e dei principali controlli previsti a mitigazione dei fattori di rischio che potrebbero favorire la commissione dei reati ("**Norme di comportamento particolare nelle Aree a Rischio**"). Per quanto concerne le possibili modalità di commissione dei reati potenzialmente applicabili, si rimanda alle schede di mappatura di Risk Assessment (Allegato A) da considerarsi parte del presente Modello.

[5] Si definiscono "attività sensibili" quelle attività al cui svolgimento è connesso il rischio di commissione dei reati.

NORME DI COMPORTAMENTO PARTICOLARE NELLE SINGOLE AREE A RISCHIO-REATO

AREA A RISCHIO N. 1: AMMINISTRAZIONE, CONTABILITÀ E BILANCIO

a) Attività Sensibili

In relazione alla presente Area a Rischio sono state identificate le seguenti attività:

- Gestione della contabilità fornitori e clienti
- Incassi e gestione del credito
- Gestione degli ammortamenti dei cespiti
- Gestione della contabilità generale
- Gestione dei rapporti con le banche - istituti finanziari
- Gestione della piccola cassa
- Gestione della Tesoreria
- Gestione dei rapporti con il Revisore Legale
- Gestione dei contenziosi
- Gestione degli adempimenti societari
- Gestione delle imposte e delle relative dichiarazioni
- Gestione dei rapporti con la Pubblica Amministrazione

b) Funzioni aziendali /unità organizzative e figure coinvolte

Le Funzioni Aziendali / unità organizzative e figure coinvolte nello svolgimento delle attività sopra descritte sono:

- Ufficio Amministrazione;
- Presidente del Consiglio di Gestione;
- Direttore Sviluppo Programmi;
- Tutte le altre funzioni coinvolte nelle attività di amministrazione, contabilità e bilancio.

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

- Reati contro la Pubblica Amministrazione o in danno dell'Unione Europea (Art. 24 e Art. 25 del D.Lgs. 231/01):
  - Corruzione per l'esercizio della funzione (art. 318 c. p.);
  - Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
  - Corruzione in atti giudiziari (art. 319 *ter*);
  - Indebita induzione a dare o promettere utilità (art. 319 *quater*);
  - Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
  - Pene per il corruttore (art. 321 c.p.);
  - Istigazione alla corruzione (art. 322 c.p.);
  - Truffa ai danni dello Stato o di altri enti pubblici (art. 640, comma 2, n. 1 c.p.);
  - Frode informatica (art. 640-*ter* c.p.).

- Delitti di criminalità organizzata (Art. 24-*ter* del D.Lgs. 231/01)
  - Associazione per delinquere (art. 416 c.p.);
  - Associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.);
  - Scambio elettorale politico mafioso (art. 416-*ter* c.p.).

- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-*bis* del D.Lgs. 231/01)
  - Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
  - Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.).

- Reati societari (Art. 25-*ter* del D.Lgs. 231/01)
  - False comunicazioni sociali (art. 2621 c.c.);
  - Fatti di lieve entità (art. 2621 *bis* c.c.);
  - Impedito controllo (art. 2625 c.c.);
  - Indebita restituzione di conferimenti (art. 2626 c.c.);
  - Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
  - Illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.);
  - Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
  - Omessa comunicazione del conflitto d'interessi (art. 2629 *bis* c.c.);
  - Formazione fittizia del capitale (art. 2632 c.c.);
  - Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
  - Corruzione tra privati (art. 2635 c.c.);
  - Istigazione alla corruzione tra privati (art. 2635-*bis* c.c.);

- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 comma 1 e 2 c.c.).

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (Art. 25-*quater* del D.Lgs. 231/01)
  - Finanziamento al terrorismo (art. 2 Convenzione di New York).

- Reati in materia di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita (Art. 25-*octies* del D.Lgs. 231/01)
  - Riciclaggio (art. 648 *bis* c.p.);
  - Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);
  - Autoriciclaggio (art. 648 *ter* 1 c.p.).

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Art. 25-*decies* del D.Lgs. 231/01)
  - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.).

- Reati tributari (Art. 25-*quinquiesdecies* del D.Lgs. 231/01)
  - Dichiarazione fraudolenta mediante fatture per operazioni inesistenti (art. 2 D.Lgs. 74/2000);
  - Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000);
  - Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. 74/2000);
  - Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000);
  - Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000);
  - Delitto di dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
  - Delitto di omessa dichiarazione (art. 5 D.Lgs. n. 74/2000);
  - Delitto di indebita compensazione (art. 10-quater D.Lgs. n. 74/2000).

- Delitti informatici (Art. 24 del D.Lgs. 231/01)
  - Danneggiamento di dati, programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.);
  - Danneggiamento di sistemi informatici o telematici di pubblica utilità (artt. 635-*quinquies* c.p.).

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda al *Risk Assesment* di riferimento "*Gestione delle attività di Amministrazione, Contabilità e Bilancio e Gestione dei Flussi Finanziari*"):

- La creazione di una nuova anagrafica fornitore, deve ottenere una previa autorizzazione da parte dei soggetti competenti.
- I dati relativi ai fornitori sono gestiti attraverso il sistema E - SOLVER. La gestione avviene secondo un processo strutturato che assicura la segregazione delle funzioni, la completezza ed accuratezza dei dati, il controllo preliminare di esistenza ad eventuali modifiche ai dati.
- L'entrata merce e la fatturazione sono gestite attraverso il sistema E-SOLVER che effettua a sistema controlli ""three way match - allineamenti tra entrata merce, fattura e ordine"", nonchè controlli rispetto ad eventuali precedenti contabilizzazioni.
- Tutta la documentazione viene archiviata a cura dell'Ufficio Amministrazione.
- I pagamenti sono effettuati secondo un iter strutturato che prevede la segregazione "di fatto"" tra soggetto predisponente e soggetto approvante il flusso. L'esecuzione dei pagamenti viene effettuata dal Responsabile Amministrazione mediante l'utilizzo di specifici token (su delega "di fatto" del Presidente del Consiglio di Gestione).
- La creazione di una nuova anagrafica cliente, deve ottenere una previa autorizzazione da parte dell' Ufficio Amministrazione.
- Le richieste di quotazione del cliente sono gestite sulla base di specifiche procedure.
- Mensilmente vengono realizzate riconciliazioni bancarie, confrontando i saldi del conto bancario e della contabilità.
- Eventuali non conformità rilevate rispetto alla fornitura vengono gestite tramite l'emissione della nota di credito da parte del cliente ovvero apposito storno di somme.
- La gestione dei pagamenti dovuti alla Società avviene secondo un iter strutturato che prevede scadenze definite, verifica mensile formalizzata degli scaduti e pagamenti tracciati.
- Le eventuali cessioni del credito della Società possono essere effettuate solo con specifica autorizzazione del Responsabile Amministrazione.
- La registrazione degli ammortamenti e la relativa contabilizzazione avviene a sistema secondo scadenze predefinite a calendario. La funzione di calcolo

ammortamenti registra il valore di ammortamento sia con riferimento al costo storico che ad eventuali rivalutazioni. In caso di dismissioni il sistema permette di chiudere la voce-anagrafica relativa al cespite in automatico a seguito della registrazione contabile della fattura di vendita. Il calcolo di un'eventuale plusvalenza o minusvalenza viene fatto in automatico a sistema, salvo ipotesi minoritarie in cui la fattura viene registrata manualmente. In questi ultimi casi il calcolo viene effettuato dagli addetti dell'Amminstrazione e verificato dal Responsabile Amministrazione.

- La creazione di nuovi conti e/o la modifica di conti esistenti è gestita in maniera centralizzata e viene approvata da parte del Responsabile Amminstrazione di SIIT S.c.p.a.
- La Società ha predisposto e condiviso un calendario/scadenzario relativo alle chiusure del bilancio.
- Il periodo contabile viene gestito mediante il sistema informatico di riferimento del Consulente Fiscale esterno.
- L'allineamento contabile con riferimento ai dati relativi alla Contabilità Clienti, Fornitori e Cespiti avviene in automatico a sistema, ad esclusione di eventuali scritture manuali di fine periodo e/o di rettifiche registrate in corso d'anno.
- Sono mensilmente effettuate attività di riconciliazione tra la fatturazione e quanto riportato in contabilità.
- La Società segue un iter strutturato per la predisposizione del bilancio, prevedendo controlli da parte della Funzione Amministrazione e del Revisore Legale rispetto ai dati mensilmente elaborati a sistema.
- Il calcolo delle imposte dovute viene effettuato dal Consulente Fiscale esterno.
- L'importo delle imposte calcolate viene rivisto dal Revisore Legale.
- La società ha identificato "di fatto" il soggetto che può intrattenere i rapporti con gli Istituti finanziari, nella figura del Presidente del Consiglio di Gestione.
- Eventuali finanziamenti sono gestiti a livello dalla Società da figure dotate di adeguati poteri d’ acceso previa gara tra più istituti creditizi.
- La gestione della piccola cassa avviene secondo prassi consolidate che prevedono forme di presidio quali riconciliazioni tra entrate ed uscite, registrazione dei giustificativi di spesa e specifici monitoraggi.
- La Società di revisione incaricata annualmente effettua la conta di cassa e verifica la quadratura con il sistema SAP.
- La Società ha identificato i soggetti responsabili di intrattenere i rapporti con la società di revisione, nonchè di curare la tenuta dei libri sociali. La Società ha inoltre identificato, seppur di fatto, i soggetti responsabili di intrattenere i rapporti con gli enti e le autorità pubbliche.

- La Società ha identificato nei consulenti fiscali esterni di riferimento i soggetti deputati alla predisposizione delle dichiarazioni di natura fiscale.
- Le comunicazioni annuali, prima dell'invio all'Agenza delle Entrate, subiscono un doppio controllo (condivisione con il consulente esterno, condivisione con il revisore incaricato).
- L'utilizzo eventuale del credito IVA viene deciso dalla Società, sulla base di quanto discusso con il Consulente Fiscale esterno.
- Le imposte dovute in ambito di personale (dipendente o assimilato) sono determinate dal Consulente del Lavoro esterno.
- Le imposte dovute in ambito personale (liberi professionisti) sono calcolate dal Consulente del Lavoro esterno.
- Il documento di dichiarazione 770 viene predisposto per la Società da parte del Consulente Fiscale, sulla base dei dati messi a disposizione dalla Società.
- "SIIT S.c.p.A. ha adeguato il proprio comportamento a quanto esposto.

AREA A RISCHIO N. 2: GESTIONE DELLE ATTIVITÀ DI RICERCA E SVILUPPO

a) Attività Sensibili

In relazione alla presente Area a Rischio sono state identificate le seguenti attività:

- Attività di Ricerca e Sviluppo realizzate per conto dei membri del consorzio
- Attività di Ricerca e Sviluppo realizzate per conto della Società Cliente
- Rendicontazione fiscale delle attività di Ricerca e Sviluppo
- Misure di sicurezza (fisica e logica) a presidio dei progetti di ricerca e sviluppo
- Gestione delle Piattaforme Informatiche
- Gestione della Proprietà Intellettuale

b) Funzioni aziendali /unità organizzative e figure coinvolte

Le Funzioni Aziendali / organizzative e figure coinvolte nello svolgimento delle attività sopra descritte sono:

- Presidente del Consiglio di Gestione;
- Direttore Sviluppo Programmi;
- Tutte le altre funzioni coinvolte nelle attività di Ricerca e Sviluppo.

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

- <u>Reati contro la Pubblica Amministrazione e/o in danno dell'Unione Europea (Artt. 24 e 25 del D.Lgs 231/01)</u>
  - Malversazione a danno dello Stato (art. 316 bis c.p.)
  - Indebita percezione di erogazioni a danno dello Stato (art 316-ter c.p.)
  - Frode nelle pubbliche forniture (art. 356 c.p.)
  - Corruzione per l'esercizio della funzione (art.318 c.p.)
  - Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)

- <u>Delitti Informatici e Trattamento Illecito di Dati</u>
  - Documenti informatici (art. 491-bis c.p.)
  - Accesso abusivo ad un sistema informatico o telematico (art.615-ter c.p.)

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art.615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art.617-quater c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art.635-bis c.p.)
- Danneggiamento di sistemi informatici o telematici (art.635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art.635-quinquies c.p.)

- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-*bis* del D.Lgs. 231/01)
  - Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473 c.p.).

- Delitti contro l'industria e il commercio (Art. 25-*bis* 1 del D.Lgs. 231/01)
  - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.).

- Reati societari (Art. 25-*ter* del D.Lgs. 231/01)
  - Corruzione tra privati (art. 2635 c.c.) ed Istigazione alla corruzione tra privati (art. 2635 *bis* c.c.).

- Delitti in materia di violazione del Diritto d'Autore (Art. 25-novies del D.Lgs. 231/01)
  - Immissione in un sistema di reti telematiche di opere d'ingegno protette (art. 171 – a bis, Legge 633 del 1941).

- Reati tributari (Art. 25 quinquiesdecies del D.Lgs. 231/01)
  - Delitto di indebita compensazione (art. 10-quater D.Lgs. n. 74/2000).

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda al *Risk Assesment* di riferimento "Ricerca e Sviluppo).

- La Società ha definito nella prassi consolidata un processo strutturato per le attività di ricerca e sviluppo di nuovi prodotti e nuove tecnologie interessate dall'utilizzo di brevetti, marchi e disegni che prevede un iter consolidato e conosciuto dal proprio personale.
- Quando sono sviluppati nuovi prodotti o loro nuovi utilizzi, sono condotte indagini in merito alla effettiva novità degli stessi ed alla non violazione della proprietà intellettuale di terzi.
- Sono previsti specifici indirizzi per quanto riguarda la titolarità dei risultati di ricerca, la tutela e l'utilizzo degli stessi.
- Sono svolte periodiche attività di monitoraggio sull'avanzamento del progetto realizzativo (a seguito dell'eventuale ottenimento del contributo pubblico) e sul relativo reporting alla PA, con evidenza e gestione delle eventuali anomalie.
- Sono svolte attività di controllo sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.
- Sono utilizzate adeguate forme contrattuali al fine di regolamentare gli obblighi della controparte (es. fornitori, partner) in merito al rispetto della proprietà intellettuale.
- Sono chiaramente definite le modalità e i criteri di gestione dei brevetti e dei prodotti/processi coperti da diritti di proprietà industriale.
- Laddove previsto dalle tipologie di incarico, sono strutturate apposite clausole che garantiscono la rinuncia della Società ai diritti relativi alla Proprietà Intellettuale nei confronti dei soggetti consorziati.
- Nel predisporre la rendicontazione dei dati necessari per l'ottenimento dei benefici fiscali previsti dall'attività di ricerca e sviluppo svolta, la Società si avvale di studi professionali esterni, garantendo la tracciabilità, accuratezza e ripercorribilità dei dati relativi ai costi di ricerca e sviluppo sostenuti.
- La Società si avvale della consulenza di studi professionali esterni per stabilire le stime dei costi sostenuti per finalità di ricerca e sviluppo dal personale aziendale delle Funzioni di supporto.
- Tutta la documentazione afferente l'Area Ricerca e Sviluppo è debitamente archiviata.
- La Società ha previsto misure di sicurezza a garanzia della riservatezza e segretezza industriale.
- Sono definite, nei contratti con i terzi, apposite previsioni contrattuali relativamente al trattamento delle informazioni riservate e alla tutela dei diritti di proprietà intellettuale.
- La Società ha disciplinato l'attività inventiva svolta dal personale dell'Area Ricerca e Sviluppo in maniera strutturata all'interno di specifici contratti.

- La Società ha impostato il proprio sistema di gestione delle tematiche IT tenendo anche in conto le esigenze di cyber security, impostando sistemi di sicurezza (firewall virtuali, antivirus, e altri meccanismi di monitoraggio e prevenzione della sicurezza della rete aziendale).
- La Società ha implementato un meccanismo di monitoraggio volto a verificare l'effettiva utilità delle licenze acquistate nonchè l'utilizzo non in violazione dei diritti di autore.
- La Società ha impostato il proprio sistema di gestione delle tematiche IT in compliance con i requisiti normativi previsti dal Reg. UE 2016/679.
- Viene effettuato un regolare backup di dati e applicazioni nonché delle informazioni salvate nelle aree condivise centralizzate.
- E' garantito l'aggiornamento periodico delle vulnerabilità dei sistemi aziendali, attraverso l'identificazione e installazione di patches di sicurezza rilasciate da parte del fornitore del software.
- Sono presenti e utilizzati strumenti finalizzati alla registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche, alla registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico http) e alla protezione delle informazioni registrate (log) contro accessi non autorizzati.
- È prevista l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password od altro sistema di autenticazione sicura.
- Vengono svolte periodiche attività di rivalidazione delle utenze e dei privilegi ad esse collegate da parte delle figure autorizzate.
- Sono adottati 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.
- Tutte le attività svolte da consulenti esterni sono regolamentate da accordi contrattuali preventivamente autorizzati.
- SIIT S.c.p.A. ha adeguato il proprio comportamento a quanto esposto inoltre all'interno delle seguenti specifiche Procedure adottate nonché alle altre istruzioni/procedure aziendali in essere:

Procedure formalizzate in seguito alle attività di Risk Assessment 231	Altre procedure ed istruzioni operative collegate all'Area
N/A	- Linee Guida della Proprietà Industriale nei progetti di ricerca di SIIT;

AREA A RISCHIO N° 3 : AFFARI LEGALI E SOCIETARI

a) Attività Sensibili

In relazione alla presente Area a Rischio sono state identificate le seguenti attività:

- Gestione del Contenzioso Giudiziale e Stragiudiziale
- Comunicazione di Informazioni Societarie e della reportistica periodica
- Gestione delle relazioni o delle altre comunicazioni Sociali
- Gestione delle operazioni societarie

b) Funzioni aziendali /unità organizzative e figure coinvolte

Le Funzioni Aziendali / unità organizzative e figure coinvolte nello svolgimento delle attività
sopra descritte sono:

- Presidente del Consiglio di Gestione;
- Direttore Sviluppo Programmi;
- Tutte le altre funzioni coinvolte negli Affari Legali e Societari.

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

- Reati contro la Pubblica Amministrazione o in danno dell'Unione Europea (Artt. 24 e 25 del D.Lgs. 231/01)
  - Corruzione per l'esercizio della funzione (art. 318 c.p.);
  - Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
  - Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
  - Pene per il corruttore (art. 321 c.p.);
  - Istigazione alla corruzione (art. 322 c.p.);
  - Traffico di influenze illecite (art. 346-bis c.p.).

- Delitti di criminalità organizzata (Art. 24-*ter* del D.Lgs. 231/01)
  - Associazione per delinquere (art. 416 c.p.);
  - Associazione di stampo mafioso (art. 416 *bis* c.p.).

- Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico (Art. 25 *quater* del D.Lgs. 231/01)
    - Finanziamento al terrorismo (art. 2 Convenzione di New York).

- Reati societari (Art. 25-*ter* del D.Lgs. 231/01)
    - Corruzione tra privati (art. 2635 c.c.) ed Istigazione alla corruzione tra privati (art. 2635 *bis* c.c.).

- Delitti contro la personalità individuale (art. 25-*quinquies)*
    - Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)

- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-*octies* del D.Lgs. 231/01)
    - Ricettazione (art. 648 c.p.), Riciclaggio (art. 648-*bis* c.p.) e Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);
    - Autoriciclaggio (art. 648 -*ter*1 c.p.).

- Reati Tributari (art. 25 - *quinquiesdecies* del D.Lgs 231/01)
    - Dichiarazione Fraudolenta mediante fatture per operazioni inesistenti (art. 2 D.Lgs 74/2000)
    - Dichiarazione fraudolenta mediante altri artifizi (art. 3 D.Lgs 74/2000)
    - Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs 74/2000)

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda alla relativa scheda di mappatura di Risk Assessment di cui all'Allegato A).

- Mediante il Supporto del legale esterno viene svolta un'attività di monitoraggio sullo stato dei contenziosi mediante segnalazioni e riunioni periodiche anche al fine di sottoporre alla Direzione la necessaria valutazione dei rischi e dei costi a loro connessi.
- Nell'ambito di situazioni di contenzioso civile, amministrativo, penale, tributario/fiscale esistono modalità definite di valutazione dell'impatto e gestione del rischio (es. verifica giurisprudenza, precedenti contenziosi).

- Sono definiti specifici flussi di reporting in relazione ad eventi giudiziari di particolare rilevanza ed è previsto l'invio di reportistica periodica verso l'Alta Direzione.
- Viene svolta, con il supporto legale esterno, una attività di analisi dell'introduzione di nuove leggi/regolamenti che impattino sull'attività svolta.
- Sono identificate le responsabilità e le modalità di verifica dell'allineamento delle attività societarie alla normativa vigente e della comunicazione alle Funzioni/persone interessate all'interno della Società.
- Eventuali operazioni sul capitale sono monitorate ed autorizzate dai soggetti dotati di adeguati poteri.
- SIIT S.c.p.A. ha adeguato il proprio comportamento a quanto esposto.

AREA A RISCHIO N. 4: GESTIONE DELLE RISORSE UMANE

a) Attività Sensibili

In relazione alla presente Area a Rischio sono state identificate le seguenti attività:

- Perfezionamento del contratto di assunzione;
- Gestione dei Benefit e degli Asset Aziendali assegnati ai dipendenti;
- Gestione delle anagrafiche dei dipendenti e monitoraggio presenze;
- Elaborazione e trasmissione dei cedolini e contabilizzazione del costo di lavoro;
- Gestione Note Spese e trasferte;
- Gestione adempimenti contributivi, previdenziali e assistenziali;
- Formazione del personale;
- Valutazione delle performance;
- Gestione dei finanziamenti;
- Gestione dei contenziosi;
- Gestione dei rapporti con le organizzazioni sindacali.

b) Funzioni aziendali /unità organizzative e figure coinvolte

Le Funzioni Aziendali / unità organizzative e figure coinvolte nello svolgimento delle attività sopra descritte sono:

- Presidente Consiglio di Gestione;
- Funzione Amministrazione Personale;
- Direttore Sviluppo Programmi;
- RSPP.

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

- Reati contro la Pubblica Amministrazione e/o a danno dell'Unione Europea (art. 24 e Art. 25)
  - Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.);
  - Truffa ai danni dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1 c.p.);
  - Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
  - Frode informatica (art. 640-ter c.p.);
  - Malversazione a danno dello Stato art. 316-bis;
  - Corruzione per l'esercizio della funzione (art. 318 c.p.);
  - Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
  - Circostanze aggravanti (art. 319-bis c.p.);
  - Induzione indebita a dare o promettere utilità (art. 319 -quater c.p.);
  - Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
  - Istigazione alla corruzione (art. 322 c.p.);
  - Pene per il corruttore (art. 321 c.p.).

- Delitti informatici e Trattamento illecito dei dati (art.24-bis)
  - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità (art.635-ter c.p.);
  - Danneggiamento di sistemi informatici o telematici di pubblica utilità (art.635-quinquies c.p.).

- Delitti di criminalità organizzata (Art. 24-*ter* del D.Lgs. 231/01)
  - Associazione per delinquere (art. 416 c.p.);
  - Associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.);
  - Scambio elettorale politico-mafioso (art. 416-ter c.p.).

- Reati Societari (Art. 25-*ter* del D.Lgs. 231/01)
  - Corruzione tra privati (art. 2635 c.c.);
  - Istigazione alla corruzione tra privati (art. 2635-*bis* c.c.);
  - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art.2368 c.1 e 2 c.c.

- Delitti contro la personalità individuale (art. 25-quinquies)
  - Intermediazione Illecita e Sfruttamento del Lavoro (art. 603-bis c.p.);

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies)

- Reati tributari (art. 25 *quinquiesdecies* del D.Lgs. 231/01)
  - Dichiarazione fraudolenta mediante fatture per operazioni inesistenti (art. 2 D.Lgs. 74/2000);

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda alla relativa scheda di mappatura di *Risk Assessment* di cui all'Allegato A).

- La Società ha adottato un proprio Codice di Condotta-Comportamento, all'interno del quale sono definiti i principi che ispirano la Sua azione nell'ambito dei rapporti con tutti gli *stakeholders*. All'interno di tale Codice sono state formalizzate specifiche previsioni riguardanti le fattispecie di reato previste dal D.Lgs. 231/01. I principi etici definiti dalla Società rientrano tra le materie oggetto del piano di informazione e formazione del personale.
- La selezione del personale avviene sulla base di prassi consolidate che prevedono diversi step valutativi.
- Sono svolte verifiche pre-assuntive relativamente all'onorabilità ed eticità dei potenziali candidati finalizzate a prevenire l'insorgere di situazioni pregiudizievoli che espongano la società al rischio di commissione di reati presupposto in tema di responsabilità amministrativa d'impresa (ad esempio relativamente all'esistenza di procedimenti penali o carichi pendenti, di conflitto di interesse, etc).
- Tutti i dati personali relativi al personale candidato ovvero assunto sono raccolti e trattati nel rispetto della normativa vigente in materia di privacy.
- L'accesso all'anagrafica dipendenti/collaboratori è riservato a un numero ristretto di persone autorizzate.
- Le modifiche all'anagrafica dipendenti sono adeguatamente documentate e autorizzate.
- E' garantito il tempestivo aggiornamento dei dati e delle informazioni relative al personale in concomitanza a variazioni nel profilo professionale del dipendente.
- L'anagrafica dipendenti è verificata periodicamente per assicurare l'accuratezza ed attinenza delle relative informazioni e che tutti i dipendenti assunti/dimessi siano correttamente aggiunti/rimossi.

- Per ogni dipendente/collaboratore esiste una cartella contenente tutta la documentazione concernente la sua vita lavorativa in Azienda.
- Nell'ambito delle attività di perfezionamento del contratto di lavoro, la Società richiede e verifica una serie di documenti, tra cui la regolarità del permesso di soggiorno per personale straniero. Di tutti i documenti ne viene, inoltre, monitorata la validità nel tempo (con richiesta di documenti rinnovati, qualora necessario).
- La consegna dei device aziendali al personale è accompagnata da specifica documentazione di riferimento.
- L'elaborazione dei cedolini avviene sulla base di automatismi a sistema che permettono di associare le presenze rilevate a lavoro con il gestionale Infinity di Zucchetti, utilizzato per i calcoli del costo del lavoro. Ferie, permessi e straordinari devono essere previamente autorizzati dal Responsabile della Funzione di appartenenza.
- I livelli retributivi sono definiti nel rispetto di quanto previsto dai Contratti Collettivi Nazionali del Lavoro (ove applicabili) ed in coerenza con le tabelle retributive di riferimento (es. retribuzioni di mercato), tenuto conto dell'esperienza pregressa e di eventuali competenze specifiche richieste.
- La completezza e correttezza dei dati riportati all'interno del cedolino viene verificata da un Consulente esterno, esperto in materia.
- Sono definite le regole per la rilevazione delle presenze/assenze, ore di straordinario, permessi e ferie del personale dipendente, attraverso adeguati sistemi (anche informatizzati).
- Tutti gli elementi non ricorrenti, come malattia, ferie e straordinari sono opportunamente rivisti da soggetti dotati di adeguati poteri.
- E' verificata la congruenza del calcolo dei cedolini rispetto alle informazioni comunicate allo studio paghe esterno.
- Il pagamento di salari e stipendi è autorizzato da soggetti dotati di adeguati poteri ed verificata la correttezza delle retribuzioni erogate.
- Eventuali variazioni delle componenti retributive del personale (es. bonus una tantum, premi di risultato, aumenti retributivi, etc.) sono preventivamente approvati da soggetti dotati di adeguati poteri.
- La prassi seguita dalla Società per la gestione delle note spese prevede che tutte le spese anticipate dal dipendente possano essere rimborsate solo previa esibizione dei giustificativi di spesa. La Funzione Amministrazione effettua verifiche su tutte le note spese presentate.
- SIIT S.c.p.A. ha adeguato il proprio comportamento a quanto esposto.

AREA A RISCHIO N. 5: GESTIONE DELLA SALUTE E SICUREZZA SUL LAVORO

a) Attività Sensibili

L'analisi dei processi aziendali di SIIT S.c.p.A. ha consentito di *(i)* individuare le Attività Sensibili nel cui ambito potrebbero astrattamente essere realizzate le fattispecie di reato previste dall'art. 25-*septies* D. Lgs. 231/01, così come richiamate dall'art. 30, comma 1, D.Lgs. 81/2008, *(ii)* identificare ed analizzare i possibili rischi potenziali ed, infine, *(iii)* costruire un sistema di controllo preventivo interno in materia di SSL idoneo a ridurre, ad un livello considerato "accettabile", il rischio di commissione dei reati considerati rilevanti.

Qui di seguito sono, quindi, elencate le cosiddette Attività Sensibili o *"a rischio-reato"* identificate dalla Società con riferimento agli illeciti in materia di SSL, di cui dall'art. 25-*septies* del Decreto:

- Organizzazione dei ruoli e delle attività connesse alla tutela della Salute e Sicurezza sul lavoro;
- Gestione attività di sorveglianza sanitaria;
- Gestione attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- Gestione delle emergenze;
- Attività di informazione, formazione e coinvolgimento dei lavoratori in tema di Salute e Sicurezza sul lavoro;
- Gestione dei rapporti con i fornitori con riferimento alle attività connesse alla salute e sicurezza sul lavoro;
- Gestione e manutenzione degli asset aziendali con riferimento alle attività connesse alla Salute e Sicurezza sul lavoro;
- Rilevazione, registrazione e gestione degli infortuni e degli incidenti;
- Misurazione e monitoraggio delle prestazioni in materia di Salute e Sicurezza sul Lavoro.

b) Funzioni aziendali/unità organizzative e figure coinvolte

Nell'ambito di tali Attività Sensibili, un ruolo preminente è svolto dalle funzioni aziendali che la Società ha identificato nel proprio organigramma della sicurezza, di seguito precisate:

- **Datore di lavoro**: definito dall'art. 2 comma 1 lett. b) D.Lgs. 81/2008 come *"il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa"*;

- **Preposti**: ovvero quelle persone che, in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico loro conferito, sovrintendono alla attività lavorativa e garantiscono l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa (vedi art. 2, comma 1 lett. e) D.Lgs. 81/2008);
- **Lavoratori**: definiti dall'art. 2, comma 1, lett. a) D.Lgs. 81/2008 come le *"persone che, indipendentemente dalla tipologia contrattuale, svolgono un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione"*;
- **Responsabile del Servizio di Prevenzione e Protezione** (di seguito anche ***"RSPP"***): definito dall'art. 2, comma 1 lett. f) D.Lgs. 81/2008 come la *"persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 del D.Lgs. 81/2008, designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi della Società"*;
- **Addetti prevenzione incendi e gestione delle emergenze**: lavoratori nominati dal datore di lavoro e chiamati a gestire le situazioni di emergenza reali e potenziali in azienda (rif. **All.** *"Piano d'Emergenza"*);
- **Addetti primo soccorso**: lavoratori designati dal datore di lavoro ed incaricati dell'attuazione delle misure di primo soccorso, del mantenimento e della verifica dei presidi di primo soccorso (rif. **All. -** *"Primo soccorso"*);

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

<u>Reati contro la Pubblica Amministrazione</u>

- Corruzione per l'esercizio della funzione (art. 318 Cod. Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- Induzione indebita a dare o promettere utilità (art. 319-*quater* c.p.);
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- Istigazione alla corruzione (art. 322 c.p.).

Reati di omicidio colposo o lesioni gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (art. 25-*septies* del D.Lgs. 231/01)

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose gravi o gravissime (art. 590, comma 3, c.p.).

Le potenziali modalità astratte di commissione dei reati in esame sono state oggetto di valutazione da parte dei responsabili della Società nella costruzione del presente Modello.

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda al *Risk Assesment* di riferimento "*Risk Assesment 231 – Reati in materia di Salute e Sicurezza sul Lavoro".*

- Formale attribuzione di ruoli, compiti e responsabilità, nel rispetto del principio di "segregation of duties".
- Attribuzione di ruoli e responsabilità circa la pianificazione, consuntivazione degli impegni di spesa e della relativa analisi degli scostamenti rispetto a quanto pianificato.
- Definizione delle modalità di rendicontazione e documentazione delle spese in materia di SSL.
- Tracciabilità delle analisi condotte circa l'effettiva realizzazione e attuazione degli impegni di spesa in materia di SSL.
- Identificazione dei soggetti cui è affidato il compito di garantire l'aggiornamento delle prescrizioni normative in materia di SSL.
- Diffusione degli aggiornamenti normativi in materia di SSL ai soggetti interessati.
- Identificazione formale dei soggetti cui sono affidati ruoli e responsabilità in materia di SSL e delle relazioni gerarchico - funzionali intercorrenti tra i diversi soggetti.
- Identificazione e formale designazione del RSPP, e definizione dei requisiti specifici, coerentemente con le disposizioni di legge, che devono caratterizzare tale figura.
- Tracciabilità delle verifiche svolte in ordine a garantire il possesso dei requisiti previsti dalla normativa prevenzionistica vigente.
- Tracciabilità della formale accettazione dell'incarico da parte del soggetto designato.

- Identificazione e formale designazione degli addetti alle emergenze e degli addetti al primo soccorso.
- Definizione dei requisiti specifici, coerentemente con le disposizioni di legge, che devono caratterizzare tali figure.
- Identificazione di regole formali a supporto del processo di valutazione dei rischi attraverso il coinvolgimento di tutte le figure previste dalla normativa prevenzionistica vigente.
- Formalizzazione di un Documento di Valutazione dei rischi conforme alle previsioni della normativa prevenzionistica vigente.
- Identificazione di regole formali per la gestione delle emergenze.
- Identificazione delle 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.
- Formalizzazione del Piano di Emergenza e di evacuazione.
- Definizione delle modalità, frequenza e tracciabilità delle prove di evacuazione periodiche e di simulazione delle situazioni di emergenza.
- Svolgimento periodico delle prove di evacuazione e di simulazione delle situazioni di emergenza.
- Svolgimento e tracciabilità delle riunioni periodiche in materia di SSL (Ex. Art. 35 del D.lgs. 81/08).
- Svolgimento di attività di revisione periodica da parte del management aziendale in materia di SSL che garantiscano l'appropriatezza e l'adeguatezza dei principi definiti rispetto ai rischi della Società.
- Identificazione di regole formali circa le modalità di informazione e formazione dei lavoratori relativamente alle tematiche in materia di SSL.
- Identificazione dei soggetti cui è affidata l'informazione e la formazione dei lavoratori circa le tematiche in materia di SSL.
- Identificazione di regole formali circa la gestione dell'informativa alle imprese esterne che svolgono lavori in appalto sui rischi specifici dell'ambiente in cui sono destinate a operare e sulle misure da adottare in relazione alle proprie attività.
- Identificazione di regole formali circa l'attribuzione le modalità di predisposizione e aggiornamento del Documento Unico di Valutazione dei rischi di interferenza (DUVRI).
- Identificazione formale dei soggetti responsabili della predisposizione, autorizzazione e aggiornamento del DUVRI.
- Gestione dei rischi da interferenza nelle aree comuni.
- Identificazione di regole formali circa la rilevazione, registrazione e investigazione degli infortuni.

- Identificazione di regole formali circa la tracciabilità e investigazione degli incidenti e dei "mancati incidenti".
- Definizione dei flussi informativi al Datore di Lavoro e agli altri soggetti aziendali coinvolti degli infortuni e incidenti occorsi.
- Tenuta ed aggiornamento del registro infortuni.
- Analisi del fenomeno incidentale e individuazione delle eventuali azioni preventive e correttive.

AREA A RISCHIO N. 6: GESTIONE DEGLI ACQUISTI

a) Attività Sensibili

In relazione alla presente Area a Rischio sono state identificate le seguenti attività:

- Gestione del *Budget*;
- Gestione delle attività di selezione e valutazione del fornitore;
- Gestione del listino prezzi con il fornitore;
- Gestione del processo di acquisto.

b) Funzioni aziendali /unità organizzative e figure coinvolte

Le Funzioni Aziendali / unità organizzative e figure coinvolte nello svolgimento delle attività sopra descritte sono:

- Presidente del Consiglio di Gestione;
- Direttore Sviluppo Programmi;
- Ufficio Acquisti;
- Ufficio Amministrazione.

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

- Reati contro la Pubblica Amministrazione o in danno dell'Unione Europea (Artt. 24 e 25 del D.Lgs. 231/01)
  - Corruzione per l'esercizio della funzione (art. 318 c. p.);
  - Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.),
  - Indebita induzione a dare o promettere utilità (art. 319 *quater*);
  - Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);

- Pene per il corruttore (art. 321 c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Traffico di influenze illecite (art. 346-*bis* c.p.).

- Delitti di criminalità organizzata (Art. 24-*ter* del D.Lgs. 231/01)
  - Associazione per delinquere (art. 416 c.p.);
  - Associazione di stampo mafioso (art. 416 *bis* c.p.).

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 *quater* del D.Lgs. 231/01)
  - Finanziamento al terrorismo (art. 2 Convenzione di New York).

- Reati Transnazionali (L. 146/2006)
  - Associazione per delinquere (art. 416 c.p.);
  - Associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.).

- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-*bis* del D.Lgs. 231/01)
  - Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

- Delitti contro l'industria ed il commercio (Art. 25-*bis* 1 del D.Lgs. 231/01)
  - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.).

- Reati societari (Art.25-*ter* del D.Lgs. 231/01)
  - Corruzione tra privati (art. 2635 c.c.);
  - Istigazione alla corruzione tra privati (art. 2635 *bis* c.c.).

- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (Art.25-*octies* del D.Lgs. 231/01)
  - Ricettazione (Art. 648 c.p.);
  - Riciclaggio (Art. 648 *bis* c.p.);
  - Impiego di denaro, beni o utilità di provenienza illecita (Art. 648 *ter* c.p.);
  - Autoriciclaggio (Art. 648 *ter* 1 c.p.).

- Reati tributari (art. 25 *quinquiesdecies* del D.Lgs. 231/01)

- Dichiarazione fraudolenta mediante fatture per operazioni inesistenti (art. 2 D.Lgs. 74/2000);
- Dichiarazione fraudolenta mediante altri artifizi (art. 3 D.Lgs. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. 74/2000).

- Delitti contro la personalità individuale (art. 25-*quinquies* del D.Lgs. 231/01)
  - Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.) (nella forma del concorso).

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda al *Risk Assessment* di riferimento).

- La Società ha adottato un proprio Codice di Condotta-Comportamento, all'interno del quale sono definiti i principi che ispirano la Sua azione nell'ambito dei rapporti con tutti gli *stakeholders*. All'interno di tale Codice sono state formalizzate specifiche previsioni riguardanti le fattispecie di reato previste dal D.Lgs. 231/01. I principi etici definiti dalla Società rientrano tra le materie oggetto del piano di informazione e formazione del personale.
- Le anagrafiche dei fornitori sono gestite tramite il ricorso alla Società Ausind srl, con la quale risulta in essere specifico contratto di collaborazione.
- I fabbisogni di approvvigionamento sono formalizzati attraverso la predisposizione di Richieste di Acquisto
- E' sistematicamente verificata la congruenza tra le Richieste di Acquisto e quanto previsto a budget.
- Eventuali spese di approvvigionamento che superino i limiti definiti dal budget aziendale sono sottoposte all'approvazione del Consiglio di Gestione.
- Sono definiti i criteri per la selezione competitiva delle offerte presentate dai fornitori di beni e servizi (es.mediante la richiesta di due o più offerte).
- Le assegnazioni dirette sono sottoposte all'approvazione del Consiglio di Gestione.
- I rapporti con i fornitori sono formalizzati tramite la stipula di ordini/accordi quadro/contratti formalmente autorizzati da soggetti dotati di adeguati poteri.
- Gli ordini effettuati nei confronti dei nuovi fornitori, prima della loro emissione, devono essere firmati per approvazione dal Presidente del Consiglio di Gestione.

- E' definito un processo di valutazione periodica delle performance dei fornitori.
- Le valutazioni delle performance dei fornitori sono considerate nel processo di qualifica e assegnazione di nuovi approvvigionamenti.
- E' verificata la conformità delle caratteristiche dei beni, lavori e servizi oggetto di acquisto, rispetto al contenuto dell'Ordine/ Contratto.
- SIIT S.c.p.A. ha adeguato il proprio comportamento a quanto esposto.

AREA A RISCHIO N. 7: GESTIONE DELLE TEMATICHE AMBIENTALI

a) Attività Sensibili

In relazione alla presente Area a Rischio sono state identificate le seguenti attività:

- Attività di identificazione, caratterizzazione e classificazione dei rifiuti;
- Attività di raccolta e gestione del deposito temporaneo dei rifiuti;
- Selezione e gestione dei fornitori per attività di trasporto e smaltimento dei rifiuti;
- Gestione delle autorizzazioni alle emissioni;
- Effettuazione delle emissioni;
- Gestione delle autorizzazioni agli scarichi idrici;
- Effettuazione degli scarichi idrici;
- Definizione di un piano di manutenzione ed ispezione degli asset durante il loro ciclo di vita;
- Definizione di un piano di manutenzione periodica degli impianti di raffreddamento e riscaldamento;
- Monitoraggio dello smaltimento relativo a sostanze nocive prodotte dagli impianti di riscaldamento e raffreddamento.

b) Funzioni aziendali /unità organizzative e figure coinvolte

Le Funzioni Aziendali / unità organizzative e figure coinvolte nello svolgimento delle attività sopra descritte sono:

- Presidente del Consiglio di Gestione;
- Direttore Sviluppo Programmi;
- RSPP.

c) Fattispecie di reato potenzialmente applicabili

Le fattispecie di reato che potrebbero potenzialmente essere realizzate nello svolgimento delle attività sopra menzionate sono:

- 25-undecies: Reati Ambientali (introdotto dal Decreto Legislativo n.121 del 7 luglio 2011) e aggiornato a seguito della Legge 68/2015 (Eco-reati):

  - Inquinamento Ambientale (art. 452 bis c.p.);
  - Disastro ambientale (art. 452 quater c.p.);
  - Reati in materia di Gestione non Autorizzata dei Rifiuti (art. 452 quinquies c.p.)
  - Attività organizzate per il traffico illecito di rifiuti (art 452 quaterdecies c.p.);
  - Sanzioni Penali in materia di scarichi di acque reflue (art 137 Codice dell'Ambiente).

d) Controlli Preventivi

In relazione al rischio di commissione dei reati sopra elencati, SIIT S.c.p.A. ha implementato il seguente sistema di controlli preventivi (per il dettaglio si rimanda al *Risk Assessment* di riferimento).

- La Società ha adottato un proprio Codice di Condotta-Comportamento, all'interno del quale sono definiti i principi che ispirano la Sua azione nell'ambito dei rapporti con tutti gli *stakeholders*. All'interno di tale Codice sono state formalizzate specifiche previsioni riguardanti le fattispecie di reato previste dal D.Lgs. 231/01. I principi etici definiti dalla Società rientrano tra le materie oggetto del piano di informazione e formazione del personale.
- Sono svolte da parte del RSPP e dalle figure aziendali dotate di adeguati poteri le attività di monitoraggio relative alle novità normative inerenti le tematiche ambientali.
- La Società svolge attività di identificazione, caratterizzazione e classificazione dei rifiuti prodotti.
- Sono svolte attività specifiche di raccolta, gestione e deposito temporaneo dei rifiuti.
- Le attività di trasporto e smaltimento dei rifiuti sono affidate ad aziende qualificate, attive nel settore.
- Sono svolte dalla Società attività di monitoraggio relativamente agli scarichi di acque reflue, di natura domestica ed igienico sanitaria, e relativamente alle emissioni, per valutare se periodicamente vi siano elementi che debbano essere oggetto di segnalazione alle autorità competenti.

- Sono svolte periodiche attività di monitoraggio relative agli asset aziendali, al fine di garantirne il corretto utilizzo, integrità ed adeguatezza in termini di rispetto della tutela aziendale.
- Sono monitorate con l'ausilio del RSPP le attività di manutenzione degli asset aziendali durante il loro ciclo di vita ed utilizzo.
- Lo smaltimento di eventuali asset aziendali (quali pc, stampanti, ed altri strumenti ad essi assimilati), o di parti integranti degli stessi, viene monitorato, ed affidato ad aziende qualificate ed attive nel settore.
- Sono svolte dalla Società attività di monitoraggio e supervisione costante in merito ai sistemi di riscaldamento e raffreddamento degli ambienti aziendali, gestiti a livello centralizzato nello stabile di riferimento, per quanto riguarda la corretta manutenzione.