Modello di organizzazione, gestione e controllo

ex Decreto Legislativo 8 giugno 2001 n. 231 e s.m.i.

di S.I.T.O S.p.A

Adottato dal Consiglio di Amministrazione del 20/11/2006

Revisione	Data	Redatto e Verificato da	Approvato da	Note
REV. 01	13.01.2009	Organismo di Vigilanza	Consiglio di Amministrazione	Integrazione nel MOG del Sistema di Gestione per la Sicurezza
REV. 02	30.01.2014	Responsabile delle Prevenzione della Corruzione	Consiglio di Amministrazione	Integrazione art. 14, implementazione con il Piano di Prevenzione della Corruzione
REV. 03	18.12.2014	Advisor Studio Vernero Manavella & Associati in collaborazione con l'Organismo di Vigilanza	Consiglio di Amministrazione	Aggiornamento del MOG
REV. 04	26.06.2015	Responsabile delle Prevenzione della Corruzione	Consiglio di Amministrazione	Aggiornamento catalogo reati Aggiornamento del Piano di prevenzione della corruzione Adozione del Programma triennale per la trasparenza e integrità
REV. 05	29.09.2016	Advisor Studio Vernero Manavella & Associati in collaborazione con l'Organismo di Vigilanza	Consiglio di Amministrazione	Aggiornamento del MOG

INDICE

PARTE GENERALE 6
1.Il Decreto Legislativo 231/2001 6
1.1 Fattispecie di reato 7
1.2 Apparato sanzionatorio 9
1.3 Modelli di organizzazione, gestione e controllo 10
2.Il Codice Etico della Società S.I.TO S.p.A 11
2.1 Normativa anticorruzione 11
3.Il Modello di S.I.TO S.p.A 12
3.1 Costruzione e scopo del Modello 12
3.2 La funzione e le caratteristiche generali del Modello 13
3.3 Struttura del Modello 14
3.4 L'adozione del Modello ed il suo aggiornamento 14
4.L'Organismo di Vigilanza 16
4.1. Composizione, requisiti, poteri, nomina e revoca dell'Organismo di Vigilanza 16
4.2. Cause di ineleggibilità, revoca, recesso e rinuncia dei componenti dell'OdV 17
4.3 Funzioni e poteri dell'Organismo di Vigilanza 18
4.4 Flussi informativi da/verso l'Organismo di Vigilanza 19
4.5 Attività di reporting dell'Organismo di Vigilanza 21
4.6 Raccolta e conservazione delle informazioni 22
5.La diffusione del Modello e formazione del personale 23
5.1 Formazione ed informazione del personale dipendente 23
5.2 Formazione e informazione agli Amministratori e al Collegio Sindacale 24
5.3 Informazione ai collaboratori, fornitori, consulenti e altri soggetti terzi 24
6. Il sistema disciplinare 25
6.1 Principi generali 25
6.2 Il sistema disciplinare nei confronti dei lavoratori dipendenti 25
6.3 Misure nei confronti dei dirigenti 26
6.4 Misure nei confronti degli Amministratori e dei Sindaci 26

6.5 Misure nei confronti dei collaboratori, fornitori, consulenti e altri soggetti terzi 26
7.Reati rilevanti e Aree sensibili in S.I.TO S.p.A 27
PARTE SPECIALE 1 35
Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*) 35
PARTE SPECIALE 2 39
Delitti informatici e trattamento illecito di dati (art. 24 *bis*) 39
PARTE SPECIALE 3 42
Reati societari (art. 25 *ter*) 42
PARTE SPECIALE 4 45
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies*) 45
4.1. Il Sistema di gestione per la sicurezza e salute sul lavoro (S.G.S.L.) 51
4.1.a) Elementi del sistema di gestione per la salute e sicurezza nei luoghi di lavoro 54
4.1.b) Pianificazione per l'identificazione del pericolo, valutazione e controllo del rischio 56
4.1.c) Identificazione dei rischi per la sicurezza e la salute 57
4.1.d) Requisiti legali e di altra natura 61
4.1.e) Obiettivi 61
4.1.f) Programma di gestione per la salute e sicurezza nei luoghi di lavoro 62
4.1.g) Attuazione e funzionamento: struttura e responsabilità 62
4.1.h) Attuazione e funzionamento: addestramento, consapevolezza e competenza 63
4.1.i) Attuazione e funzionamento: consultazione e comunicazione 63
4.1.l) Documentazione e controllo dei dati e dei documenti 64
4.1.m) Controllo operativo 65
4.1.n) Preparazione e risposta alle emergenze 66
4.1.o) Azioni correttive e di controllo: misurazione e monitoraggio delle prestazioni 67
4.1.p) Azioni correttive e di controllo: infortuni, incidenti, azioni correttive e preventive 67
4.1.q) Azioni correttive e di controllo: registrazioni e loro gestione 68
4.1.r) Azioni correttive e di controllo: audit 68
4.1.s) Riesame 70
4.1.t) Riesame: modalità operativa 71

PARTE SPECIALE 5 73
Delitti in materia di violazione del diritto d'autore (art. 25 *nonies*) 73
PARTE SPECIALE 6 74
Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 *octies*) 74
PARTE SPECIALE 7 76
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies*) 76
PARTE SPECIALE 8 77
Reati ambientali (art. 25 – *undecies*) 77
PARTE SPECIALE 9 79
Piano Triennale di Prevenzione della Corruzione (P.T.P.C.) 79
9.1 Quadro normativo 80
9.1.1 Ambito soggettivo di applicazione 80
9.1.2 Sanzioni 81
9.2 Il Piano triennale per la prevenzione della corruzione di Sito S.p.A 82
9.2.1 Rapporti con il Modello organizzativo ex d.lgs. 231/2001 82
9.2.2 Procedura per l'aggiornamento del Piano di Sito S.p.A 82
9.3 Responsabile per la prevenzione della corruzione e trasparenza 83
9.4 Individuazione dei rischi 86
9.4.1 Fattispecie di reato rilevanti in Sito S.p.A 86
9.5 Misure per la gestione del rischio 90
9.5.1 Regolamenti e direttive 90
9.5.2 Procedure 90
9.5.3 Sistemi di controllo 91
9.5.4 Incompatibilità e inconferibilità per gli incarichi di amministratore e di dirigente 91
9.5.6 Selezione del personale 92
9.6 Gli adempimenti in materia di trasparenza in S.I.T.O S.p.A. 93
9.6.1 Principi generali della trasparenza in S.I.TO S.p.A. 93
9.6.2 Ruoli e responsabilità 93

9.6.3 Società Trasparente 94
9.6.4 Accesso civico 96
9.7 Codice di comportamento 98
9.8 Formazione 99
9.9 Flussi informativi e tutela dei "whistleblowers" 100
9.11 Sistema disciplinare 101
9.12 Programmazione triennale 102

PARTE GENERALE

1.Il Decreto Legislativo 231/2001

Con il decreto legislativo 8 giugno 2001 n. 231 (di seguito anche "Decreto"), emanato in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 300[1] è stata dettata la disciplina della "responsabilità degli enti per gli illeciti amministrativi dipendenti da reato".

Tale disciplina si applica agli enti dotati di personalità giuridica, nonché alle società e associazioni anche prive di personalità giuridica.

Il D.Lgs. 231/01 trova la sua genesi in alcune convenzioni internazionali e comunitarie ratificate dall'Italia che impongono di prevedere forme di responsabilità degli enti collettivi per talune fattispecie di reato.

Quanto poi al profilo soggettivo, il Legislatore, all'articolo 5 del Decreto, prevede la responsabilità dell'ente qualora il reato sia commesso da:

a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (c.d. "*apicali*");

b) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (c.d. "*sottoposti*").

Costoro devono aver agito nell'interesse o a vantaggio – anche non esclusivo – dell'ente stesso.

Per quanto attiene alla nozione di "interesse", esso si concretizza ogniqualvolta la condotta illecita sia posta in essere con l'i**ntento** di far conseguire un beneficio alla società o all'ente, indipendentemente dalla circostanza che tale obiettivo sia stato conseguito.

Alternativamente la responsabilità può ricadere sulla persona giuridica ogniqualvolta l'autore dell'illecito, pur non avendo agito al fine di beneficiare quest'ultima, le abbia comunque fatto conseguire un "**vantaggio**" economico o di altra natura.

[1] Il D.lgs. 231/01 è pubblicato sulla Gazzetta Ufficiale del 19 giugno 2001, n. 140, la Legge 300/2000 sulla Gazzetta Ufficiale del 25 ottobre 2000, n. 250.

La responsabilità amministrativa dell'ente è invece esclusa, per espressa previsione legislativa (art. 5, comma 2, del D.Lgs. 231/01), se i soggetti apicali e/o i loro sottoposti hanno agito nell'i**nteresse esclusivo** proprio o di terzi[2].

La responsabilità amministrativa delle persone giuridiche è comunque autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato. Ai sensi dell'art. 8, comma 1 del Decreto, la responsabilità dell'ente sussiste anche quando:

a) l'autore del reato non è stato identificato o non è imputabile;

b) il reato si estingue per una causa diversa dall'amnistia.

La responsabilità amministrativa dell'ente è collegata alla commissione – da parte dei soggetti di cui sopra – degli specifici reati presupposto previsti dal Decreto"[3].

La responsabilità amministrativa dell'ente può essere esclusa ai sensi dell'art. 6, comma 1 del Decreto se:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

È inoltre previsto ai sensi dell'**art. 6, comma 4** del Decreto che, negli enti di piccole dimensioni, le riferite funzioni di vigilanza possano essere assunte direttamente dall'organo dirigente.

1.1 Fattispecie di reato

Le fattispecie di reato oggi suscettibili di configurare la responsabilità amministrativa dell'ente, se commessi nel suo interesse o a suo vantaggio dai soggetti sopra menzionati, sono espressamente richiamate dagli artt. 24, 24-*bis*, 24-*ter*, 25, 25-*bis*, 25-*bis.1*, 25-*ter*, 25-*quater,* 25-*quater.1,* 25-

[2] Art. 5, comma 2, del D.lgs. 231/01: "Responsabilità dell'ente – L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi".
[3] Per l'elenco completo dei reati si veda il paragrafo successivo, nonché l'Allegato 1 al presente Modello.

quinquies, 25-*sexies*, 25-*septies,* 25-*octies,* 25-*novies,* 25-*decies,*25-*undecies e* 25-*duodecies* del D.Lgs. 231/2001, nonchè dalla L. 146/2006.

Tali fattispecie di reato possono essere comprese, per comodità espositiva, nelle seguenti categorie:

Reati contro la Pubblica Amministrazione (art. 24 e 25)
Reati informatici (art. 24 bis)
Criminalità organizzata (art. 24-ter) e reati transnazionali (art. 10 L. 146/2006)
Falsità documentali (art. 25-*bis*)
Delitti contro l'industria e il commercio (art. 25-*bis*.n.1)
Reati societari (art. 25 *ter*)
Delitti con finalità di terrorismo (art. 25-*quater*)
Infibulazione femminile (art. 25-*quater* n. 1)
Tratta di persone (art. 25 - *quinquies*)
Market abuse (art. 25-*sexies*)
Omicidio colposo o lesioni in violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies)*
Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro o altra utilità di provenienza illecita (art. 25 *octies*)
Delitti in materia di violazione del diritto d'autore (art. 25 *novies*)
Induzione a non rendere dichiarazioni (art. 25-*decies*)
Reati ambientali (art. 25-*undecies*)
Impiego di lavoratori irregolari (art. 25 *duodecies*)

Per il dettaglio dei reati di cui sopra si rinvia all' **Allegato A**.

1.2 Apparato sanzionatorio

Qualora venga accertata la responsabilità dell'ente, in conseguenza della commissione o tentata commissione dei reati sopra menzionati, sono comminabili, ai sensi dell'art. 9 del Decreto, le seguenti sanzioni:

- sanzione pecuniaria, calcolata tramite un sistema basato su quote, che vengono determinate dal giudice nel numero e nell'ammontare, entro limiti definiti per legge[4]. La sanzione può variare da un minimo di 100 quote (pari ad un minimo di € 25.822,84) ad un massimo di 1000 quote (pari ad un massimo € 1.549.370,70) (aumentabile fino a 10 volte nel caso di abusi di mercato);
- sanzioni interdittive (applicabili anche in via cautelare) di durata non inferiore a tre mesi e non superiore a due anni (con la precisazione che, ai sensi dell'art. 14, comma 1, D.lgs. 231/01, "*Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente*") che, a loro volta, possono consistere in:
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
  - esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
  - divieto di pubblicizzare beni o servizi;
- confisca (e sequestro preventivo in sede cautelare);
- pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

[4] Ai sensi dell'art.10, c.3, D.Lgs. 231/2001: "*L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni*."
L'importo di una quota perciò può variare da un minimo di € 250,23 ad un massimo di € 1549,37.

1.3 Modelli di organizzazione, gestione e controllo

Il Decreto prevede una specifica forma di esimente dalla suddetta responsabilità amministrativa, qualora l'ente dimostri di aver adottato ed efficacemente attuato misure organizzative idonee a prevenire la commissione dei "reati presupposto" da parte dei soggetti "apicali" o "sottoposti" che operano nel suo interesse o vantaggio.

La presenza di un'adeguata organizzazione è, infatti, misura e segno della diligenza dell'ente nello svolgimento delle proprie attività, con particolare riferimento a quelle in cui si manifesta il rischio della commissione dei "reati presupposto" previsti dal Decreto.

L'accertata esistenza di un'efficiente ed efficace organizzazione di impresa esclude, dunque, la "colpa in organizzazione" dell'ente e fa venir meno la necessità di sanzionarlo mediante l'applicazione delle previste e riferite sanzioni.

Gli ultimi due commi dell'**articolo 7** del Decreto dettano i criteri generali per la costruzione di un simile modello di organizzazione e gestione, tanto nel rilievo contenutistico che funzionale.

Lo stesso, infatti, in relazione alla natura ed alle dimensioni dell'organizzazione dell'ente, nonché al tipo di attività svolta, deve prevedere misure idonee a garantire lo svolgimento delle attività sociali dell'ente medesimo nel rispetto della legge, nonché misure atte a rilevare ed eliminare tempestivamente le situazioni di rischio. Inoltre, la sua efficace attuazione richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando intervengono mutamenti normativi o cambiamenti nell'organizzazione o nell'attività dell'ente stesso, ovvero quando vengono rilevate significative violazioni delle prescrizioni;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione e gestione.

Ulteriori indicazioni utili alla costruzione dei modelli organizzativi sono le linee guida delle associazioni di categoria e in particolare le linee guida predisposte da Confindustria[5].

Va inoltre precisato che il modello organizzativo rappresenta un elemento "positivo" nel calcolo del "*rating* di impresa" così come introdotto dall'art. 83, comma 10, del D.Lgs. 50/2016 e recepito dall'Autorità Nazionale Anticorruzione.

[5] Linee guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231, aggiornate al 2014.

2.Il Codice Etico della Società S.I.TO S.p.A

Le norme di comportamento contenute nel presente Modello sono coerenti con quelle indicate nel Codice Etico. Lo stesso è stato successivamente modificato e nuovamente approvato mediante delibera del Consiglio di Amministrazione in vigore.

Il Codice Etico è stato elaborato al fine di promuovere ed evidenziare i principi deontologici di diligenza, correttezza, lealtà e trasparenza a cui la Società si ispira con riferimento non solo alla conduzione della propria attività sociale, ma anche con riferimento ai rapporti intrattenuti con altri individui e/o Organizzazioni.

Il Codice identifica ed esprime gli impegni e le responsabilità etiche che la Società assume nella conduzione degli affari e delle attività assunte da tutti i partecipanti della Società medesima.

Il Codice rappresenta l'insieme di quei principi sostanziali la cui osservanza è di fondamentale importanza per il perseguimento degli obiettivi, l'affidabilità della gestione, la reputazione e l'immagine della Società.

2.1 Normativa anticorruzione

Alla luce della L. 190/2012 e delle varie delibere, circolari e determine dell'ANAC (con particolare riguardo alla Determina 8/2015 e al Piano Nazionale Anticorruzione 2016), i modelli di organizzazione gestione e controllo adottati dagli enti controllati o partecipati dalle Pubbliche Amministrazioni sono, altresì, funzionali agli adempimenti legati alla prevenzione della corruzione.

La legge 190/2012 disciplina un complesso sistema di prevenzione e repressione della corruzione e dell'illegalità nella pubblica amministrazione, nell'ambito del quale è previsto che gli enti controllati dalla P.A adottino un apposito Piano di prevenzione della corruzione (art. 1, commi 5, 8, 9, 10, 12).

A tale proposito, l'ANAC ha precisato l'esigenza di tenere conto della necessità di coordinamento tra quanto previsto nella Legge 190/2012 con le disposizioni del D.Lgs. 231/2001, prevedendo che i Piani di prevenzione della corruzione possano "fare perno" sul Modello 231 eventualmente adottato dall'ente.

3.Il Modello di S.I.TO S.p.A

3.1 Costruzione e scopo del Modello

La Società ha inizialmente adottato con delibera del Consiglio di Amministrazione del 20 novembre 2006 il Modello Organizzativo conformemente al D.Lgs. 231/2001, ed in specie agli articoli 6 e 7 del medesimo, in quanto trattasi di un sistema strutturato e organico di procedure nonché di attività di controllo volto a prevenire la commissione delle diverse tipologie di reato contemplate dal D.Lgs. 231/2001 e successive modifiche.

Il successivo processo di revisione del Modello Organizzativo, avviato a gennaio 2014, si è articolato nelle seguenti fasi:

- "*As-Is Analysis*": revisione dei processi e/o delle aree aziendali significative ai fini della prevenzione dei reati presupposto e identificazione delle modalità con le quali si possono realizzare gli illeciti (individuazione dei processi e delle Aree Sensibili);
- "*Gap Analysis*": individuazione delle possibili azioni di miglioramento del sistema di gestione e di controllo interno (processi e procedure) già esistenti e dei requisiti organizzativi essenziali per la definizione di un Modello "specifico";
- "*Refresh* del Modello": implementazione del Modello in linea con la *best practice* esistente in materia e in coerenza con i Codici di Comportamento redatti dalle Associazioni rappresentative degli Enti e comunicati al Ministero della Giustizia ai sensi dell'art. 6, comma 3 del D.Lgs. 231/2001;
- "Adozione formale del Modello aggiornato": formale adozione del Modello da parte del Consiglio di Amministrazione.

I principi fondamentali su cui si basa il Modello sono i seguenti:

- quelli richiamati al comma 2 dell'art. 6 del D.Lgs. 231/2001 ed in particolare:
  - individuazione delle attività esposte al rischio di commissione di reati;
  - previsione di specifici protocolli per programmare la formazione e l'attuazione delle decisioni della Società in funzione della prevenzione del rischio (ossia in relazione ai reati da prevenire);
  - individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
  - previsione di obblighi di informazione nei confronti dell'Organismo di Vigilanza sul funzionamento e l'osservanza del Modello;

- introduzione di un adeguato sistema disciplinare per sanzionare il mancato rispetto delle misure indicate nel Modello;

- quelli richiamati dalle Linee Guida di Confindustria;
- quelli sanciti dal Codice Etico della Società;
- i principi generali di un adeguato Sistema di Controllo Interno ed in particolare:
  - la verificabilità e documentabilità di ogni operazione rilevante ai fini del D.Lgs. 231/2001;
  - il rispetto del principio della separazione delle funzioni e delle responsabilità e della correlata segregazione dei compiti;
  - la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;

Alla luce di tali principi la Società ha avviato:

- la mappatura del rischio reato seguita dall'individuazione di specifiche Aree Sensibili nel cui ambito vi è la possibilità di commissione di un reato *ex* D.Lgs. 231/2001;
- un'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- la nomina di un Organismo di Vigilanza a cui sono stati attribuiti specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;

Per un'efficace attuazione di tale sistema, sono stati previsti, in particolare:

- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la formalizzazione di procedure dirette a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
- l'individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione di reati *ex* D.Lgs. 231/2001;
- specifici obblighi di informazione nei confronti dell'Organismo di Vigilanza.

3.2 La funzione e le caratteristiche generali del Modello

Il Modello Organizzativo predisposto dalla Società si fonda su un complesso di procedure e controlli posti a tutela delle attività aziendali potenzialmente esposte alla commissione dei reati contemplati dal D.Lgs. 231/2001.

Obiettivi del Modello Organizzativo sono:

- prevenire ovvero rendere residuo il rischio di commissione di reati-presupposto *ex* D.Lgs. 231/2001;

- informare coloro che operano nelle aree sensibili sulle conseguenze sanzionatorie della commissione di reati e della violazione del Modello applicabili nei loro confronti e nei confronti della Società.

Lo scopo del Modello è quindi quello di predisporre un sistema strutturato e organico di prevenzione, dissuasione e vigilanza finalizzato alla riduzione del rischio di commissione dei reati-presupposto mediante l'individuazione delle aree sensibili e la conseguente regolamentazione dei processi sensibili. Tale sistema detta regole e prevede procedure che la Società si impegna a far rispettare al fine di migliorare le regole di *governance* societarie e gli assetti organizzativi esistenti e ridurre il rischio di commissione dei reati previsti dal D.Lgs. 231/2001.

3.3 Struttura del Modello

Il Modello di SITO S.p.A. è così strutturato:

- **PARTE GENERALE**
- **PARTI SPECIALI:**

- **PARTE SPECIALE 1:** Reati nei rapporti con la Pubblica Amministrazione, corruzione fra privati e delitti di criminalità organizzata;
- **PARTE SPECIALE 2:** Delitti informatici e trattamento illecito dei dati societari;
- **PARTE SPECIALE 3:** Reati Societari;
- **PARTE SPECIALE 4:** Delitti derivanti dalle violazioni in materia di Sicurezza e Salute dei lavoratori;
- **PARTE SPECIALE 5:** Delitti in materia di violazione del diritto di autore;
- **PARTE SPECIALE 6:** Ricettazione, riciclaggio, autoriciclaggio, impiego di denaro, beni o utilità di provenienza illecita;
- **PARTE SPECIALE 7:** Impiego di cittadini di paesi terzi cui soggiorno è irregolare;
- **PARTE SPECIALE 8:** Reati ambientali;
- **PARTE SPECIALE 9:** Piano di Prevenzione della Corruzione.

3.4 L'adozione del Modello ed il suo aggiornamento

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, la Società ha deciso in data 20 novembre 2006 di dotarsi di tale Modello con apposita delibera del Consiglio di Amministrazione.

Il Modello Organizzativo è uno strumento dinamico suscettibile di implementazioni, modifiche ed aggiornamenti. A seguito dell'adozione del Modello, quindi, anche dietro impulso dell'Organismo di Vigilanza, lo stesso dovrà essere rivisto, indicativamente ogni qual volta si verifichi un evento che palesi l'esigenza di integrazione con nuove e migliori procedure o un mutamento strutturale dell'Ente che comporti un aggiornamento del Modello ovvero una modifica normativa rilevante ai fini della responsabilità amministrativa dell'Ente (mappatura costante/periodica del rischio).

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità all'articolo 6, comma 1, lettera a) del D.Lgs. 231/2001), le modifiche ed integrazioni di carattere sostanziale che dovessero rendersi necessarie per i motivi di cui sopra, sono rimesse alla competenza del Consiglio di Amministrazione della Società.

Le procedure, richiamate nel presente Modello e che completano e integrano i protocolli previsti nelle Parti Speciali, sono soggette ad autonome modifiche ad opera dei responsabili di area, anche in conseguenza dell'attività di controllo circa la loro adeguatezza che verrà svolto dall'Organismo di Vigilanza.

É attribuito all'Organismo di Vigilanza il potere di proporre modifiche al Modello stesso o ai documenti ad esso correlati, quali esemplificativamente:

- l'introduzione di nuove procedure e controlli nel caso in cui non sia sufficiente una revisione di quelle esistenti;
- la revisione dei documenti aziendali e societari che formalizzano l'attribuzione delle responsabilità e dei compiti alle posizioni responsabili di strutture organizzative "sensibili" o comunque che svolgono un ruolo di snodo nelle attività a rischio;
- l'introduzione di ulteriori controlli delle attività sensibili, con formalizzazione delle iniziative di miglioramento intraprese in apposite procedure;
- l'evidenziazione delle esigenze di modifica di regole di carattere generale.

4.L'Organismo di Vigilanza

4.1. Composizione, requisiti, poteri, nomina e revoca dell'Organismo di Vigilanza

L'art. 6 del D.Lgs. 231/2001 prevede che il compito di vigilare sul funzionamento, l'osservanza e l'aggiornamento del modello organizzativo spetti a un organismo interno alla società dotato di autonomi poteri di iniziativa e controllo denominato Organismo di Vigilanza.

Possono essere nominati quali membri dell'Organismo di Vigilanza coloro che posseggono i seguenti requisiti:

- autonomia e indipendenza: l'Organismo di Vigilanza non deve essere direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo;
- professionalità: i componenti dell'Organismo di Vigilanza hanno competenze tecnico-professionali adeguate alle funzioni che sono chiamati a svolgere;
- onorabilità: è assicurata dall' inesistenza, sia al momento della nomina che per tutta la durata dell'incarico, delle cause di ineleggibilità di cui al paragrafo 4.2;
- continuità di azione: l'Organismo di Vigilanza (i) deve svolgere in modo continuativo le attività necessarie per la vigilanza del Modello Organizzativo con adeguato impegno e con i necessari poteri di indagine; (ii) è una struttura riferibile alla Società, in modo da garantirne la dovuta continuità nell'attività di vigilanza; (iii) cura l'attuazione del Modello Organizzativo e ne assicura il costante aggiornamento; (iv) non svolge mansioni operative che possono condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

La composizione dell'Organismo di Vigilanza non può dunque prescindere dalla sussistenza dei requisiti sopra esposti.

Inoltre ai sensi del sopracitato art. 6, l'Organismo di Vigilanza deve essere dotato di autonomi poteri di iniziativa e controllo e quindi:

- è inserito all'interno dell'organizzazione societaria quale organo di staff rispetto al Cda;
- allo stesso è riconosciuta l'indipendenza gerarchica rispetto agli altri organi societari;
- è dotato di autonomia finanziaria.

In caso di necessità l'Organismo di Vigilanza dovrà richiedere preventivamente al Presidente e al Vice Presidente i fondi necessari all'espletamento delle proprie attività volte al corretto svolgimento dei compiti e potrà avere la possibilità di avvalersi di consulenti esterni, previa informativa congiunta al Presidente e al Vice Presidente.

La composizione dell'Organismo di Vigilanza può essere di tipo monocratico ovvero plurisoggettivo (da 2 a 5 membri). Possono farne parte sia soggetti interni alla società che soggetti esterni. In caso di composizione mista il grado di indipendenza dell'Organismo di Vigilanza dovrà essere valutato nella sua collegialità.

Nel caso di composizione plurisoggettiva l'Organismo di Vigilanza nomina un Presidente che deve essere scelto tra i membri esterni.

L'Organismo di Vigilanza, per lo svolgimento dei propri compiti, potrà avvalersi del supporto delle funzioni aziendali della Società ritenute utili.

È di competenza del Consiglio di Amministrazione, oltre alla nomina e alla scelta della composizione dell'Organismo di Vigilanza, anche la revoca dello stesso.

Lo stesso Consiglio di Amministrazione provvede alle necessarie sostituzioni in caso di dimissioni dell'Organismo di Vigilanza e/o di mutamenti organizzativi.

4.2. Cause di ineleggibilità, revoca, recesso e rinuncia dei componenti dell'OdV

Non potranno essere eletti quali componenti dell'Organismo di Vigilanza:

- soggetti legati alla Società o a membri degli organi sociali da rapporti di qualsivoglia natura tali da generare conflitti di interessi;
- soggetti che non sono dotati dei necessari requisiti di autonomia, indipendenza, professionalità e onorabilità;
- soggetti che sono o sono stati sottoposti a misure di prevenzione antimafia così come previsto dall'art. 85 D.Lgs. 159/2011;
- soggetti che hanno riportato una sentenza di condanna passata in giudicato, ad una pena che comporti l'interdizione, anche temporanea dai pubblici uffici, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche ovvero la sospensione dall'esercizio di una professione;
- soggetti che hanno riportato una sentenza di condanna passata in giudicato per uno dei reati previsti dal D.Lgs. 231/2001.

Il Consiglio di Amministrazione può revocare in qualsiasi momento, per giusta causa, uno o più membri dell'Organismo di Vigilanza al verificarsi di una delle seguenti condizioni:

- perdita dei requisiti di eleggibilità ovvero mancanza originaria degli stessi;

- l'interdizione, l'inabilitazione, ovvero una grave infermità che renda uno o più componenti dell' Organismo di Vigilanza inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti l'assenza dal luogo di lavoro per un periodo continuativo superiore a sei mesi;
- perdita dei requisiti di autonomia, indipendenza, professionalità e onorabilità;
- la mancata partecipazione, senza giustificato motivo, a due o più riunioni anche non consecutive nel corso di un anno;
- una sentenza di condanna della Società ai sensi del D.Lgs. 231/2001 passata in giudicato, ovvero un procedimento penale concluso tramite il c.d. patteggiamento, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del suddetto Decreto.

Ogni componente dell'Organismo di Vigilanza può in qualsiasi momento recedere dall'incarico, previo preavviso di almeno 3 mesi.

Nei casi di (i) rinuncia, (ii) sopravvenuta incapacità, (iii) morte, (iv) revoca o (v) decadenza di un componente dell'Organismo di Vigilanza, l'Organismo stesso dovrà darne immediata comunicazione al Consiglio di Amministrazione e al Collegio Sindacale. Il Consiglio di Amministrazione provvederà senza indugio a nominare dei nuovi componenti dell'Organismo di Vigilanza.

4.3 Funzioni e poteri dell'Organismo di Vigilanza

È compito dell'Organismo di Vigilanza:

- vigilare sul funzionamento e l'osservanza del Modello;
- verificare l'effettiva idoneità del Modello e delle procedure esistenti a prevenire la commissione dei reati richiamati dal D.Lgs. 231/2001;
- curare, sviluppare e promuovere, in collaborazione con le funzioni aziendali interessate, il costante aggiornamento del Modello e del sistema di vigilanza sull'attuazione dello stesso, suggerendo, ove necessario, all'organo dirigente gli aggiornamenti necessari;
- mantenere i rapporti e assicurare i flussi informativi verso il Consiglio di Amministrazione ed il Collegio Sindacale;
- compiere verifiche ed ispezioni al fine di accertare eventuali violazioni del Modello;
- elaborare un programma di vigilanza, in coerenza con i principi contenuti nel Modello, sulle attività a rischio;
- assicurare l'attuazione del programma di vigilanza anche attraverso la calendarizzazione delle attività;

- assicurare l'elaborazione della reportistica sulle risultanze degli interventi effettuati;
- condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura dei Processi Sensibili;
- definire e promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché della formazione del personale e della sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
- interpretare la normativa rilevante e verificare l'adeguatezza del Modello alle prescrizioni;
- fornire chiarimenti in merito al significato ed all' applicazione delle previsioni contenute nel Modello;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere allo stesso trasmesse o tenute a sua disposizione;
- monitorare ed eventualmente implementare un efficace sistema informativo interno per consentire la trasmissione e raccolta di notizie rilevanti ai fini del D.Lgs. 231/2001;
- formulare la previsione di spesa per lo svolgimento della propria attività da sottoporre all'approvazione del Consiglio di Amministrazione (eventuali spese straordinarie, non contemplate nel documento previsionale, dovranno essere parimenti sottoposte alla preventiva approvazione del Consiglio di Amministrazione);
- promuovere l'attivazione di eventuali procedimenti disciplinari.

L'Organismo di Vigilanza, provvede alla redazione e approvazione di un proprio Regolamento conforme a quanto previsto dal presente Modello. Tale documento avrà come obiettivo quello di definire l'attività, le funzioni, i poteri e le modalità di funzionamento dell'Organismo medesimo. Una volta provveduto alla sua redazione ed approvazione formale da parte dei membri dell'Organismo di Vigilanza, il Regolamento dovrà essere trasmesso al Consiglio di Amministrazione per presa d'atto.

4.4 Flussi informativi da/verso l'Organismo di Vigilanza

Come disposto dall'art. 6 comma 2 lettera d) del Decreto, il presente Modello deve rispondere all'esigenza di prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato alla vigilanza sul funzionamento e osservanza del Modello.

Pertanto, all'Organismo di Vigilanza devono pervenire, da parte dei destinatari del presente Modello, *in primis* da parte degli Organi Sociali, dei referenti delle aree sensibili e, a seguire, da parte di tutti gli altri soggetti coinvolti (*i.e.* dipendenti, consulenti ed eventuali Partners), tutte le informazioni relative ad eventi che potrebbero determinare per la Società una responsabilità *ex* D.Lgs. 231/2001 ovvero a

violazioni delle regole societarie, del presente Modello, delle procedure e del Codice Etico. A tal fine l'organo amministrativo deve prevedere idonei e specifici strumenti, procedure e canali di informazione e comunicazione (*i.e.* specifica casella di posta elettronica).

Debbono inoltre ritenersi quali flussi informativi verso l'Organismo di Vigilanza anche:

- l'invio delle convocazioni e degli ordini del giorno dei Consigli di Amministrazione e delle Assemblee;
- l'invio di copia dei verbali delle riunioni delle Assemblee, dei Consigli di Amministrazione e del Collegio Sindacale.

I flussi informativi, come sopra descritti, costituiscono (secondo le Linee Guida di Confindustria) un ulteriore strumento per agevolare l'attività di vigilanza dell'Organismo di Vigilanza in merito all'efficacia del Modello Organizzativo e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi del reato – presupposto *ex* D.Lgs. 231/2001.

I suddetti flussi informativi possono essere così schematizzati:

- flussi indirizzati all'Organismo di Vigilanza:
  - flussi periodici e report dalle aree sensibili;
  - flussi al verificarsi di particolari eventi;
- flussi provenienti dall'Organismo di Vigilanza:
  - informativa periodica/continuativa al Consiglio di Amministrazione;
  - informativa periodica, con cadenza almeno annuale al Collegio Sindacale che può consistere anche in un incontro verbalizzato;
  - informativa al verificarsi di particolari eventi.

Alla luce dell'approvazione del Piano di prevenzione della Corruzione (**PARTE SPECIALE 9**) e delle competenze in parte sovrapponibili tra Organismo di Vigilanza e Responsabile per la prevenzione della corruzione, è necessario prevedere un flusso informativo biunivoco (sia periodico che ad evento) tra tali funzioni.

Salvo il caso di calunnia o diffamazione, il soggetto che segnala all'Organismo di Vigilanza ipotesi di violazione del Modello o di commissione di reati non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla segnalazione.

In caso di ricezione di una segnalazione, l'Organismo di Vigilanza dovrà:

- procedere alla preliminare disamina della stessa per valutarne il livello di fondatezza;

- procedere ad effettuare delle indagini interne qualora dalle segnalazioni si ravvisi il fondato rischio di commissione di un reato;
- relazionare, in base agli esiti delle indagini di cui sopra, agli organi societari affinché vengano intraprese le relative azioni preventive e/o correttive.

Oltre alle segnalazioni relative alle violazioni di carattere generale sopra descritte, sono immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.Lgs. 231/2001 e che possano coinvolgere la Società;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui al D.Lgs. 231/2001, salvo espresso divieto dell'autorità giudiziaria;
- i rapporti preparati dai responsabili di unità organizzative e funzioni aziendali nell'ambito della loro attività di controllo, dai quali emergono fatti, atti, eventi od omissioni con profili critici rispetto all'osservanza delle norme del D.Lgs. 231/2001;
- le notizie relative ai procedimenti disciplinari svolti ed alle eventuali sanzioni erogate, in relazione alle fattispecie previste dal D.Lgs. 231/2001.

4.5 Attività di reporting dell'Organismo di Vigilanza

L'Organismo di Vigilanza assolve agli obblighi di *reporting* nei confronti degli organi societari secondo una triplice modalità:

- su base continuativa, nei confronti del Presidente e del Vice Presidente e del Consiglio di Amministrazione, del Collegio Sindacale nonché del Responsabile per la Prevenzione della Corruzione (ciascuno per le materie di propria competenza), anche attraverso l'invio dei verbali delle proprie riunioni;
- su base annuale, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale;
- al verificarsi di particolari eventi.

Il *reporting* ha ad oggetto:

a) l'attività svolta dall'Organismo di Vigilanza (indicando in particolare i controlli effettuati e l'esito degli stessi, l'eventuale aggiornamento della mappa dei Processi Sensibili, ecc.);
b) le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni alla Società, sia in termini di efficacia del Modello;

c) eventuali proposte di aggiornamento del Modello;
d) annualmente, il piano di attività di vigilanza prevista per l'anno successivo.

Gli incontri con gli organi cui l'Organismo di Vigilanza riferisce devono essere verbalizzati e copia dei verbali deve essere custodita dall'Organismo di Vigilanza.

4.6 Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report, relazione prevista nel Modello è conservata dall'Organismo di Vigilanza in apposito archivio informatico e/o cartaceo, che rappresenterà il "*set documentale 231*". Quest'ultimo servirà per dimostrare l'attività di vigilanza svolta dall'Organismo di Vigilanza, anche in un'ottica difensiva qualora pervenga un'eventuale contestazione di responsabilità *ex* D.Lgs. 231/2001 da parte dell'Autorità giudiziaria.

5.La diffusione del Modello e formazione del personale

L'attività di formazione e informazione dell'intera struttura organizzativa della Società costituisce uno degli elementi necessari per l'efficace ed efficiente attuazione del presente Modello Organizzativo. In specie l'attività info-formativa è rilevante per i seguenti motivi:

- costituisce una prova della reale volontà della Società di essere parte attiva alla prevenzione dei reati;
- stimola la cooperazione delle persone nell'effettiva realizzazione dell'obiettivo della legalità.

Obiettivi di un'adeguata attività info-formativa sono:

- promuovere la cooperazione;
- promuovere il principio di interazione;
- garantire la continuità nella cooperazione da parte di tutte le componenti del Sistema;
- creare occasioni di informazione e confronto.

L'individuazione dei destinatari dei corsi formativi (che verteranno in via esemplificativa e non esaustiva sui disposti del D.Lgs. 231/2001, sul contenuto del presente Modello Organizzativo e del Codice Etico) è punto fondamentale per l'efficacia dei suddetti corsi e per la corretta attuazione del Modello. I destinatari dei corsi formativi saranno tutti i dipendenti che operano nell'ambito dei Processi Sensibili. La partecipazione ai corsi è obbligatoria ed è demandato all'Organismo di Vigilanza il controllo in merito all'effettiva frequenza.

La Società dà massima pubblicità al Codice Etico ed al Modello Organizzativo sia al proprio interno che verso i terzi, anche attraverso link dedicato del proprio sito web.

5.1 Formazione ed informazione del personale dipendente

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza in collaborazione con il responsabile della funzione delegata a gestire le Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione del Modello.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 è destinata a tutti i dipendenti della Società che operano nell'ambito dei Processi Sensibili individuati nel presente Modello (cfr. le Parti Speciali).

Sarà inoltre previsto, nei programmi di formazione, un *refresh* annuale sui contenuti del Codice Etico, del D.Lgs. 231/2001 e del Modello.

5.2 Formazione e informazione agli Amministratori e al Collegio Sindacale

Il presente Modello viene approvato espressamente dal Consiglio di Amministrazione che è tenuto a conoscerne i contenuti, con particolare riguardo alla mappatura dei rischi e alle misure preventive conseguenti.

Il Modello approvato verrà consegnato a ciascun componente del Consiglio di Amministrazione e del Collegio Sindacale, i quali si impegnano a rispettarlo.

5.3 Informazione ai collaboratori, fornitori, consulenti e altri soggetti terzi

I collaboratori, fornitori, consulenti e altri soggetti terzi sono rispettivamente informati dell'adozione e dell'aggiornamento, da parte della Società, del Modello organizzativo e dell'esigenza che il loro comportamento sia conforme ai principi etici e alle linee di condotta adottati da Sito S.p.A.

6. Il sistema disciplinare

6.1 Principi generali

Aspetto essenziale per l'effettività del presente Modello, come previsto dagli art. 6 c. 2 lett. e) ed art. 7 c. 4 lett. b) del D.Lgs. 231/2001, è dato dalla presenza di un adeguato sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello, nei confronti dei soggetti apicali ovvero di quelli sottoposti all'altrui direzione o vigilanza.

Di seguito i caratteri essenziali (oltre a quello sopra esposto) del sistema disciplinare:

- è interno alla Società, ed è correlato alla normativa in materia di rapporto di lavoro e dai contratti collettivi in vigore;
- deve riguardare ogni infrazione (ovvero non solo quelle che comporterebbero una responsabilità *ex* D.Lgs. 231/2001 per l'Ente) alle regole del Modello e delle procedure aziendali ad esso riconducibili;
- deve essere formalizzato per iscritto e divulgato unitamente al Modello;
- deve essere compatibile, con i precetti legislativi e contrattuali (individuali e collettivi) di cui costituisce parte integrante;
- deve rispettare il principio di proporzionalità nella misura sanzionatoria rispetto alla gravità dell'infrazione contestata ed accertata;
- deve rispettare il principio del contraddittorio.

L'accertamento delle eventuali responsabilità derivanti dalla violazione del Modello e l'attribuzione della conseguente sanzione sarà condotto nel rispetto della normativa vigente, della *privacy*, della dignità e della reputazione dei soggetti coinvolti.

6.2 Il sistema disciplinare nei confronti dei lavoratori dipendenti

I comportamenti in violazione del presente Modello da parte dei dipendenti soggetti al CCNL per le aziende esercenti attività di commercio costituiscono illecito disciplinare.

I lavoratori saranno passibili dei provvedimenti nel rispetto delle procedure previste dall'art. 7 della Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili - previsti dall'apparato sanzionatorio di cui all'art. 225, Capo ventunesimo rubricato "provvedimenti disciplinari" del CCNL sopra menzionato, e precisamente:

a) ammonizione verbale

b) ammonizione scritta
c) multa non superiore all'importo di 4 ore di retribuzione
d) sospensione dal lavoro e della retribuzione per un periodo non superiore a 10 giorni di effettivo lavoro, salva la misura del licenziamento per i casi di particolare gravità.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, al vertice aziendale.

6.3 Misure nei confronti dei dirigenti

In caso di violazione, da parte di dirigenti, delle procedure previste dal presente Modello, o di adozione, nell'espletamento di attività connesse con i Processi Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso saranno applicate le seguenti sanzioni:

a) ammonizione verbale;
b) ammonizione scritta;
c) licenziamento ex art. 2118 c.c.;
d) licenziamento per giusta causa.

6.4 Misure nei confronti degli Amministratori e dei Sindaci

In caso di accertata violazione da parte degli Amministratori o dei membri del Collegio Sindacale, l'Organismo di Vigilanza informerà tempestivamente l'intero Consiglio di Amministrazione ed il Collegio Sindacale i quali provvederanno ad assumere tutte le opportune iniziative previste dalla vigente normativa.

6.5 Misure nei confronti dei collaboratori, fornitori, consulenti e altri soggetti terzi

In caso di accertata violazione da parte di soggetti terzi alla Società, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali presenti nelle lettere di incarico, nei contratti o negli accordi commerciali, la risoluzione anticipata del rapporto contrattuale fatta salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti alla Società.

7.Reati rilevanti e Aree sensibili in S.I.TO S.p.A

Dalla revisione della mappatura dei rischi condotta ai fini del D.Lgs. 231/2001, nonché dalle precedenti versioni del Modello, è emerso che i Processi Sensibili, allo stato attuale, riguardano principalmente i seguenti reati-presupposto:

- art. 24: indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico;
- art. 24-*bis*: delitti informatici e trattamento illecito di dati;
- art. 24-*ter*: delitti di criminalità organizzata;
- art. 25: concussione, induzione indebita a dare o promettere utilità e corruzione;
- art. 25-*ter*: reati societari;
- art. 25-*septies:* omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- art. 25-*octies*: ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- art. 25-*novies*: delitti in materia di violazione del diritto d'autore;
- art. 25-*undecies*: reati ambientali
- art. 25-*duodecies*: impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

Il rischio relativo alle altre fattispecie di reato contemplate dal D.Lgs. 231/2001 appare solo astrattamente e non concretamente ipotizzabile.

In relazione ai reati-presupposto ritenuti rilevanti per l'attività della Società, sono state individuate le seguenti Aree Sensibili:

PROCESSO SENSIBILE	REATO RILEVANTE	REGOLAMENTAZIONE
AFFIDAMENTO LAVORI MEDIANTE GARE D'APPALTO IN CUI LA SOCIETÀ RICOPRE LA FIGURA DI STAZIONE APPALTANTE NONCHÉ L'ACQUISTO DI BENI E SERVIZI IN APPLICAZIONE DEL D.LGS 50/2016 (SOPRA E SOTTO SOGLIA)	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE, con particolare riferimento alla: ✓ gestione dei rapporti con gli Enti Pubblici in via esemplificativa e non esaustiva per l'ottenimento di autorizzazioni, licenze, ecc…; ✓ gestione delle ispezioni (amministrative, fiscali, previdenziali, ecc.); ✓ gestione di procedimenti giudiziali, stragiudiziali e arbitrali.	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
GESTIONE DELLE ATTIVITÀ DI ACQUISIZIONE E/O GESTIONE DI CONTRIBUTI, SOVVENZIONI, FINANZIAMENTI, ASSICURAZIONI O GARANZIE CONCESSE DAI SOGGETTI PUBBLICI	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
	Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies)	**PARTE SPECIALE 6**
GESTIONE DEL PROCESSO DI SPONSORIZZAZIONE, CONCESSIONE DI EROGAZIONI LIBERALI E DONAZIONI, SPESE DI RAPPRESENTANZA (INCLUSA LA POLITICA DI OMAGGI O REGALIE)	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**

GESTIONE DI TRATTAMENTI PREVIDENZIALI DEL PERSONALE E/O GESTIONE DEI RELATIVI ACCERTAMENTI E ISPEZIONI	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
CONFERIMENTO E GESTIONE DELLE CONSULENZE (AMMINISTRATIVE, FISCALI, LEGALI, PROFESSIONALI ETC)	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s*) bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
GESTIONE DEI BENI STRUMENTALI E DELLE UTILITÀ AZIENDALI (ES. AUTOVETTURE, CELLULARI, PERSONAL COMPUTER, CARTE DI CREDITO AZIENDALI ETC.)	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
GESTIONE E CONTROLLO DELLE NOTE SPESE	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**
GESTIONE DEL SISTEMA INFORMATIVO E DI REPORTING VERSO I RESPONSABILI DI FUNZIONE DI VOLTA IN VOLTA COINVOLTI	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**
GESTIONE DEL SISTEMA DI TRACCIABILITÀ DELLE SINGOLE OPERAZIONI SVOLTE	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**

	Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 octies)	**PARTE SPECIALE 6**
UTILIZZO POTERI DI FIRMA E LEGALE RAPPRESENTANZA DEL LEGALE RAPPRESENTATE (O CHI NE FA LE VECI) E DEL DATORE DI LAVORO	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
	Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 septies)	**PARTE SPECIALE 4**
NEGOZIAZIONE, STIPULA E/O ESECUZIONE DI CONTRATTI, CONVENZIONI, CONCESSIONI CON SOGGETTI PUBBLICI AI QUALI SI PERVIENE MEDIANTE PROCEDURE NEGOZIATE (AFFIDAMENTO DIRETTO O TRATTATIVE PRIVATE) OVVERO MEDIANTE PROCEDURE AD EVIDENZA PUBBLICA (APERTE O RISTRETTE)	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
GESTIONE DEI RAPPORTI COMMERCIALI con particolare riferimento alle transazioni finanziarie	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
	Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 *octies*)	**PARTE SPECIALE 6**
GESTIONE DI SISTEMI INFORMATICI E TELEMATICI, con particolare riferimento alle seguenti attività a rischio**:** ✓ detenzione di codici di accesso ai sistemi;	Delitti informatici e trattamento illecito di dati (art. 24 *bis*)	**PARTE SPECIALE 2**

✓ diffusione ed installazione di programmi diretti a danneggiare o interrompere i sistemi. ✓ gestione degli accessi logici ai dati e ai sistemi; ✓ gestione dei backup; ✓ gestione di software, apparecchiature, dispositivi o programmi informatici (change management); ✓ gestione della sicurezza della rete; ✓ gestione della sicurezza fisica.		
PREDISPOSIZIONE DELLE COMUNICAZIONI A SOCI E/O A TERZI RELATIVE ALLA SITUAZIONE ECONOMICA, PATRIMONIALE E FINANZIARIA DELLA SOCIETÀ (BILANCIO D'ESERCIZIO, CORREDATO DALLE RELATIVE RELAZIONI DI LEGGE, ECC.), con particolare riferimento alla: ✓ redazione dello Stato Patrimoniale, del Conto Economico, della Nota Integrativa, della Relazione sulla Gestione;	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**
GESTIONE DEI RAPPORTI CON I SOCI, IL COLLEGIO SINDACALE E LA SOCIETÀ DI REVISIONE, con particolare riferimento al: ✓ controllo svolto dai Soci, dal Collegio Sindacale (anche con riferimento al controllo legale dei conti);	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**
GESTIONE DEI CONFLITTI DI INTERESSE, con particolare riferimento alla: ✓ segnalazione dei conflitti di interesse;	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**
"AREA TAX": ✓ adempimenti fiscali.	Reati societari (art. 25 *ter*)	**PARTE SPECIALE 3**
	Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro,	**PARTE SPECIALE 6**

	beni o utilità di provenienza illecita (art. 25 *octies*)	
GESTIONE DEGLI ADEMPIMENTI PREVISTI DAL D.LGS. 9 APRILE 2008, N. 81 E SUCCESSIVE MODIFICHE E INTEGRAZIONI "ATTUAZIONE DELL'ART. 1 DELLA LEGGE 3 AGOSTO 2007, N. 123, IN MATERIA DI TUTELA DELLA SALUTE E DELLA SICUREZZA NEI LUOGHI DI LAVORO", con particolare riferimento alla: ✓ attribuzione di ruoli e responsabilità in materia di salute e sicurezza sul lavoro; ✓ predisposizione e aggiornamento del Documento di Valutazione dei Rischi (DVR); ✓ verifica dell'idoneità tecnico-professionale dell'impresa affidataria, delle imprese esecutrici e dei lavoratori autonomi in relazione alle funzioni o ai lavori da affidare; ✓ verifica, nell'ambito delle attività in regime di appalto e subappalto, del possesso della tessera di riconoscimento da parte dei lavoratori delle imprese esterne; ✓ gestione dei contratti di appalto con le ditte esterne; ✓ gestione della risoluzione delle interferenze nell'ambito dei contratti d'opera o d'appalto o di somministrazione che lo richiedono (predisposizione del Documento Unico di Valutazione dei Rischi – DUVRI); ✓ gestione nella formazione ed informazione adeguata e specifica destinata ai dipendenti e dell'informativa per personale esterno operante all'interno della Società; ✓ monitoraggio del corretto utilizzo, da parte dei lavoratori interni ed esterni, dei Dispositivi di Protezione Individuale (DPI) messi a disposizione per lo svolgimento delle mansioni loro attribuite;	Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies***)**	**PARTE SPECIALE 4**

✓ definizione e gestione dei programmi di manutenzione delle attrezzature; ✓ formalizzazione e registrazione delle verifiche effettuate dalla Società in materia di salute e sicurezza sul lavoro; ✓ ottenimento e conservazione delle dichiarazioni di conformità degli impianti elettrici/idraulici/termici/di condizionamento e dei macchinari in uso; ✓ ottenimento e conservazione del Certificato di Prevenzione Incendi (CPI) e dei certificati di agibilità dei locali; ✓ formazione ed informazione in tema di salute e sicurezza; ✓ circolazione di automezzi all'interno delle aree di pertinenza della Società; ✓ manutenzione di impianti industriali ed elettrici nella sede della Società;		
GESTIONE DI SISTEMI INFORMATICI E TELEMATICI, con particolare riferimento alla seguente attività a rischio: ✓ gestione delle licenze software.	Delitti in materia di violazione del diritto d'autore (art. 25 *nonies*)	**PARTE SPECIALE 5**
GESTIONE DEI FLUSSI FINANZIARI	Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 *octies*)	**PARTE SPECIALE 6**
	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
ASSUNZIONE E GESTIONE DEL PERSONALE (COMPRESI I SOGGETTI APPARTENENTI A CATEGORIE PROTETTE	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art 25 *duodecies*)	**PARTE SPECIALE 7**

	Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)	**PARTE SPECIALE 1**
GESTIONE DEI RIFIUTI (ARTT. 256 – 260 BIS D.LGS. 152/2006, T.U. AMBIENTE)	Reati ambientali (art. 25 *undecies*)	**PARTE SPECIALE 8**
SMALTIMENTO TONER E STAMPANTI	Reati ambientali (art. 25 *undecies*)	**PARTE SPECIALE 8**
GESTIONE AREE COMUNI DI PUBBLICO ACCESSO	Reati ambientali (art. 25 *undecies*)	**PARTE SPECIALE 8**
MONITORAGGIO SULL'INQUINAMENTO IDRICO (ART. 137 D.LGS 152/2006, T.U. AMBIENTE)	Reati ambientali (art. 25 *undecies*)	**PARTE SPECIALE 8**
MONITORAGGIO SUI SITI CONTAMINATI (ART. 257 D.LGS. 152/2006, T.U. AMBIENTE)	Reati ambientali (art. 25 *undecies*)	**PARTE SPECIALE 8**

PARTE SPECIALE 1

Reati nei rapporti con la Pubblica Amministrazione (art. 24 e 25), corruzione fra privati (art. 25 *ter* comma 1 lett. s) *bis*) e delitti di criminalità organizzata (art. 24 *ter*)

Si è ritenuto opportuno trattare congiuntamente i reati nei rapporti con la Pubblica Amministrazione ed il reato di corruzione tra privati per l'ontologica omogeneità tra i reati di corruzione / concussione/ induzione indebita a dare o promettere utilità ed il reato di corruzione tra privati. Per quanto riguarda i reati associativi previsti dall'art. 24 ter, ed in particolare il reato di associazione a delinquere di cui all'art. 416 c.p., essi possono rappresentare un possibile contenitore di un numero indeterminato di illeciti tra loro anche disomogenei. E' vero però che un assetto organizzativo trasparente che assicuri la tracciabilità dei processi decisionali, dei movimenti finanziari, la definizione chiara di poteri e doveri, un costante flusso informativo tra uffici e verso l'Organismo di Vigilanza, riduce di per sé il rischio della commissione di reati associativi. In particolare, i processi sensibili in relazione ai reati contro la pubblica amministrazione ed al reato di corruzione tra privati sono inevitabilmente quelli in cui potrebbero trovare terreno fertile potenziali vincoli associativi stabili per commettere un numero indeterminato di reati (si pensi, per esempio, alla gestione degli appalti pubblici).

I principali Processi Sensibili individuati sono i seguenti:

- affidamento lavori mediante gare d'appalto in cui la Società ricopre la figura di stazione appaltante nonché l'acquisto di beni e servizi in applicazione del D.Lgs. 50/2016;
- gestione dei rapporti con la Pubblica Amministrazione, con particolare riferimento alla:
    - ✓ gestione dei rapporti con gli Enti Pubblici in via esemplificativa e non esaustiva per l'ottenimento di autorizzazioni, licenze, ecc…;
    - ✓ gestione delle ispezioni (amministrative, fiscali, previdenziali, ecc.);
    - ✓ gestione di procedimenti giudiziali, stragiudiziali e arbitrali.
- gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse dai soggetti pubblici;
- gestione del processo di sponsorizzazione, concessione di erogazioni liberali e donazioni, spese di rappresentanza (inclusa la politica di omaggi o regalie);
- gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti e ispezioni;

- conferimento e gestione delle consulenze (amministrative, fiscali, legali, professionali etc);
- gestione dei beni strumentali e delle utilità aziendali (es. autovetture, cellulari, personal computer, carte di credito aziendali etc.);
- gestione e controllo delle note spese;
- gestione del sistema informativo e di reporting verso i responsabili di funzione di volta in volta coinvolti;
- gestione dei flussi finanziari;
- assunzione e gestione del personale (compresi i soggetti appartenenti a categorie protette) e politica degli incentivi/premi;
- gestione del sistema di tracciabilità delle singole operazioni svolte;
- utilizzo poteri di firma e legale rappresentanza del Legale Rappresentate (o chi ne fa le veci) e del Datore di Lavoro;
- gestione dei rapporti commerciali con particolare riferimento alle transazioni finanziarie;
- negoziazione, stipula e/o esecuzione di contratti, convenzioni, concessioni con soggetti pubblici ai quali si perviene mediante procedure negoziate (affidamento diretto o trattative private) ovvero mediante procedure ad evidenza pubblica (aperte o ristrette); Per tali processi diventa centrale la corretta applicazione del D.Lgs. 50/2016 (c.d. Codice dei contratti pubblici).

Nell'ambito dei suddetti rischi, la Società, oltre alle regole di comportamento previste nel Codice Etico, nelle procedure aziendali, nonché nel Piano per la Prevenzione della Corruzione **(PARTE SPACIALE 9)** ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- è fatto divieto di elargizioni in denaro a pubblici ufficiali o incaricati di pubblico servizio;
- è obbligatorio il rispetto della prassi aziendale per la distribuzione di omaggi e regali. In particolare, è vietata qualsiasi forma di regalo a funzionari della Pubblica Amministrazione italiani ed esteri (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico, o l'immagine della Società. I regali offerti, salvo quelli di modico valore, devono

essere documentati in modo adeguato per consentire le opportune verifiche e autorizzati nel rispetto dei poteri previsti;

- non è consentito accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le medesime conseguenze individuate al precedente punto;
- il personale che riceve omaggi o benefici non previsti dalle fattispecie consentite, è tenuto a darne comunicazione all'Organismo di Vigilanza;
- è proibito effettuare o promettere, in favore di partners commerciali o di collaboratori esterni, prestazioni che non trovino adeguata giustificazione alla luce del rapporto con essi costituito;
- i compensi riconosciuti ai collaboratori esterni devono trovare adeguata giustificazione in relazione al tipo di incarico da svolgere e alla prassi vigente nel settore di attività interessato;
- le dichiarazioni a organismi pubblici nazionali o comunitari effettuate al fine di conseguire finanziamenti, contributi o erogazioni di varia natura devono essere basate su informazioni veritiere;
- le somme ricevute da detti organismi pubblici devono essere destinate agli scopi per i quali erano stati concessi;
- i rapporti nei confronti della Pubblica Amministrazione devono essere gestiti in modo unitario, intendendosi con ciò che le persone che rappresentano la Società nei confronti della Pubblica Amministrazione sono esclusivamente, oltre ai legali rappresentanti, quelle autorizzate in tal senso dalla Società;
- coloro che svolgono una funzione di controllo e supervisione verso i Dipendenti che operano con la Pubblica Amministrazione devono seguire con attenzione e con le modalità più opportune l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- i compensi dei consulenti e dei partners commerciali devono essere determinati solo per iscritto;
- nessun tipo di pagamento non adeguatamente documentato può esser effettuato;

- devono essere rispettati, da parte di tutti i soggetti coinvolti nei processi decisionali della Società, i principi di trasparenza nell'assunzione delle decisioni aziendali che abbiano diretto impatto sui soci e sui terzi;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- nei rinnovi e/o nuovi contratti con i partners commerciali, consulenti e fornitori deve essere contenuta apposita clausola che regoli le conseguenze in caso di violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali).

Le procedure aziendali significative per la prevenzione dei reati in oggetto, che si richiamano integralmente in questa sede anche nella loro eventuale e successiva modificazione ed implementazione resa necessaria per garantirne la costante adeguatezza, sono le seguenti:

- Codice Etico
- Regolamento interno "tracciabilità dei flussi finanziari"
- Regolamento per la disciplina dei rimborsi spese a favore degli amministratori, componenti del collegio sindacale, dirigenti e dipendenti
- P_01 Contabilità e bilancio
- P_02 Operazioni monetarie e finanziarie
- P_03 Finanziamenti pubblici
- P_04 Omaggi e liberalità
- P_05 Selezione ed assunzione del personale
- P_08 Procedura affidamento e contratti di appalto
- P_09 Procedura di esecuzione dei pagamenti
- P_10 Gestione amministrativa dei rapporti commerciali
- P_11 Benefits

Al fine di ridurre il rischio dei reati in oggetto, si segnala inoltre che la L. 190/2012 richiede particolari adempimenti in materia di **conferimento degli incarichi dirigenziali**, di **rotazione degli incarichi** nonché relativamente ai **sistemi di controllo** periodici e a campione sulle diverse attività societarie**.** (cfr. **PARTE SPECIALE 9**).

PARTE SPECIALE 2

Delitti informatici e trattamento illecito di dati (art. 24 *bis*)

I principali *Processi Sensibili* individuati sono i seguenti:

- gestione di sistemi informatici e telematici, con particolare riferimento alle seguenti attività a rischio:
    - ✓ detenzione di codici di accesso ai sistemi;
    - ✓ diffusione ed installazione di programmi diretti a danneggiare o interrompere i sistemi;
    - ✓ gestione degli accessi logici ai dati e ai sistemi;
    - ✓ gestione dei backup;
    - ✓ gestione di software, apparecchiature, dispositivi o programmi informatici (*change management*);
    - ✓ gestione della sicurezza della rete;
    - ✓ gestione della sicurezza fisica.

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico nonché nelle procedure aziendali, ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- individuare e adottare misure adeguate di sicurezza (di natura organizzativa, fisica e logica) in modo da minimizzare il rischio di accessi non autorizzati, di alterazione, di divulgazione, di perdita o di distruzione delle risorse informatiche (e dei dati personali trattati);
- monitorare periodicamente l'efficacia e l'adeguatezza delle misure di prevenzione e protezione al fine di sostituirle o modificarle qualora se ne riscontri l'inefficacia e/o l'inadeguatezza, anche parziale, ovvero in relazione ad eventuali mutamenti organizzativi e dei rischi;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- rispettare le norme in materia di protezione dei dati personali (D.Lgs. 196/2003 e sue modifiche ed integrazioni) alla quale sia i vertici aziendali che i dipendenti e collaboratori della Società sono tenuti ad attenersi;

- nei rinnovi e/o nuovi contratti con i partners commerciali, consulenti e fornitori deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali);
- definire, documentare, implementare, monitorare e periodicamente aggiornare un programma di informazione / formazione in materia di trattamento dei dati personali a favore, almeno, degli incaricati;
- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- utilizzare gli strumenti aziendali nel rispetto delle procedure e delle *policy* aziendali definite;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che terzi soggetti possano venirne a conoscenza e aggiornare periodicamente le password;
- evitare di utilizzare le risorse informatiche (es. *personal computer* fissi o portatili) assegnate, per finalità diverse da quelle lavorative;
- evitare di porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
    - acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
    - danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
    - utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- non distruggere o alterare documenti informatici archiviati sulle *directory* di rete o sugli applicativi aziendali se non espressamente autorizzati, e in particolare i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- non utilizzare o installare programmi software diversi da quelli autorizzati dalla Direzione;
- non accedere ad aree riservate (quali *server rooms*, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- non aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (*antivirus, firewall, proxy server*, ecc.);
- non lasciare il proprio personal computer sbloccato e incustodito;
- non rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale o anche ad altri siti/sistemi;
- non detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- non intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;

- non utilizzare in modo improprio gli strumenti di firma digitale assegnati;
- non alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per la Società;
- evitare di entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- non installare, duplicare o diffondere a terzi programmi (*software*) senza essere in possesso di idonea licenza o esorbitando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze).

La procedura aziendale significativa per la prevenzione dei reati in oggetto, che si richiama integralmente in questa sede anche nella sua eventuale e successiva modificazione ed implementazione resa necessaria per garantirne la costante adeguatezza, è il "Disciplinare interno per l'utilizzo delle risorse informatiche".

PARTE SPECIALE 3

Reati societari (art. 25 *ter*)

In tema di reati societari, ad esclusione del reato di corruzione fra privati che per ragioni sistematiche è trattato nella **Parte Speciale 1** congiuntamente ai reati contro la Pubblica Amministrazione, i principali Processi Sensibili individuati sono i seguenti:

- predisposizione delle comunicazioni a soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della Società (bilancio d'esercizio, corredato dalle relative relazioni di legge, ecc.), con particolare riferimento alla:
  - ✓ redazione dello Stato Patrimoniale, del Conto Economico, della Nota Integrativa, della Relazione sulla Gestione;
- gestione dei rapporti con i Soci, il Collegio Sindacale e la società di Revisione, con particolare riferimento al:
  - ✓ controllo svolto dai Soci, dal Collegio Sindacale (anche con riferimento al controllo legale dei conti);
- gestione dei conflitti di interesse, con particolare riferimento alla:
  - ✓ segnalazione dei conflitti di interesse;
- gestione e controllo delle note spese;
- gestione del sistema informativo e di reporting verso i responsabili di funzione di volta in volta coinvolti;
- gestione del sistema di tracciabilità delle singole operazioni svolte;
- "area tax":
  - ✓ adempimenti fiscali.

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico, ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, occorre tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società; in particolar modo è fatto divieto di:
  - ✓ rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
  - ✓ omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- occorre assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare; in particolar modo è fatto divieto di:
  - ✓ porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Collegio Sindacale e della Società di Revisione;
  - ✓ determinare o influenzare l'assunzione delle deliberazioni dell'Assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- è necessario mettere a disposizione di tutti i componenti del Consiglio di Amministrazione, con documentata certificazione dell'avvenuta consegna, la bozza del progetto di bilancio, prima della riunione di quest'ultimo per l'approvazione dello stesso;
- occorre mettere a disposizione di tutti i componenti del Consiglio di Amministrazione il giudizio sul bilancio (o un'attestazione similare che sia sufficientemente chiara ed analitica) da parte del Collegio Sindacale e della Società di Revisione;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- nei rinnovi e/o nuovi contratti con i partners commerciali, consulenti e fornitori deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali);

Le procedure aziendali significative per la prevenzione dei reati in oggetto, che si richiamano integralmente in questa sede anche nella loro eventuale e successiva modificazione ed implementazione resa necessaria per garantirne la costante adeguatezza, sono le seguenti:

- Codice Etico
- Regolamento interno “tracciabilità dei flussi finanziari”
- P_01 Contabilità e Bilancio
- P_02 Operazioni monetarie e finanziarie
- P_04 Omaggi e liberalità
- P_06 Operazioni societarie straordinarie
- P_07 Trattamento delle informazioni riservate
- P_09 Procedura di esecuzione dei pagamenti
- P_10 Gestione amministrativa dei rapporti commerciali
- P_11 Benefits

PARTE SPECIALE 4

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies*)

I principali Processi Sensibili individuati sono i seguenti:

- gestione degli adempimenti previsti dal D.Lgs. 9 aprile 2008, n. 81 e successive modifiche e integrazioni "Attuazione dell'art. 1 della Legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro", con particolare riferimento alla:
  - ✓ attribuzione di ruoli e responsabilità in materia di salute e sicurezza sul lavoro;
  - ✓ predisposizione e aggiornamento del Documento di Valutazione dei Rischi (DVR);
  - ✓ verifica dell'idoneità tecnico-professionale dell'impresa affidataria, delle imprese esecutrici e dei lavoratori autonomi in relazione alle funzioni o ai lavori da affidare;
  - ✓ verifica, nell'ambito delle attività in regime di appalto e subappalto, del possesso della tessera di riconoscimento da parte dei lavoratori delle imprese esterne;
  - ✓ gestione dei contratti di appalto con le ditte esterne;
  - ✓ gestione della risoluzione delle interferenze nell'ambito dei contratti d'opera o d'appalto o di somministrazione che lo richiedono (predisposizione del Documento Unico di Valutazione dei Rischi – DUVRI);
  - ✓ gestione nella formazione ed informazione adeguata e specifica destinata ai dipendenti e dell'informativa per personale esterno operante all'interno della Società;
  - ✓ monitoraggio del corretto utilizzo, da parte dei lavoratori interni ed esterni, dei Dispositivi di Protezione Individuale (DPI) messi a disposizione per lo svolgimento delle mansioni loro attribuite;
  - ✓ definizione e gestione dei programmi di manutenzione delle attrezzature;
  - ✓ formalizzazione e registrazione delle verifiche effettuate dalla Società in materia di salute e sicurezza sul lavoro;
  - ✓ ottenimento e conservazione delle dichiarazioni di conformità degli impianti elettrici/idraulici/termici/di condizionamento e dei macchinari in uso;

- ✓ ottenimento e conservazione del Certificato di Prevenzione Incendi (CPI) e dei certificati di agibilità dei locali;
- ✓ formazione ed informazione in tema di salute e sicurezza;
- ✓ circolazione di automezzi all'interno delle aree di pertinenza della Società;
- ✓ manutenzione di impianti industriali ed elettrici nella sede della Società.

– utilizzo poteri di firma e legale rappresentanza del Legale Rappresentate (o chi ne fa le veci) e del Datore di Lavoro.

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico nonché nelle procedure aziendali, ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- i destinatari devono conoscere e rispettare tutte le regole e i principi contenuti (i) nel Codice Etico, (ii) nella valutazione dei rischi aziendali, (iii) nel documento unico di valutazione rischi interferenziali (DUVRI) degli appalti esistenti ed (iv) ogni altra documentazione relativa alla formazione ed informazione dei rischi aziendali interni alla Società;
- il **Datore di Lavoro**, i **Dirigenti con delega sulla sicurezza**, i **Collaboratori esterni** ed i **Partners** devono:
  - affidare i compiti ai lavoratori tenendo conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;
  - fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale;
  - 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;
  - richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro;
  - richiedere l'osservanza da parte dei singoli lavoratori dell'uso dei dispositivi individuali di protezione, eventualmente necessari durante le attività a rischio;
  - adottare le misure per il controllo delle situazioni di rischio in caso di emergenza;
  - dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
  - 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;
  - adempiere agli obblighi di informazione, formazione e addestramento;

- 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;
- 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.

- i **lavoratori** devono:
  - 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;
  - adempiere agli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
  - osservare le disposizioni e le istruzioni ricevute ai fini della protezione collettiva ed individuale;
  - utilizzare correttamente le attrezzature di lavoro, i mezzi di trasporto, nonché i dispositivi di sicurezza;
  - utilizzare in modo appropriato, gli eventuali dispositivi di protezione messi a loro disposizione;
  - segnalare immediatamente le deficienze dei mezzi di trasporto, delle attrezzature e dei dispositivi di protezione;
  - segnalare qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza;
  - eliminare o ridurre le situazioni di pericolo grave e incombente, direttamente od indirettamente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
  - non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
  - 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;
  - partecipare ai programmi di formazione e di addestramento ;
  - sottoporsi ad eventuali controlli sanitari previsti dal D.Lgs. 81/08 comunque disposti dal medico competente.

- i **lavoratori dei Partners che svolgono attività in regime di appalto o subappalto e i lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro** (i quali sono tenuti a provvedervi per proprio conto) devono:
  - rispettare le indicazioni di sicurezza e comportamento contenute nel DUVRI;
  - esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro.

- il **Responsabile del Servizio di Prevenzione e Protezione** deve:
    - aggiornare la valutazione dei rischi e le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base del cambiamento dell'organizzazione aziendale e dei sopralluoghi e delle informazioni ricevute dal RLS e dal responsabile del Modello di Gestione e Controllo;
    - elaborare, per quanto di competenza, le misure preventive e protettive ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
    - avviare sistemi di controllo di tali misure;
    - elaborare le procedure di sicurezza per le varie attività aziendali;
    - proporre e fornire i programmi di informazione e formazione dei lavoratori;
    - partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro.

Nell'ambito dei suddetti rischi la Società ha altresì individuato i seguenti principi/regole di comportamento specifici per ogni area a rischio, che devono essere rispettati da tutti i destinatari a integrazione dei principi/regole di comportamenti generali sopra esposte:

- nelle **attività di manutenzione di impianti industriali ed elettrici nella sede della Società**, le disposizioni indirizzate alle ditte operanti nel settore specifico sono quelle fornite dall'Ufficio Tecnico del S.I.TO. che richiede e gestisce gli incarichi manutentivi.
- nelle attività di **gestione dei contratti di appalto con le ditte esterne, controllo delle attività cantieristiche di appalti esterni e controllo delle disposizioni di sicurezza contenute nel DUVRI**, le disposizioni indirizzate al personale interno al Responsabile del Servizio di Prevenzione e Protezione, ai Partners e ditte esterne. Il datore di lavoro assieme al RSPP, in caso di affidamento di lavori a ditte esterne deve:
    a) Verificare, prima della firma del contratto o richiedere tra i documenti previsti in gara d'appalto, l'idoneità tecnico professionale della ditta esterna in relazione ai lavori da affidare. A tal fine si richiedono i seguenti documenti:
        - Certificato di iscrizione alla camera di commercio, industria e artigianato;
        - Autocertificazione della ditta esterna del possesso dei requisiti di idoneità tecnico professionale (art. 47 del T.U delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445);
        - DURC.
    b) Fornire dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività.

L'azienda, attraverso il datore di lavoro ed il RSPP, e la ditta esterna devono:

a) cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
b) coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera.

Il datore di lavoro dell'azienda con il supporto del RSPP elabora il "Documento Unico di Valutazione dei Rischi" (DVRI) che indica le misure adottate per eliminare o, ove ciò non è possibile, ridurre al minimo i rischi da interferenze. Tale documento deve essere allegato al contratto di appalto o di opera. Il DVRI non si applica ai rischi specifici propri dell'attività delle ditte esterne. Il DVRI è quindi così strutturato:

- Identificazione dell'Oggetto dell'appalto mediante:
  1. Descrizione appalto
  2. Aree interessate ai lavori
  3. Data presunta inizio lavori
  4. Durata presunta
  5. Contemporaneità con attività aziendale
  6. Contemporaneità con altre imprese
  7. Presenza di aziende in sub-appalto
- Identificazione dell'Impresa/e appaltatrice/i
  1. Ragione Sociale
  2. Sede
  3. Telefono / fax
  4. Responsabile dell'impresa
  5. Responsabile dei lavori
  6. Ev Subappalto: Ragione Sociale, Sede, Telefono / fax, Responsabile dell'impresa, Responsabile dei lavori
- Informazioni generali
  1. Identificazione dell'area interessata
  2. Accesso pedonale delle persone
  3. Accesso dei veicoli
  4. Vie di fuga (secondo planimetria e segnaletica in loco)
  5. Attrezzature prevenzione incendi (secondo planimetria e segnaletica in loco)
  6. Orario di lavoro
- Indicazioni della presenza o meni di Fonti specifiche di pericoli
  - Presenza di infiammabili / combustibili (Si/No)
  - Fluidi pericolosi (Si/No)

- Parti in tensione (Si/No)
- Apparecchi / attrezzature particolari (Si/No)
- Altro

❖ Indicazioni sulla fornitura di materiali di consumo
- Acqua industriale (Si/No)
- Energia elettrica (Si/No)
- Aria compressa (Si/No)
- Altro

❖ Osservazioni in merito ad eventuali rischi da interferenza lavorativa e relative misure adottate, identificazione delle Lavorazioni richiedenti preventiva specifica autorizzazione
1. Comportanti pericoli d'incendio (Si/No)
2. entro luoghi confinati (Si/No)
3. in posti sopraelevati (Si/No)
4. presenza di sostanze / preparati pericolosi (Si/No)
5. presenza di tensioni pericolose (Si/No)
6. ambienti con rumorosità superiore a 87 dB (A) (Si/No)
7. altri

❖ Indicazione dei costi relativi alla sicurezza sul lavoro, note finali e identificazione dei riferimenti per i necessari collegamenti
- per il Committente
- per impresa/e appaltatrice

All'interno del DUVRI ci sono documenti relativi a:

❖ Identificazione dei Pericoli presenti nei luoghi di svolgimento dell'incarico, verbale di incontro e sopralluogo sul luogo dell'attvità da svolgere sottoscritto dalle parti ed elenco esemplificativo e non esaustivo di informazioni di carattere generale e specifico con:
- Disposizioni ed informazioni di sicurezza
- Divieti ed obblighi da osservare scrupolosamente
- Autorizzazioni da richiedere preventivamente al personale tecnico
- Norme generali di prevenzione incendi

❖ Identificazione dei Rischi generici presenti nei luoghi di svolgimento dell'incarico

❖ Identificazione dei Rischi particolari presenti nei luoghi di svolgimento dell'incarico

Non è previsto e autorizzato l'utilizzo da parte di ditte esterne di attrezzature, mezzi e macchine dell'organizzazione S.I.TO.

Il RSGSL mantiene aggiornato il modulo "Elenco ditte esterne soggette a DUVRI".
Durante lo svolgimento delle attività da parte delle ditte esterne, il personale occupato della stessa deve essere munito di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Il RSPP deve garantire che ciò avvenga mediante controlli periodici.

- nelle attività di **circolazione di automezzi all'interno delle aree di pertinenza della Società** le disposizioni indirizzate alle ditte operanti nel settore specifico sono formalizzate all'interno del DUVRI.

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne I Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro sono i seguenti:

- curare l'aggiornamento, l'emanazione e con il RSPP, l'applicazione di istruzioni operative standardizzate relative ai comportamenti da seguire nell'ambito delle attività a rischio, come individuate nella presente Parte speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- con riferimento alla gestione dei contratti di appalto con le ditte esterne, controllo delle attività cantieristiche di appalti esterni e controllo delle disposizioni di sicurezza contenute nel DUVRI, l'Organismo di Vigilanza provvede all'espletamento dei seguenti compiti:
    - monitoraggio sull'efficacia delle procedure;
    - esame di eventuali segnalazioni specifiche provenienti dal RSPP o da qualsiasi dipendente ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
    - verifiche periodiche sul rispetto delle procedure;
    - vigilanza sull'effettiva sussistenza del mantenimento delle condizioni di sicurezza lavorativa;
    - revisione delle procedure operative.

4.1. Il Sistema di gestione per la sicurezza e salute sul lavoro (S.G.S.L.)

L'implementazione del Sistema di Gestione per la Sicurezza, nel Modello di Organizzazione, Controllo e Gestione, ha, per l'azienda i seguenti obiettivi:

- coinvolgere i lavoratori e i loro rappresentanti nel SGSL;

- aumentare l'efficienza dell'organizzazione e le proprie prestazioni in riferimento alla tutela della Salute e Sicurezza sul lavoro;
- ridurre progressivamente i costi complessivi della SSL compresi quelli derivanti da incidenti, infortuni e malattie correlate al lavoro minimizzando i rischi cui possono essere esposti i dipendenti o i terzi;
- migliorare continuamente la capacità di adattamento all'evoluzione delle normative volontarie e cogenti;
- migliorare l'immagine interna ed esterna del S.I.TO;
- contribuire a migliorare i livelli di salute e sicurezza sul lavoro;
- prevedere il monitoraggio continuo del Sistema effettuato preferibilmente con personale interno.

Per l'impostazione del Sistema di Gestione della Sicurezza sono state prese come riferimento:

- le Linee Guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) – Guida Operativa - Ottobre 2003;
- le Linee Guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) – Manuale del sistema - Ottobre 2003;
- il Decreto Legislativo 81 del 09/04/2008 e s.m.

Nell'ambito della presente sezione del Modello Organizzativo vengono utilizzati i termini e le definizioni contenuti nella normativa di legge o tecnica in vigore, che si riportano per agevolare la consultazione del documento:

- Appaltatore: è il soggetto che si obbliga nei confronti del committente a fornire un'opera e/o una prestazione con mezzi propri.
- ASPP: Addetti al Servizio di Prevenzione e Protezione.
- attrezzatura di lavoro: qualsiasi macchina, apparecchio, utensile od impianto destinato ad essere usato durante il lavoro.
- Datore di lavoro (DdL): il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva, quale definita ai sensi della lettera i), in quanto titolare dei poteri decisionali e di spesa.
- Dirigente: dipendente che ricopre un ruolo caratterizzato da elevato grado di professionalità, autonomia e potere decisionale ed esplica le sue funzioni al fine di promuovere, coordinare e gestire la realizzazione degli obiettivi dell'impresa.
- DPI: Dispositivi di Protezione Individuale.
- Fabbricante: soggetto che produce e immette sul mercato o in servizio macchine, apparecchiature, impianti, dispositivi.

- Incidente: evento dovuto a causa fortuita che ha la potenzialità di condurre ad un infortunio o di provocare danni alle cose.
- Infortunio: evento dovuto a causa fortuita che produca lesioni corporali obiettivamente riscontrabili, in occasione di lavoro.
- Lavoratore: persona che, indipendentemente dalla tipologia contrattuale, svolge 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, esclusi gli addetti ai servizi domestici e familiari. Al lavoratore così definito è equiparato: il socio lavoratore di cooperativa o di società, anche di fatto, che presta la sua attività per conto delle società e dell'ente stesso; il soggetto beneficiario delle iniziative di tirocini formativi e di orientamento.
- Luogo di lavoro: i luoghi destinati a contenere posti di lavoro, ubicati all'interno dell'azienda ovvero dell'unità produttiva, nonché ogni altro luogo nell'area della medesima azienda ovvero unità produttiva, accessibile per il lavoro ed afferente alla struttura organizzativa del datore di lavoro pubblico o privato.
- Malattia professionale: evento morboso contratto a causa e nell'esercizio delle lavorazioni svolte.
- Medico competente (MC): medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 del D.Lgs. 81/08, che collabora, secondo quanto previsto all'articolo 29, comma 1, con il datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al presente decreto.
- Pericolo: la proprietà intrinseca di un agente, una condizione o una situazione, di poter produrre effetti nocivi.
- Posto di lavoro: postazioni, fisse o variabili, in cui il lavoratore espleta la sua mansione.
- Preposto: soggetto che ha la responsabilità della vigilanza e del controllo dell'operato di altri lavoratori.
- Rappresentante dei lavoratori per la sicurezza (RLS): persona, ovvero persone, eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro, di seguito denominato rappresentante per la sicurezza.
- Requisiti legali: norme di legge e/o regolamenti di livello comunitario, statale, locale, ed ogni impegno assunto volontariamente applicabile all'organizzazione in materia di SSL.
- Responsabile del servizio di prevenzione e protezione (RSPP): persona in possesso delle capacità e dei requisiti professionali necessari, designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi.
- Responsabile del SGSL (RSGSL): soggetto incaricato dal DdL, dotato di adeguata capacità ed autorità all'interno dell'azienda, a cui è affidato in tutto o in parte il compito,

indipendentemente da ulteriori responsabilità aziendali, di coordinare e verificare che il SGSL sia realizzato in conformità alle Linee Guida UNI-INAIL. (Linee Guida UNI-INAIL).

- Rischio: la probabilità che si raggiunga il potenziale nocivo nelle condizioni di utilizzazione o esposizione.
- Servizio di prevenzione e protezione dai rischi (SPP): insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali nell'azienda, ovvero unità produttiva.
- SGSL: Sistema di Gestione della Salute e Sicurezza sul Lavoro.
- SSL: Sicurezza e Salute dei Lavoratori.
- Terzi: soggetti diversi dal datore di lavoro, dai dirigenti, dai preposti e dai lavoratori, che possono, a qualsiasi titolo, trovarsi all'interno dei luoghi di lavoro o che possono essere influenzati o influenzare le attività lavorative e/o le condizioni di prevenzione.
- Unità produttiva: stabilimento o struttura finalizzata alla produzione di beni o servizi, dotata di autonomia finanziaria e tecnico-funzionale.
- Valutazione dei rischi (VDR): valutazione globale e documentata di tutti i rischi per la salute e sicurezza dei lavoratori presenti nell'ambito dell'organizzazione in cui essi prestano la propria attività, finalizzata ad individuare le adeguate misure di prevenzione e di protezione e ad elaborare il programma delle misure atte a garantire il miglioramento nel tempo dei livelli di salute e sicurezza.

4.1.a) Elementi del sistema di gestione per la salute e sicurezza nei luoghi di lavoro

L'organizzazione si struttura affinché il Sistema di Gestione della Sicurezza venga mantenuto attivo per mezzo di un processo dinamico partendo dalla Politica della Gestione Aziendale e si sviluppa in una Programmazione / Pianificazione, Attuazione, Controlli e Verifiche, Riesami e Miglioramenti continui dei propri processi.

La capacità del Sistema di Gestione di raggiungere gli obiettivi prefissati deriva dal coinvolgimento e dall'impegno di tutti all'interno dell'azienda ognuno per quanto di competenza nell'ambito della funzione svolta.

I modi per assicurare l'efficace controllo delle attività e delle eventuali azioni correttive, vengono specificati in apposite procedure.

La Società considera il Sistema di Gestione della Sicurezza sul Lavoro (SGSL), parte del Modello di Organizzazione, Gestione e Controllo (MOG), per tale motivo la Politica dell'Azienda, racchiude gli scopi

e gli obiettivi della legislazione, norme e linee guida di riferimento così che, anche per quanto riguarda gli obiettivi riferiti alla Salute e Sicurezza, gli impegni del Datore di Lavoro sono maggiormente messi in evidenza.

Ritenuto soddisfatto il monitoraggio e controllo dei requisiti cogenti, è volontà da parte del Datore di Lavoro di coinvolgere in modo attivo il personale al fine di garantire un continuo miglioramento delle strutture e della realtà lavorativa nonché di ridurre sempre di più le situazioni di rischio potenziale sia per i dipendenti che per le parti terze.

La politica della Gestione Aziendale viene redatta, revisionata e comunicata nei termini previsti dal MOG con cadenza minima annuale con la finalità di garantire che la stessa sia sempre valida, aggiornata ed applicata all'interno dell'azienda. Il Datore di Lavoro è responsabile della comprensione, attuazione e sostegno della Politica Aziendale, sia all'interno della propria azienda, che all'esterno.

Il Datore di Lavoro ha definito la propria politica aziendale allo scopo di indicare la visione, i valori essenziali e le convinzioni dell'azienda sul Modello Organizzativo di Gestione e Controllo e del suo Sistema di Gestione per la Sicurezza.

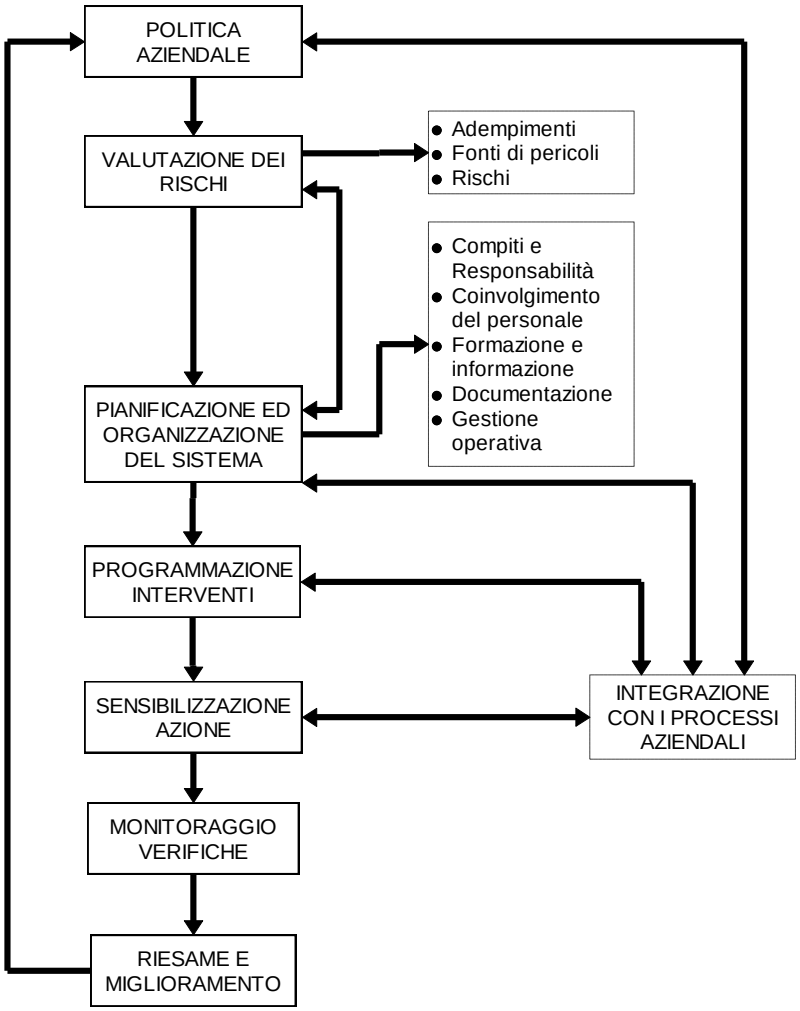
L'applicazione del Modello Organizzativo e l'implementazione del Sistema di Gestione per la Sicurezza ha, per la Società i seguenti obiettivi e impegni:

- prevenire la commissione di reati in materia di sicurezza sul lavoro;
- prevenire la commissione di reati societari, che ad oggi non si sono mai verificati;
- coinvolgere i lavoratori e i loro rappresentanti nel SIG;
- aumentare l'efficienza dell'organizzazione e le proprie prestazioni in riferimento alla tutela della Salute e Sicurezza sul lavoro;
- evitare i costi complessivi della SSL compresi quelli derivanti da incidenti, infortuni e malattie, ad oggi mai verificatesi, correlate al lavoro minimizzando i rischi cui possono essere esposti i dipendenti o i terzi;
- migliorare continuamente la capacità di adattamento all'evoluzione delle normative volontarie e cogenti;
- effettuare almeno un ciclo di verifiche del Sistema, anche verso i fornitori, effettuato preferibilmente con personale interno;
- attivare l'applicazione dei moduli e delle procedure del Sistema di Gestione per la Sicurezza in tutti i settori di riferimento;
- avviare la fase di certificazione dell'Azienda SITO nel settore della Gestione della Sicurezza Integrata secondo le linee internazionali.

4.1.b) Pianificazione per l'identificazione del pericolo, valutazione e controllo del rischio

L'organizzazione del S.I.TO stabilisce le procedure per la costante individuazione dei pericoli, la valutazione dei rischi e l'attuazione delle necessarie misure di controllo.

Il diagramma di flusso seguente rappresenta lo schema del Sistema di Gestione e dell'interrelazione tra i principali processi.



L'aspetto della Salute e Sicurezza, per la Società costituisce la base di un approccio metodologico di controllo del proprio Sistema Gestionale. Per questo motivo, nell'implementazione del SGSL, allo scopo di migliorare continuamente le proprie prestazioni nei confronti dei dipendenti e di terzi, l'organizzazione si avvale dell'Organo di Vigilanza, quale sistema di controllo al fine di:

- garantire che i risultati ottenuti siano oggetto di analisi;
- fissare sistematicamente nuovi obiettivi di miglioramento.

Poiché gli ambienti e i siti coinvolti nel processo produttivo sono tra loro di diversa tipologia strutturale (uffici, cantieri e attività di logistica), l'organizzazione si è dotata di strumenti di comunicazione finalizzata a garantire una ricca raccolta di informazioni.

Incontri programmati tra i lavoratori (o i loro rappresentanti) e il Datore di Lavoro (o i rappresentanti del Datore di Lavoro) hanno lo scopo di avere una puntuale identificazione dei pericoli e valutazione dei rischi.

L'obiettivo è quello di utilizzare sempre di più azioni preventive e non correttive.

4.1.c) Identificazione dei rischi per la sicurezza e la salute

La Società ha individuato i pericoli connessi con la salute e la sicurezza dei lavoratori effettuando una analisi a partire delle attività svolte nel sito.

Valutazione Rischi di Reati come da D.Lgs. 231

La metodologia del Modello Organizzativo consiste in:

1. Identificare le aree a rischio
2. Identificare i principali fattori di rischio
3. Sviluppare e migliorare il MOG stesso
4. Definire degli obiettivi di miglioramento

Per poter elaborare un Modello Organizzativo che garantisca la *Governance* aziendale è quindi necessario conoscere bene le attività a rischio e quindi avere una mappatura aggiornata dei rischi. All'interno dei processi aziendali devono essere individuate le attività che comportano:

- la tenuta di rapporti con Pubblica Amministrazione;
- la gestione di informazioni a valenza economica.

Nell'ambito delle attività a rischio s'individuano i fattori di rischio / interventi strumentali tramite i quali potrebbero crearsi le condizioni per commettere reati (es. Gestione oggettistica, acquisizione consulenze, sponsorizzazioni, ecc).

L'analisi sui fattori di rischio è una operazione che deve essere fatta:

- In maniera preliminare allo sviluppo del Modello Organizzativo;
- successivamente almeno una volta all'anno per valutare la frequenza e il grado di incidenza dei rischi;
- ogni qualvolta vi siano cambi significativi nell'organizzazione o nei processi/attività dell'azienda.

La valutazione dei rischi legati ai reati deve essere fatta dall'Organismo di Vigilanza. Tale valutazione viene effettuata, per ogni mansione, utilizzando un modulo per la "*Check list* Rischi Reati".

Valutazione Rischi per la Sicurezza sul Lavoro

Il procedimento di individuazione e quantificazione dei pericoli e relativa valutazione dei rischi viene fatta dal datore di lavoro in collaborazione con il RSPP ed il Medico Competente, secondo gli artt. 17, 28 e 29 del D.lgs 81/08, è stato suddiviso nelle seguenti fasi:

- identificazione dei pericoli;
- identificazione dei lavoratori e/o di terzi esposti a rischi potenziali;
- valutazione dei rischi qualitativa (si/no) e quantitativa (quanto);
- studio della possibilità di eliminare/ridurre i rischi esistenti;
- definizione delle priorità degli interventi;
- programmazione del monitoraggio permanente.

In particolare nell'effettuare la valutazione vengono seguiti gli orientamenti sotto elencati:

- osservazione dell'ambiente di lavoro;
- identificazione e analisi delle mansioni svolte;
- osservazione del lavoro in fase di esecuzione;
- esame di fattori esterni che possono avere effetti sul posto di lavoro.

La valutazione dei rischi è un processo permanente e richiede per essere esaustiva un procedimento articolato in tre fasi:

1. valutazione preliminare volta a considerare i rischi ben noti e/o più prevedibili e/o in grado di causare danni più che lievi;
2. programma di valutazioni successive di approfondimento per i rischi meno prevedibili e/o meno probabili e/o meno noti;
3. programma di valutazione permanente.

Le possibili fonti di rischio sono divise in 5 categorie:

1. fonti di pericolo attivo
2. fonti di pericolo passivo
3. fonti di pericolo per la salute
4. fonti di mancato benessere
5. fonti di organizzazione del lavoro

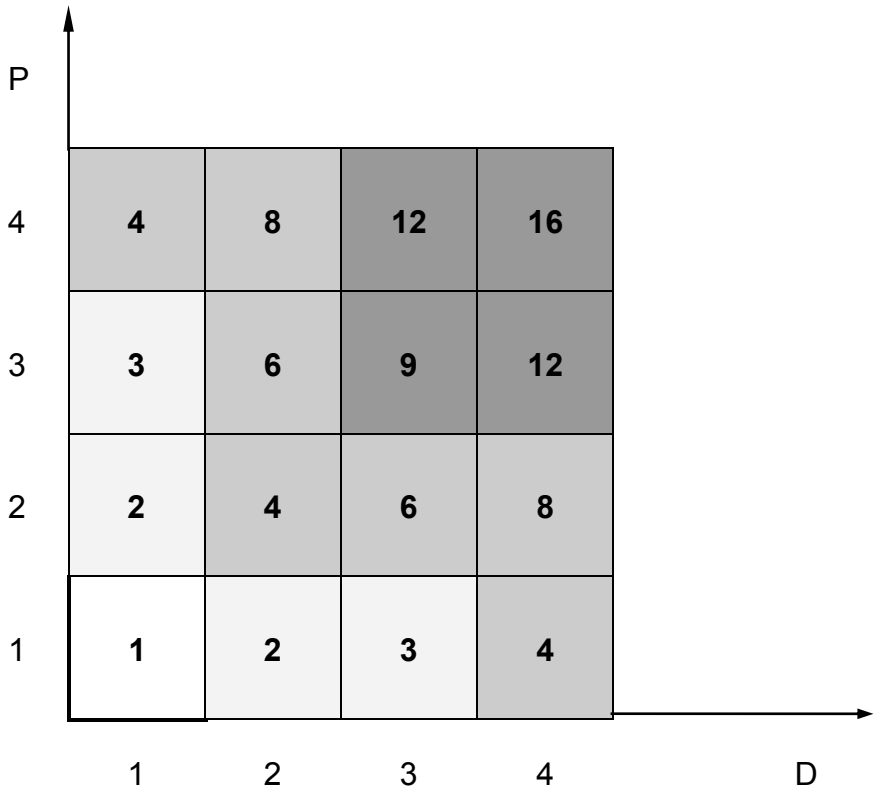
La quantificazione del **rischio** deriva dalla possibilità di definire il rischio come prodotto della Probabilità (P) di accadimento per la gravità del Danno (D) atteso: **R = P x D**.

La definizione della **Scala delle Probabilità** fa riferimento principalmente all' esistenza di una correlazione più o meno diretta tra la carenza riscontrata ed il danno ipotizzato; in secondo luogo alla esistenza di dati statistici noti a riguardo, a livello di azienda o di comparto di attività; infine, un criterio di notevole importanza, è quello del giudizio soggettivo di chi è direttamente coinvolto nella realtà lavorativa, che spesso costituisce l'unica fonte di tipo pseudo-statistico disponibile.

La **Scala di Gravità del Danno** chiama invece in causa la competenza di tipo sanitario e fa riferimento principalmente alla reversibilità o meno del danno, distinguendo tra infortunio ed esposizione acuta o cronica.

L'insieme dei dati rilevati viene condensato nella compilazione di una matrice per la valutazione del rischio e della sua criticità, il cui incrocio dei dati porta alla definizione di tre aree di intervento con conseguenti azioni, sia allega matrice utilizzata per la valutazione del rischio.

Definiti la Probabilità (P) e la gravità del Danno (D), il rischio (R) viene calcolato con la formula R = P x D e si può raffigurare in una rappresentazione a matrice, avente in ascisse la gravità del Danno ed in ordinate la Probabilità del suo verificarsi.



In tale matrice i rischi maggiori occupano le caselle in alto a destra, quelli minori le posizioni in basso a destra, con tutta la serie disposizioni intermedie.

Una tale rappresentazione è un importante punto di partenza per la definizione delle priorità e la programmazione temporale degli interventi di prevenzione e protezione da adottare.

Come da normativa, secondo l'art. 35 del D.Lgs. 81/08, viene nell'ambito della riunione annuale, alla presenza di tutti gli attori coinvolto nel sistema Sicurezza Lavoro, presentata la Valutazione dei Rischi e quindi illustrate gli adempimenti svolti e le misure da adottare.

I rischi individuati che vengono considerati potenzialmente pericolosi devono essere documentati dal RSPP.

Dalla valutazione dei rischi deriverà il carattere di urgenza o di priorità con cui intervenire sul singolo rischio. I rischi devono essere valutati nelle seguenti condizioni operative:

- attività lavorative ordinarie: condizioni abituali di esercizio;
- attività lavorative straordinarie: condizioni legate ad eventi anomali occasionali;
- situazioni di emergenza: condizioni legate ad eventi accidentali.

La valutazione deve tenere conto di tutte le strutture, i luoghi ed i metodi di lavoro, le macchine e gli impianti, le attrezzature ed eventuali sostanze utilizzate.
Inoltre la valutazione dei rischi deve tenere conto delle attività di subappaltatori, fornitori o visitatori esterni che accedono al sito.

Periodicamente il RSPP, nell'ottica del miglioramento continuo, riesamina i processi aziendali con lo scopo di aggiornare, se necessario, l'elenco dei rischi.
Tale attività è indispensabile qualora intervengano modifiche e integrazioni dei processi aziendali o l'introduzione di nuovi prodotti e/o servizi.

4.1.d) Requisiti legali e di altra natura

La Società si avvale dell'Organo di Vigilanza anche al fine di garantire l'applicazione e l'adeguamento del Modello Organizzativo in merito alle variazioni ed implementazioni delle normative relative alle proprie attività.

Ciascuna nuova informazione in merito alle normative o di altro tipo, dovrà essere trasmessa a tutte le parti interessate assicurandosi che l'informazione venga correttamente recepita dai destinatari ed applicata nei tempi e nei modi prescritti.

L'interfaccia aziendale con l'Organo di Vigilanza per recepire aggiornamenti in materia di Sicurezza è il RSPP. A questo è demandato il compito di organizzare successivamente nei tempi e nei modi dovuti, la corretta comunicazione interna e/o esterna.

La normativa e legislazione di riferimento viene riportata in apposito modulo: "Elenco dei requisiti legali e volontari applicabili".

4.1.e) Obiettivi

Nel rispetto della Politica Aziendale, gli obiettivi per il miglioramento delle prestazioni in materia di Salute e Sicurezza dei lavoratori e quelli finalizzati alla valutazione dell'efficienza dei processi di gestione della Sicurezza vengono definiti, nel contesto del Piano di Miglioramento e del Programma del Modello Organizzativo, in occasione degli incontri periodici per il Riesame.

Il Datore di Lavoro individua le funzioni aziendali cui affidare la responsabilità per il raggiungimento di ogni specifico traguardo precedentemente definito sempre su base oggettiva e verifica l'esito delle azioni stabilite indicendo incontri semestrali a cui partecipano tutte le funzioni responsabili aziendali.

4.1.f) Programma di gestione per la salute e sicurezza nei luoghi di lavoro

Al fine di raggiungere gli obiettivi prefissati, il Datore di Lavoro sviluppa strategie di controllo e di monitoraggio degli obiettivi stessi definendo non solo un calendario che fornisca delle precise scadenze alle azioni da intraprendere e ai risultati da raggiungere, ma prevedendo responsabilità e figure coinvolte in dette azioni.

Gli obiettivi, le azioni e le figure aziendali coinvolte vengono registrate sugli stessi documenti sui quali vengono definiti i traguardi e gli obiettivi di miglioramento. Tali documenti costituiscono dunque i documenti di programmazione per la Gestione della Sicurezza.

4.1.g) Attuazione e funzionamento: struttura e responsabilità

Affinché il Sistema di Gestione della Sicurezza risulti efficace, occorre che il Datore di Lavoro designi ruoli e responsabilità con estrema puntualità.
Nell'allegato B al presente Modello si riporta l'Organigramma aziendale dove vengono individuate le funzioni aziendali.

Il Datore di Lavoro stabilisce di affidare l'incarico di Responsabile del Sistema di Gestione della Sicurezza alla funzione Amministrazione, che oltre alle sue normali attività, descritte nel mansionario aziendale, supporterà e rappresenterà il Datore di Lavoro nella gestione del SGSL.

Il Datore di Lavoro coinvolge e responsabilizza, ancora di più di quanto già non lo faccia nei termini della normativa cogente, sia la figura del Rappresentante dei Lavoratori (RLS), che del Servizio di Prevenzione e Protezione (RSPP).

Tali figure sono chiamate a rispondere in primo luogo al Responsabile del Sistema di Gestione della Sicurezza (RSGSL), il quale, per le responsabilità che gli sono state affidate, è tenuto a garantire che le informazioni raccolte arrivino al Datore di Lavoro complete di indicazioni per possibili azioni di miglioramento e/o di prevenzione.

RSGSL assicura, inoltre, che tutti i dipendenti e collaboratori siano in possesso di tutte le informazioni che la normativa cogente prevede. Ha inoltre il compito di assicurare il coinvolgimento del personale, ai fini di intraprendere adeguate azioni preventive, coordinando i vari responsabili dei settori aziendali, organizzando riunioni periodiche, interviste al personale, ecc.

4.1.h) Attuazione e funzionamento: addestramento, consapevolezza e competenza

Il Datore di Lavoro definisce le modalità affinché tutto il personale, ad ogni livello, sia consapevole dei potenziali rischi legati alle proprie attività ed alle attività aziendali in genere.

Come per la formazione relativa ad altri aspetti, anche per la Sicurezza, in occasione del Riesame del Datore di Lavoro, vengono programmate le attività formative specifiche per l'anno seguente. RSGSL provvede ad organizzare tale formazione, anche tramite i rappresentanti dei lavoratori e, successivamente, a monitorarne e registrarne gli esiti.

La formazione verrà definita per specifica competenza di ciascuna figura coinvolta nel processo produttivo del S.I.TO, come già previsto dalla normativa cogente di riferimento in materia di Salute e Sicurezza nei luoghi di lavoro; sarà peraltro arricchita di tutte le tematiche riguardanti la corretta applicazione del Sistema di Gestione della Sicurezza sul Lavoro.

4.1.i) Attuazione e funzionamento: consultazione e comunicazione

Il Datore di Lavoro ritiene che la circolazione delle informazioni all'interno dell'Azienda sia un elemento fondamentale per garantire adeguati livelli di consapevolezza. Questa cultura aziendale viene trasmessa facilitando il flusso informativo sia nelle comunicazioni tra dipendenti e struttura dirigente che tra i dipendenti stessi.

Il personale viene periodicamente consultato sia tramite i Rappresentanti dei lavoratori che tramite il Responsabile del Sistema di Gestione o anche direttamente dal Datore di Lavoro stessa con colloqui interpersonali.

Caratteristiche della comunicazione interna

Tutte le informazioni, conoscenze, notizie, problematiche relative alla sicurezza sul lavoro e alla responsabilità amministrativa devono essere oggetto di comunicazione tra tutti i dipendenti e a tutti i livelli. L'azienda predispone idonee procedure per agevolare il flusso comunicativo tra le diverse funzioni aziendali sia in senso orizzontale sia in senso verticale, in genere l'azienda utilizza le comunicazioni via e-mail e bacheche.

Allo scopo di favorire la cooperazione tra i soggetti coinvolti l'azienda predispone metodologie di consultazione del Rappresentante dei lavoratori per la sicurezza (RLS) e di raccolta delle segnalazioni, osservazioni e proposte dei lavoratori rivolte al datore di lavoro.

Caratteristiche della comunicazione esterna

L'azienda si attiva per informare le persone esterne (clienti, visitatori e altri soggetti) sugli eventuali rischi collegati alla loro presenza in sede.

L'azienda gestisce con specifiche procedure (DUVRI) i rapporti con fornitori, manutentori esterni, committenti di attività esterne all'azienda per ridurre al minimo i rischi collegati alle interferenze tra le attività.

Considerata la peculiarità della comunicazione con soggetti esterni, l'azienda utilizzerà strumenti facilmente comprensibili e di immediata individuazione come: immagini fotografiche, segnaletica verticale ed orizzontale, cartellonistica, disegni, note scritte ed affisse in punti strategici.

4.1.l) Documentazione e controllo dei dati e dei documenti

La documentazione completa del Modello Organizzativo di gestione e controllo, è costituito da:

- Modello Organizzativo di gestione e controllo e della Sicurezza sul lavoro (MOG);
- La relativa modulistica di registrazione;
- Normativa cogente di riferimento;

I documenti e le registrazioni relative agli aspetti del MOG e della Sicurezza vengono gestiti facendo riferimento a modalità descritte in specifica modulistica.

4.1.m) Controllo operativo

L'organizzazione identifica le attività associate a rischi e conseguentemente stabilisce, in accordo alla normativa cogente di riferimento, le misure di controllo da adottare.

Vengono puntualmente elaborati specifici documenti di Valutazione del Rischio, del rischio dei videoterminali, della misurazione delle vibrazioni, nonché specifici DUVRI per ogni appalto che viene aperto ed in cui deve andare ad intervenire il personale e/o suoi subappaltatori.

Osservazione dei comportamenti pericolosi

Ogni anomalia riscontrata nel luogo di lavoro, sia di gestione e controllo sia per la salute e sicurezza sul luogo di lavoro, deve essere documentata su idoneo strumento a cura del dirigente o del lavoratore utilizzando il modulo "Osservazione delle situazioni pericolose e comportamenti pericolosi".

Le azioni correttive/preventive proposte in questi casi da chi ha effettuato l'osservazione, dal RSGSL o RSPP (in caso di osservazione legata al SGSL) oppure dall'Organo di Vigilanza (in caso di osservazione legata al Modello Organizzativo aziendale), sono verifica ed eventualmente, se approvate dalla DIR, attuate a cura delle funzioni aziendali coinvolte nell'azione.

L'attuazione delle azioni correttive è verificata durante il riesame del MOG.

Le azioni correttive e preventive proposte durante la gestione di infortuni, incidenti e rilevazione comportamenti e situazioni pericolose devono essere monitorate e verficate la loro efficacia in modo da evitare il ripetersi di situazioni difformi, a rischio o non conformi.

Infortunio

Ogni infortunio deve essere gestito secondo le seguenti fasi:

- attivazione della procedura di primo soccorso;
- registrazione dell'evento in apposito registro;
- attivazione della procedura per l'analisi.

Il report di infortunio può essere compilato dal preposto con il coinvolgimento del RLS e dei presenti al momento dell'infortunio e/o da un superiore dell'infortunato.

Successivamente il report di infortunio viene analizzato dai compilatori con il RSGSL e il RSPP che lo raccolgono e provvedono a definirne la gestione (azioni correttive adottate e/o da adottare, responsabile dell'attuazione, tempi di attuazione). Gli infortuni vengono esaminati al momento dell'accadimento per la gestione, ed al momento del riesame del MOG per l'ulteriore analisi e verifica delle soluzioni adottate.

Incidente

In caso di incidente i lavoratori coinvolti, i presenti, i testimoni riferiscono al dirigente le cause oggettive, i comportamenti pericolosi, le possibili azioni correttive, con idonea modulistica.

Successivamente il report di incidente viene analizzato dai compilatori con il RSGSL ed il RSPP che lo raccolgono e provvedono a definirne la gestione (azioni correttive adottate e/o da adottare, responsabile dell'attuazione, tempi di attuazione). Gli incidenti vengono esaminati al momento dell'accadimento per la gestione, ed al momento del riesame del MOG per l'ulteriore analisi e verifica delle soluzioni adottate.

4.1.n) Preparazione e risposta alle emergenze

Il Datore di Lavoro con il supporto delle figure preposte, sviluppa adeguati Piani di emergenza per individuare e rispondere tempestivamente a particolari potenziali situazioni d'emergenza e prevenire ed attenuare ogni possibile danno ed incidente che da questi ne potrebbero conseguire.

Tali piani vengono elaborati dal RSPP e riesaminati dal Datore di Lavoro, oltre che durante i periodici Riesami anche dietro segnalazioni specifiche, soprattutto dopo il verificarsi di incidenti e/o situazioni di emergenze reali.

L'Organizzazione provvede inoltre all'addestramento teorico e pratico del personale in riferimento al piano di emergenza, traendo spunto anche da queste attività per eventuali azioni di miglioramento.

Il Piano di emergenza è così strutturato:

- identificazione delle potenziali situazioni di emergenza;
- individuazione del/i responsabile/i e dei relativi compiti;
- individuazione delle azioni da compiere;
- unità preposta da avvertire (VVFF, Soccorsi, ecc…) ed interfaccia aziendale;
- procedure di evacuazione;
- comunicazioni interne (altre strutture aziendali esterne al luogo dell'emergenza);
- comunicazioni esterne (strutture adiacenti o limitrofe);
- localizzazione ed utilizzo dei DPI;

- sistemi di allarme;
- vie di fuga.

Tutte le attrezzature previste per eventuali situazioni di emergenza dovranno essere mantenute efficienti e verificate periodicamente per il loro uso specifico.

Il RSPP ha la responsabilità di detta manutenzione e della relativa registrazione.

4.1.o) Azioni correttive e di controllo: misurazione e monitoraggio delle prestazioni

Il Sistema di Gestione della Sicurezza della Società viene monitorato costantemente dalle varie figure coinvolte nel processo produttivo ciascuna per le proprie specifiche competenze.

Ogni figura è stata messa in grado di valutare la corretta applicazione delle disposizioni fornite al fine di tutelare la Salute e la Sicurezza nei luoghi di lavoro.

Il RSSP si coordina periodicamente con i vari responsabili dei settori e di attività (uffici, cantieri, attività logistica) ed ha con loro confronti interpersonali. Una lista di riferimento ed apposita scheda facilitano le registrazioni, soprattutto sugli appalti esterni, sia per quanto riguarda i rischi corsi che per i rischi potenziali.

Tali registrazioni hanno inoltre lo scopo di monitorare il corretto utilizzo da parte del personale dei dispositivi di sicurezza individuali, ove previsto.

4.1.p) Azioni correttive e di controllo: infortuni, incidenti, azioni correttive e preventive

Nel caso della Gestione della Sicurezza, gli scostamenti dalle procedure previste, possono portare, non solo a Osservazioni del Sistema, ma anche ad incidenti e/o veri e propri infortuni.

L'organizzazione stabilisce che in caso di infortunio e/o incidente, RSPP ha la responsabilità di raccogliere i dati, registrare gli avvenimenti e prendere le misure necessarie per ridurre al minimo le conseguenze causate dall'evento.

Anche l'infortunio e/o l'incidente è motivo, nel Sistema di Gestione della Sicurezza, dell'apertura di una Osservazioni e di una conseguente azione correttiva (AC) da intraprendere.

E' RSGSL che ha il compito di stabilire le azioni e le responsabilità necessarie per risolvere le situazioni non conformi verificatesi.

E' sempre del RSGSL il compito di monitorare l'attuazione dell'azione prevista (AP), registrarne la chiusura e i risultati raggiunti.

RSGSL, in seguito all'analisi di situazioni e/o di dati rilevati nell'ambito dell'organizzazione, può ritenere opportuno intraprendere una o più Azioni Preventive al fine di evitare eventuali circostanze che potrebbero potenzialmente dare luogo a situazioni non conformi.

Se alcune procedure operative dovessero mutare a causa di AC o AP intraprese, si dovrà provvedere a revisionare conseguentemente la documentazione in cui queste vengono descritte.

4.1.q) Azioni correttive e di controllo: registrazioni e loro gestione

Le Registrazioni del Sistema di Gestione della Sicurezza vengono curate come tutta la documentazione della Società con modalità specifiche.

Le registrazioni specifiche del Sistema di Gestione Sicurezza sono:

- registrazioni della formazione e dell'addestramento;
- verifiche ispettive (interne e da parte dell'Organismo);
- rapporti di incidenti ed infortuni;
- registrazioni di verifiche/sopralluoghi;
- rapporti di verifiche mediche;
- rapporti di sorveglianza del sistema di gestione per la salute e sicurezza;
- *check list*;
- riesami del Datore di Lavoro;

4.1.r) Azioni correttive e di controllo: audit

Al fine di verificare la gestione degli aspetti aziendali relativi all'organizzazione e alla SSL, le modalità di realizzazione di tale gestione ed il rispetto dell'obiettivo di miglioramento continuo in questo ambito l'azienda prevede due livelli di monitoraggio:

- Monitoraggio di 1° livello
- Monitoraggio di 2° livello o Audit

Monitoraggio di 1° livello

Questo livello di monitoraggio prevede le verifiche del raggiungimento degli obiettivi relativi all'adozione delle misure di prevenzione e protezione e i progressi nell'attuazione di tali attività.
Tali monitoraggi, svolti in autocontrollo da parte dell'operatore adeguatamente formato o da parte del preposto o del dirigente.

Il RSGSL ha il compito di pianificare e coordinare l'attività di verifica del Sistema di Gestione della Sicurezza coinvolgendo le funzioni che hanno influenza sul Sistema da verificare

La pianificazione dei monitoraggi di 1° livello è definita dall'Organo di Vigilanza.

La documentazione relativa ai monitoraggi di 1° livello consiste nel siglare, a carico del RSPP e/o del RSGSL, le misure preventive e correttive riportate sul Piano di attuazione degli interventi collegato al documento di valutazione dei rischi. Detto piano conterrà tutti gli interventi previsti a seguito di diversi livelli e specificità della valutazione che possono essere oggetto di integrazioni ed aggiornamenti della stessa (aggiornamento generale del DVR, valutazione rischi, incendio, rumore, ecc.).

Monitoraggio di 2° livello o Audit

Questo tipo di verifica, che consiste in un sistema di monitoraggio interno, strutturato dall'azienda, viene eseguito dall'OdV che ha una formazione adeguata, indipendenti dall'area/settore che viene preso in esame.

I monitoraggi di 2° livello devono essere effettuati almeno una volta all'anno per la parte di MOG relativa alla sicurezza sul luogo di lavoro

Per quanto riguarda la conduzione degli audit di 2° livello saranno quindi presi in esame i documenti contenenti le seguenti indicazioni:

- gli obiettivi delle diverse figure aziendali, lo stato di attuazione ed efficacia degli stessi;
- il risultato dei monitoraggi di 1° livello;
- le azioni preventive e correttive proposte, complete del loro stato di attuazione;
- lo stato di attuazione della gestione della documentazione del sistema;
- lo stato di attuazione delle procedure previste dal sistema.

Le azioni correttive e preventive che scaturiscono dagli audit, riportate nel Verbale di verifica saranno inserite tra i documenti che saranno riverificati in sede di riesame del sistema.

I compiti dell'OdV nell'ambito dell'audit sono di:

- stabilire i requisiti del monitoraggio in funzione degli obiettivi;
- agire in conformità ai requisiti stabiliti per il monitoraggio;

- seguire le procedure;
- raccogliere ed analizzare elementi rilevanti e sufficienti che consentano di giungere a conclusioni relative all'efficacia MOG e relativo SGSL sottoposto a monitoraggio;
- prestare attenzione agli elementi che possono influenzare gli esiti del monitoraggio;
- documentare i risultati del monitoraggio;
- verificare l'efficacia delle misure correttive adottate conseguentemente al monitoraggio;
- analizzare i dati relativi a situazioni e comportamenti pericolosi o a rischio, non conformità;
- segnalare le azioni necessarie per prevenire situazioni e comportamenti pericolosi o a rischio, non conformità;
- confermare l'efficacia delle azioni correttive e preventive eseguite.

Le verifiche relative al SGSL sono estese a quanto stabilito in apposite schede di verifica e prevedono la raccolta dei casi di infortuni, incidenti e comportamenti e situazioni pericolose dei quali si terrà conto nel riesame del sistema.

I risultati del monitoraggio e le eventuali azioni preventive o correttive individuate vengono verbalizzate da parte dell'OdV.

I risultati degli audit vengono discussi con il Datore di Lavoro durante le riunioni di riesame e miglioramento del sistema e utilizzati per stabilire se il sistema è conforme a quanto pianificato, è correttamente applicato, mantenuto attivo e permette di raggiungere gli obiettivi consentendo al vertice aziendale l'adozione delle decisioni strategiche di propria competenza.

La predisposizione di una azione correttiva comporta sempre l'obbligo di una successiva immediata verifica che risulti in grado di accertare il superamento della non conformità. Tale condizione deve essere indicata nella verifica di efficacia della stessa azione.

La pianificazione dell'audit viene effettuata durante le riunioni di riesame e miglioramento del sistema.

Nel corso di ogni audit vengono riesaminati i risultati di quelli svolti in precedenza; le registrazioni degli audit sono riportate su specifici verbali a cura dell'OdV e vengono analizzate nel corso del Riesame.

4.1.s) Riesame

L'OdV, riesamina periodicamente il Modello di Organizzazione, Gestione e Controllo implementato in azienda ed il relativo il Sistema di Gestione per la Sicurezza, al fine di verificare l'adeguatezza e l'efficacia dello stesso, in particolare è costantemente verificato il pieno soddisfacimento dei requisiti normativi e degli obiettivi aziendali definiti nella Politica aziendale, al fine verificare la corretta gestione del MOG e del SGSL.

4.1.t) Riesame: modalità operativa

L'Organo di Vigilanza, monitora costantemente dati, informazioni, relazioni, reporting e quant'altro possa essere necessario per l'efficace attuazione dei riesami del MOG.

Al termine dei processi di monitoraggio, all'Organo di Vigilanza provvede alla valutazione dei risultati ed al riesame del MOG al fine di valutare se lo stesso sia conforme a quanto pianificato, correttamente applicato, mantenuto attivo e risulti sempre idoneo al conseguimento degli obiettivi prefissati dalla politica aziendale.

Alla conclusione del riesame, il Datore di Lavoro e l'Organismo di Vigilanza tengono conto principalmente:

- dei risultati forniti dal monitoraggio del sistema;
- della esecuzione delle azioni correttive e preventive attuate a seguito delle non conformità riscontrate durante tutte le attività di implementazione del sistema;
- delle statistiche sugli infortuni e situazioni a rischio per il MOG;
- dei rapporti sulla efficacia del sistema di gestione, delle prestazioni complessive e della valutazione e controllo del rischio;
- dell'andamento dei rapporti con i fornitori;
- della valutazione delle conoscenze e delle esigenze di formazione.

L'RSGSL, nel periodo antecedente il Riesame, provvede a raccogliere tutti i dati necessari per le valutazioni dei vari aspetti del SGSL (verbali degli audit, rapporti, osservazioni e rilevazioni, AC e AP, valutazione dei fornitori, esiti della formazione, ecc.) e li fornisce all'OdV affinché possa analizzare e trarne le considerazioni opportune.

Questa verifica viene formalizzata in opportuna modulistica, su cui vengono sintetizzate le evidenze esaminate, le valutazioni effettuate e le decisioni prese.

Il Verbale di riesame e gli eventuali allegati devono essere catalogati, archiviati e conservati in apposito dossier facilmente rintracciabile.

Inoltre, viene effettuato un riesame di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'Organismo di Vigilanza e dagli altri soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal D.Lgs. 231/2001, dalla Legge 123/07 e dal D.Lgs. 81/08, con raccolta di dati.

I risultati del Riesame dovranno permettere la pianificazione di nuovi obiettivi e la verifica della validità della Politica aziendale.

L'esito del riesame viene redatto sotto forma di un rapporto, da sottoporre all'attenzione del Consiglio di Amministrazione di S.I.TO, che evidenzi le possibili manchevolezze e suggerisca le azioni da intraprendere.

PARTE SPECIALE 5

Delitti in materia di violazione del diritto d'autore (art. 25 *nonies*)

I principali *Processi Sensibili* individuati sono i seguenti:

- gestione di sistemi informatici e telematici, con particolare riferimento alla seguente attività a rischio:
  - ✓ gestione delle licenze software.

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico nonché nelle procedure aziendali, ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- divieto per tutti gli operatori (dirigenti, dipendenti, collaboratori) di installare, modificare, disinstallare software (o hardware) senza preventiva autorizzazione della referente dell'area CED aziendale;
- individuare le figure di Amministratore di Sistema, ottemperare agli obblighi di legge previsti per tali figure e mantenere un idoneo livello di attenzione sull'operato di tali soggetti;
- provvedere senza indugio alla disattivazione degli account attribuiti agli Amministratori al termine del relativo rapporto contrattuale;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- nei rinnovi e/o nuovi contratti con i partners commerciali, consulenti e fornitori deve essere contenuta apposita clausola che regoli le conseguenze in caso di violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali);
- definire, documentare, implementare, monitorare e periodicamente aggiornare un programma di informazione / formazione in materia di sicurezza informatica a favore, almeno, degli incaricati.

Le procedure aziendali significative per la prevenzione dei reati in oggetto, che si richiamano integralmente in questa sede anche nella loro eventuale e successiva modificazione ed implementazione resa necessaria per garantirne la costante adeguatezza, sono le seguenti:

- Codice Etico
- P_08 Procedura affidamento e contratti di appalto

PARTE SPECIALE 6

Ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25 *octies*)

I principali *Processi Sensibili* individuati sono i seguenti:

- gestione dei flussi finanziari;
- gestione dei rapporti commerciali con particolare riferimento alle transazioni finanziarie;
- "area tax":
  - ✓ adempimenti fiscali;
- gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse dai soggetti pubblici;
- gestione del sistema di tracciabilità delle singole operazioni svolte.

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico nonché nelle procedure aziendali, ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- le operazioni di rilevante entità devono essere concluse con persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli e accertamenti;
- mantenere evidenza, su archivi informatici, delle transazioni effettuate su conti correnti aperti presso Stati in cui permangono regole di trasparenza più blande (c.d. Paesi *off shore*) per importi superiori, complessivamente, alle soglie previste dalla normativa di riferimento;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- nei contratti con consulenti, partners e fornitori deve essere contenuta apposita clausola che regoli le conseguenze in caso di violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 nonché del presente Modello;
- non utilizzare strumenti anonimi per il compimento di qualsiasi operazione finanziaria;
- assicurare la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati.

Le procedure aziendali significative per la prevenzione dei reati in oggetto, che si richiamano integralmente in questa sede anche nella loro eventuale e successiva modificazione ed implementazione resa necessaria per garantirne la costante adeguatezza, sono le seguenti:

- Regolamento interno “tracciabilità dei flussi finanziari”
- Regolamento per la disciplina dei rimborsi spese a favore degli amministratori, componenti del Collegio Sindacale, dirigenti e dipendenti
- P_01 Contabilità e bilancio
- P_02 Operazioni monetarie e finanziarie
- P_03 Finanziamenti pubblici
- P_04 Omaggi e liberalità
- P_09 Procedura di esecuzione dei pagamenti
- P_11 Benefits

PARTE SPECIALE 7

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

I principali *Processi Sensibili* individuati sono i seguenti:

- assunzione e gestione del personale (compresi i soggetti appartenenti a categorie protette);

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico nonché nelle procedure aziendali, ha individuato i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- accertare l'esistenza del permesso di soggiorno al momento dell'assunzione ed il controllo sulla scadenza ed il rinnovo dello stesso;
- verificare a campione il permesso di soggiorno dei lavoratori stranieri;
- verificare il sistema di controllo sui lavoratori di società esterne che comunque svolgono attività all'interno della Società o per conto della Società sulla base di un contratto di appalto di servizi;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- nei rinnovi e/o nuovi contratti con i partners commerciali, consulenti e fornitori deve essere contenuta apposita clausola che regoli le conseguenze in caso di violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali).

Le procedure aziendali significative per la prevenzione dei reati in oggetto, che si richiamano integralmente in questa sede anche nella loro eventuale e successiva modificazione ed implementazione resa necessaria per garantirne la costante adeguatezza, sono le seguenti:

- Codice Etico
- P_05 Selezione ed assunzione del personale
- P_08 Procedura affidamento e contratti di appalto

PARTE SPECIALE 8

Reati ambientali (art. 25 – *undecies*)

I principali *Processi Sensibili* individuati sono i seguenti:

- gestione dei rifiuti e abbandono degli stessi da parte di terzi(artt. 256 – 260 *bis* D.Lgs. 152/2006, T.U. Ambiente)
- inquinamento idrico (art. 137 D.Lgs. 152/2006, T.U. Ambiente)
- siti contaminati (art. 257 D.Lgs. 152/2006, T.U. Ambiente)
- gestione aree comuni di pubblico accesso
- smaltimento toner e stampanti

Nell'ambito dei suddetti rischi, la Società, oltre ai principi e alle regole di comportamento previste nel Codice Etico, ha: (i) avviato una specifica mappatura dei rischi ambientali tuttora in corso il cui esito potrebbe rendere opportuno un'eventuale revisione del Modello e (ii) individuato in prima istanza i seguenti principi/regole di comportamento generali al fine di ridurre il rischio di commissione di reati:

- occorre rispettare la disciplina di settore e in particolare la normativa in tema di gestione dei rifiuti, inquinamento idrico e dei siti contaminati;
- occorre rispettare le prescrizioni dettate da eventuali provvedimenti autorizzativi, dalle disposizioni di legge vigenti inerenti la disciplina ambientale, dalle prescrizioni dell'autorità di vigilanza;
- è vietato porre in essere, partecipare o dare causa a comportamenti che, individualmente ovvero collettivamente, siano suscettibili di arrecare un danno all'ambiente;
- è vietata l'omissione di verifica dei requisiti di idoneità e professionalità dei soggetti cui sono affidati incarichi inerenti la materia ambientale;
- occorre identificare le aree ambientali ed i relativi responsabili al fine di individuare potenziali interventi in ottica di prevenzione degli incidenti ambientali;
- occorre coinvolgere i fornitori e gli affittuari in obiettivi ambientali e di sicurezza;
- occorre organizzare un piano di formazione che coinvolga tutto il personale, con particolare attenzione ed approfondimenti sulle procedure verso coloro che svolgono attività che

hanno, o che potrebbero avere, impatti significativi sull'ambiente in relazione alla gestione dei rifiuti;

- i fornitori di servizi di smaltimento e trasporto rifiuti devono essere selezionati in base alla conformità legislativa ed alla qualità del servizio;
- occorre raccogliere i rifiuti e conferirli, per il recupero e lo smaltimento, a trasportatori esterni autorizzati secondo le leggi vigenti in materia;
- occorre definire periodicamente una serie di obiettivi di miglioramento e controllo delle prestazioni ambientali;
- segnalare all'Organismo di Vigilanza eventuali operazioni ritenute sospette;
- nei rinnovi e/o nuovi contratti con i partners commerciali, consulenti e fornitori deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali).

Nell'ambito dei suddetti rischi, la Società in data 21 aprile 2016 ha dato inizio all'attività necessaria per l'ottenimento della certificazione ambientale.

PARTE SPECIALE 9

Piano Triennale di Prevenzione della Corruzione (P.T.P.C.)

REVISIONE	DATA	PREDISPOSTO E PROPOSTO DA:	APPROVATO DA:	NOTE
REV.00	30.1.2014	Responsabile della Prevenzione della Corruzione	Consiglio di Amministrazione	Prima adozione
REV.01	26.6.2015	Responsabile della Prevenzione della Corruzione	Consiglio di Amministrazione	Aggiornamento
REV.02	30.1.2017	Responsabile della Prevenzione della Corruzione	Consiglio di Amministrazione	Aggiornamento

9.1 Quadro normativo

La legge 190/2012 e il d.lgs. 33/2013 disciplinano un complesso sistema di prevenzione e repressione della corruzione e dell'illegalità nella pubblica amministrazione, nell'ambito del quale è previsto che gli enti pubblici provvedano a nominare al loro interno un Responsabile della prevenzione della corruzione e della trasparenza (di seguito anche "**RPCT**") e adottino, su proposta dello stesso responsabile, un apposito Piano triennale per la prevenzione della corruzione.

Il Piano assume sempre di più un valore programmatico incisivo, dovendo necessariamente prevedere obiettivi strategici per il contrasto alla corruzione fissati dall'organo di indirizzo.

In materia di trasparenza, il combinato disposto tra la L. 190/2012 e il d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, richiede l'adempimento di una serie di obblighi di pubblicazione relativi ai dati indicati dalle normative citate.

9.1.1 Ambito soggettivo di applicazione

Il Piano Nazionale Anticorruzione 2016 di seguito anche "**PNA**" (Determina dell'Autorità nazionale anticorruzione del 3.8.2016) e le "Linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici" elaborate dall'Autorità Nazionale Anticorruzione (ANAC) con Determina 8/2015 hanno meglio definito l'ambito di applicazione soggettiva delle misure di prevenzione della corruzione e trasparenza *ex* L. 190/2012 e d.lgs. 33/2013 e s.m.i.

Le diverse tipologie di controllo sono state definite con chiarezza anche dal Testo unico sulle società partecipate (art. 2 del d.lgs. 175/2016).

In particolare il d.lgs. 97/2016, con lo scopo di meglio chiarire l'ambito soggettivo di applicazione, inserisce all'interno del d.lgs. 33/2013, un nuovo articolo, l'art. 2-*bis,* che sostituisce l'art. 11 del d.lgs. 33/2013, contestualmente abrogato.

Il suddetto articolo 2-*bis* individua tre macro categorie di soggetti: le pubbliche amministrazioni (art. 2-*bis*, co. 1); altri soggetti tra cui enti pubblici economici, ordini professionali, società in controllo ed enti di diritto privato (art. 2-*bis*, co. 2); altre società a partecipazione pubblica ed enti di diritto privato (art. 2-*bis*, co. 3).

Si possono dunque distinguere:

• le società c.d. "controllate", in cui la P.A. in qualunque sua forma, direttamente o indirettamente, esercita un effettivo controllo individuato con i criteri dell'art. 2359 co. 1 nn. 1 e 2 c.c. (si tratta dei casi in cui la pubblica amministrazione dispone della maggioranza dei voti esercitabili nell'assemblea ordinaria, ovvero di voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria);

• le società "meramente partecipate" o "partecipate non in controllo", in cui la presenza pubblica non è atta ad esercitare il predetto controllo, trattandosi di una partecipazione talvolta anche minimale.

La linea di confine tra società ed enti "in controllo pubblico" e società ed enti "a partecipazione pubblica non di controllo" non ha carattere meramente formale bensì conforma, in modo differenziato, l'applicazione della normativa anticorruzione, in ragione del diverso grado di coinvolgimento delle Pubbliche Amministrazioni all'interno delle due diverse tipologie di soggetti.

Le prime sono a tutti gli effetti assimilate alle amministrazioni per quanto riguarda la prevenzione della corruzione e la trasparenza; le seconde, invece, hanno delle attenuazioni rispetto all'applicazione integrale della disciplina di cui alla L. 190/2012 e del d.lgs. 33/2013.

In particolare, le società "controllate" saranno tenute alla nomina di un Responsabile per la prevenzione della corruzione e trasparenza e all'adozione di uno specifico Piano, oltre che all'adempimento integrale degli obblighi di pubblicazione nell'ambito della disciplina della trasparenza.

9.1.2 Sanzioni

Nel caso in cui venga omessa l'adozione del Piano triennale di prevenzione della corruzione o dei Codici di comportamento (Codice etico), è prevista l'applicabilità di una sanzione amministrativa non inferiore nel minimo a euro 1000 e non superiore nel massimo a euro 10.000

In materia di trasparenza, la mancata o incompleta comunicazione delle informazioni e dei dati relativi alla compagine societaria (artt. 14 e 22 del D.lgs. 33/2013) può dar luogo a una sanzione amministrativa pecuniaria da 500 a 10.000 euro a carico del responsabile della mancata comunicazione e il relativo provvedimento è pubblicato sul sito internet dell'amministrazione o organismo interessato.

Inoltre, con l'orientamento n. 24 del 23 settembre 2015, l'ANAC ha formulato indicazioni in merito all'applicazione della sanzione consistente nel divieto per le pubbliche amministrazioni di erogare somme a qualsiasi titolo in favore di enti pubblici vigilati, enti di diritto privato in controllo pubblico e società partecipate, nei casi di omessa o incompleta pubblicazione dei dati.

Il procedimento sanzionatorio per l'irrogazione delle sanzioni per il mancato adempimento della disciplina anticorruzione e trasparenza è disciplinato da apposito "Regolamento in materia di esercizio del potere sanzionatorio" emanato dall'ANAC in data 16 novembre 2016.

9.2 Il Piano triennale per la prevenzione della corruzione di Sito S.p.A

S.I.TO S.p.A., il cui capitale sociale è detenuto a maggioranza da Finpiemonte Partecipazioni S.p.A a sua volta controllata dalla Regione Piemonte, rientra nella definizione di "società in controllo pubblico" e pertanto è tenuta ad adempiere agli obblighi previsti dalla L. 190/2012 e dal d.lgs. 33/2013 e s.m.i.

Il presente Piano è stato approvato dal Consiglio di Amministrazione su proposta del Responsabile della prevenzione della corruzione.

Il Piano di S.I.TO S.p.A nasce da un'attività di *self risk assessment* che è consistita nella mappatura del rischio attraverso l'analisi della documentazione societaria e l'effettuazione di interviste ai soggetti responsabili delle aree maggiormente a rischio, da parte del Responsabile della prevenzione della corruzione e trasparenza.

Il Piano di Prevenzione, a seguito della sua approvazione e delle successive modificazioni, deve essere portato alla conoscenza delle pubbliche amministrazioni vigilanti e pubblicato sul sito istituzionale.

9.2.1 Rapporti con il Modello organizzativo ex d.lgs. 231/2001

L' ANAC suggerisce che "*per evitare inutili ridondanze*" il Piano può essere integrato nel Modello di Organizzazione e Gestione, ove esistente, e "*fare perno*" su di esso estendendone l'ambito di applicazione non solo ai reati contro la pubblica amministrazione previsti dal D.Lgs. n. 231/2001 ma anche a tutti quelli considerati nella Legge n. 190/2012, dal lato attivo e passivo, anche in relazione al tipo di attività svolta dall'ente.

L'ANAC ha inoltre precisato l'esigenza di tenere conto della necessità di coordinamento tra quanto previsto nella legge 190 del 2012 per i piani di prevenzione della corruzione con le disposizioni del d.lgs. 231/2001, sia in termini di modello di organizzazione e gestione che di controlli e di responsabilità.

Pertanto il presente Piano, pur conservando una sua autonomia dal punto di vista dell'ambito di applicazione e dell'aggiornamento, viene inserito quale Parte Speciale 9 del Modello organizzativo adottato da Sito S.p.A, coordinandosi con esso per quanto compatibile.

9.2.2 Procedura per l'aggiornamento del Piano di Sito S.p.A

Il Piano viene modificato dal Consiglio di Amministrazione su proposta del Responsabile della Prevenzione della Corruzione sentito anche l'Organismo di Vigilanza.

La L. 190/2012 prevede un aggiornamento annuale entro il 31 gennaio.

Inoltre il PTPC, così come il Modello di Organizzazione e Gestione nel quale è incastonato organicamente, può essere aggiornato in qualsiasi momento e ogniqualvolta si verifichi un evento che palesi la esigenza di integrazione con nuove e migliori procedure, un mutamento strutturale della Società che comporti un aggiornamento ovvero una modifica normativa rilevante.

9.3 Responsabile per la prevenzione della corruzione e trasparenza

La figura del RPC è stata interessata in modo significativo dalle modifiche introdotte dal d.lgs. 97/2016. La nuova disciplina è volta a unificare in capo ad un solo soggetto l'incarico di Responsabile della prevenzione della corruzione e della trasparenza e a rafforzarne il ruolo, prevedendo che ad esso siano riconosciuti poteri e funzioni idonei a garantire lo svolgimento dell'incarico con autonomia ed effettività, eventualmente anche con modifiche organizzative.

D'ora in avanti, pertanto, il Responsabile viene identificato con riferimento ad entrambi i ruoli come Responsabile della prevenzione della corruzione e della trasparenza (RPCT). Si precisa sin da ora che in attuazione delle nuove disposizioni normative, gli organi di indirizzo formalizzano con apposito atto l'integrazione dei compiti in materia di trasparenza agli attuali RPC, avendo cura di indicare la relativa decorrenza.

La nuova disciplina tende a rafforzare il ruolo dei Responsabili della prevenzione della corruzione (RPC) quali soggetti titolari del potere di predisposizione e di proposta del PTPC all'organo di indirizzo.

Il responsabile per la prevenzione della corruzione e della trasparenza per S.I.TO SPA è la **dott.ssa Laura Molinario nominata in data 23 dicembre 2013 con delibera del Consiglio di Amministrazione**.

Indipendenza e di autonomia

In considerazione dei numerosi compiti direttamente attribuiti al RPCT nei confronti del personale dell'ente, ed eventualmente per quel che concerne le disfunzioni anche nei confronti degli organi di indirizzo, è indispensabile che tra le misure organizzative da adottarsi da parte degli organi di indirizzo vi siano anche quelle dirette ad assicurare che il RPCT svolga il suo delicato compito in modo imparziale, al riparo da possibili ritorsioni.

A garanzia dello svolgimento delle funzioni del RPCT in condizioni di autonomia e indipendenza, occorre considerare anche la durata dell'incarico di RPCT che deve essere fissata tenendo conto della non esclusività della funzione.

Supporto conoscitivo e operativo

Al fine di garantire che il RPCT possa svolgere il proprio ruolo con autonomia ed effettività, come previsto dall'art. 41 del d.lgs. 97/2016, l'organo di indirizzo dispone «*le eventuali modifiche organizzative necessarie per assicurare funzioni e poteri idonei*» al RPCT.

È, dunque, altamente auspicabile, da una parte, che il RPCT sia dotato di una struttura organizzativa di supporto adeguata, per qualità del personale e per mezzi tecnici, al compito da svolgere. Dall'altra, che vengano assicurati al RPCT poteri effettivi, preferibilmente con una specifica formalizzazione nell'atto di nomina, di interlocuzione nei confronti di tutta la struttura, sia nella fase della predisposizione del Piano e delle misure sia in quella del controllo sulle stesse.

Interlocuzione e controllo

Nelle modifiche apportate dal d.lgs. 97/2016 risulta evidente l'intento di rafforzare i poteri di interlocuzione e di controllo del RPCT nei confronti di tutta la struttura. Emerge più chiaramente che il RPCT deve avere la possibilità di incidere effettivamente all'interno dell'ente e che alla responsabilità del RPCT si affiancano con maggiore decisione quelle dei soggetti coinvolti nell'attuazione delle misure di prevenzione.

Compiti

Al Responsabile della prevenzione della corruzione spetta:

- Proporre l'adozione del PTPC e il suo annuale aggiornamento;
- Verificare l'efficace attuazione del Piano e la sua idoneità, proponendo eventualmente le modifiche necessarie;
- Redigere annualmente (entro il 15 dicembre o nel diverso termine indicato dall'ANAC) una relazione sull'attività svolta che offra il rendiconto sull'efficacia delle misure di prevenzione (i.e. gestione dei rischi, formazione in tema di anticorruzione, codice di comportamento, sanzioni ed altre iniziative quali forme di tutela offerte ai *whistleblowers* e rispetto dei termini dei procedimenti) definite dal Piano di Prevenzione della Corruzione da presentare al Consiglio di Amministrazione e da pubblicare sul sito web;
- Definire procedure appropriate per selezionare e formare i dipendenti che operano in settori esposti al rischio di corruzione;
- Garantire la pubblicazione sul sito web di SITO S.p.A dei dati della Società richiesti dalla normativa vigente in materia di trasparenza;
- Formalizzare i flussi informativi relativi alla prevenzione della corruzione e una linea di *report* nei confronti dell'organo di indirizzo politico.

Stante la comunanza di competenze e mansioni attribuite, gli strumenti di operatività dell'Organismo di Vigilanza – di cui al Modello di Organizzazione, Gestione e Controllo – potrebbero essere mutuati dal responsabile della prevenzione della corruzione nello svolgimento della propria attività, e in particolare:

(i) la casella di posta elettronica dedicata (**rpc@sitospa.it**), esclusivamente consultabile dal responsabile e dai soggetti da questo espressamente delegati (i.e. informazioni periodiche o di carattere eccezionale, segnalazioni di deroghe, violazioni o meri sospetti di violazione del Piano e/o del Codice etico). Tale mezzo consentirà anche di dare attuazione a quanto previsto dall'art. 54 bis, d.lgs. 165/2001 (*whistleblowing* del dipendente);

(ii) le modalità di verbalizzazione dell'attività e la conseguente archiviazione (la tracciabilità dei controlli rappresenta un punto cruciale ai fini della dimostrazione da parte del RPCT di aver efficacemente attuato, il Piano e di aver vigilato sul funzionamento e sull'osservanza dello stesso).

Responsabilità

Le modifiche apportate dal d.lgs. 97/2016 precisano che in caso di ripetute violazioni del PTPC sussiste la responsabilità dirigenziale e per omesso controllo, sul piano disciplinare, se il RPCT non prova di aver comunicato agli uffici le misure da adottare e le relative modalità e di aver vigilato sull'osservanza del Piano. I dirigenti, pertanto, rispondono della mancata attuazione delle misure di prevenzione della corruzione, ove il RPCT dimostri di avere effettuato le dovute comunicazioni agli uffici e di avere vigilato sull'osservanza del Piano.

Resta immutata, in capo al RPCT, la responsabilità di tipo dirigenziale, disciplinare, per danno erariale e all'immagine della pubblica amministrazione, prevista all'art. 1, co. 12, della l. 190/2012, in caso di commissione di un reato di corruzione, accertato con sentenza passata in giudicato, all'interno dell'amministrazione. Il RPCT può andare esente dalla responsabilità ove dimostri di avere proposto un PTPC con misure adeguate e di aver vigilato sul funzionamento e sull'osservanza dello stesso.

Referenti

Come già chiarito nell'Aggiornamento 2015 al PNA, eventuali "referenti" del RPCT possono rivelarsi utili nelle organizzazioni particolarmente complesse. Fermo restando il regime delle responsabilità in capo al RPCT, i referenti possono svolgere attività informativa nei confronti del responsabile, affinché questi abbia elementi e riscontri per la formazione e il monitoraggio del PTPC e sull'attuazione delle misure.

Gli eventuali Referenti per la prevenzione sono designati dal Responsabile per l'attuazione del piano anticorruzione e ad essi sono affidati i seguenti compiti:

- concorrere alla definizione di misure idonee a prevenire e contrastare i fenomeni di corruzione e a controllarne il rispetto da parte dei dipendenti dell'ufficio cui sono preposti;
- fornire le informazioni richieste dal soggetto competente per l'individuazione delle attività nell'ambito delle quali è più elevato il rischio corruzione e formulare specifiche proposte volte alla prevenzione del rischio medesimo;
- provvedere al monitoraggio delle attività svolte nell'ufficio a cui sono preposti nell'ambito delle quali è più elevato il rischio corruzione;
- definire specifiche misure di monitoraggio e di vigilanza sull'attuazione degli obblighi di trasparenza.

9.4 Individuazione dei rischi

9.4.1 Fattispecie di reato rilevanti in Sito S.p.A

La prevenzione della corruzione non riguarda i reati di corruzione *stricto sensu* ma l'intera gamma dei reati contro la pubblica amministrazione disciplinati nel Titolo II del Capo I della Parte Speciale del Codice Penale, e altresì tutte quelle situazioni in cui – a prescindere dalla concreta rilevanza penale – venga in evidenza un malfunzionamento dell'ente o un danno alla sua immagine o all'immagine della pubblica amministrazione a causa dell'uso improprio delle funzioni attribuite (cfr. Determina Anac n.8/2015).

Sotto il profilo della qualificazione soggettiva degli amministratori e dei dipendenti della Società si può affermare la loro possibile sussunzione nella categoria degli incaricati di pubblico servizio. Tali soggetti svolgono, infatti, una pubblica funzione caratterizzata però dalla mancanza dei poteri tipici del pubblico ufficiale che, invece, svolge una funzione amministrativa caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi (artt. 357 e 359 codice penale).

Inoltre, nella prospettiva della Legge 190/2012 le fattispecie da selezionare per la mappatura dei rischi devono essere analizzate sotto il profilo del possibile uso a fini privati delle funzioni attribuite e non nell'ottica dell'interesse o del vantaggio dell'ente che è tipica della responsabilità ai sensi del d.lgs. 231/2001.

Ciò comporta che il reato presupposto deve essere commesso nell'esercizio delle funzioni e nel rapporto organico con la Società.

Si ritiene pertanto che i reati presupposto di cui al codice penale da prendere in considerazione per la mappatura dei rischi sono i seguenti:

- art. 314 (peculato);
- art. 316 (peculato mediante profitto dell'errore altrui);
- art. 316 bis (Malversazione a danno dello Stato);
- art. 316 ter (Indebita percezione di erogazione a danno dello Stato);
- art. 317 c.p. (Concussione);
- art. 318-320 (Corruzione per l'esercizio della funzione);
- art. 319-320 (Corruzione per un atto contrario ai doveri d'ufficio);
- art. 319 quater (Induzione indebita a dare o promettere utilità);
- art. 322 (Istigazione alla corruzione);
- art. 323 (abuso d'ufficio);

- art. 325 (Utilizzazione d'invenzioni o scoperte conosciute per ragioni d'ufficio);
- art. 326 (Rivelazione ed utilizzazione di segreti di ufficio);
- art. 328 (Rifiuto di atti d'ufficio. Omissione);
- art. 331 (Interruzione di un servizio pubblico o di pubblica necessità).

Oltre alle condotte tipiche sopra elencate, devono essere presi in considerazione – ai fini del presente documento – anche tutti i comportamenti prodromici a tali reati che, sebbene ancora privi di un disvalore penalmente rilevante, possano tuttavia essere la premessa di condotte autenticamente corruttive (c.d. *maladmnistration*).

Si ritiene, viceversa, di dover escludere i seguenti reati tra quelli potenzialmente configurabili nell'esercizio delle funzioni di amministratori e dipendenti della Società:

- Corruzione in atti giudiziari (**art. 319 ter**), peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (**art. 322 bis**), rifiuto o ritardo di obbedienza commesso da un militare o da un agente della forza pubblica (**art. 329**), per evidenti ragioni di qualifica soggettiva dell'autore del reato che li rende ontologicamente incompatibili con l'ambito di attività della Società.
- Sottrazione o danneggiamento di cose sottoposte a sequestro disposto nel corso di un procedimento penale o dall'autorità amministrativa (**art. 334**), violazione colposa di doveri inerenti alla custodia di cose sottoposte a sequestro disposto nel corso di un procedimento penale o dall'autorità amministrativa (**art. 335**) perché, pur essendo in astratto possibile la commissione di tali reati, non si ravvisano in concreto segnali significativi di un reale rischio di verificazione, alla luce della mappatura dei rischi svolta per predisporre il Modello di Organizzazione e Gestione.

La mappatura dei rischi svolta per l'adozione del Modello di Organizzazione e Gestione ex d.lgs. 231/2001 rappresenta il punto di riferimento imprescindibile. Peraltro, in quella sede, così come emerge da quanto previsto nella parte dedicata alla prevenzione dei reati contro la pubblica amministrazione, si è già tenuto conto di processi sensibili che effettivamente rilevano anche nella prospettiva del reato commesso dall'incaricato di pubblico servizio che opera all'interno dell'organico della Società o comunque da un soggetto interno (apicale o subordinato) che agisce per un interesse privato in conflitto con l'interesse pubblico perseguito dalla Società.

In particolare, rilevano i processi attinenti alla scelta del contraente per l'affidamento di lavori, forniture e servizi di cui all'art. 1, comma sedici, L. 190/2012. In quest'ambito diventa centrale la corretta applicazione del d.lgs. 50/2016 (c.d. Codice dei contratti pubblici).

Le aree di rischio identificate nel Modello di Organizzazione e Gestione possono rilevare anche in relazione ai reati previsti dalla L. 190/2012 sopra richiamati perché attengono alla gestione di denaro, agli acquisti, alle vendite, alla tracciabilità dei flussi finanziari, alla conclusione di contratti, ai bandi di gara, tutte attività nelle quali si potrebbero commettere i reati sopra selezionati.

Le **aree a rischio** che in prima istanza si ritengono di rilevanza tenuto conto dell'attività svolta dalla Società sono dunque le seguenti:

affidamento lavori mediante gare d'appalto in cui la Società ricopre la figura di stazione appaltante
acquisto di beni e servizi in applicazione del d.lgs. 50/2016
rapporti con la Pubblica Amministrazione, con particolare riferimento alla: ✓ gestione dei rapporti con gli Enti Pubblici in via esemplificativa e non esaustiva per l'ottenimento di autorizzazioni, licenze, ecc…; ✓ gestione delle ispezioni (amministrative, fiscali, previdenziali, ecc.); ✓ gestione di procedimenti giudiziali, stragiudiziali e arbitrali.
gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse dai soggetti pubblici
gestione del processo di sponsorizzazione, concessione di erogazioni liberali e donazioni, spese di rappresentanza (inclusa la politica di omaggi o regalie)
assunzione e gestione del personale (compresi i soggetti appartenenti a categorie protette) e politica degli incentivi/premi
gestione di trattamenti previdenziali del personale
gestione degli accertamenti e delle ispezioni
conferimento e gestione delle consulenze (amministrative, fiscali, legali, professionali etc)
gestione dei beni strumentali e delle utilità aziendali (es. autovetture, cellulari, personal computer, carte di credito aziendali etc.)
gestione e controllo delle note spese
gestione dei flussi finanziari
gestione del sistema informativo e di reporting verso i responsabili di funzione di volta in volta coinvolti
gestione del sistema di tracciabilità delle singole operazioni svolte
utilizzo poteri di firma e legale rappresentanza del Legale Rappresentate (o chi ne fa le veci) e del Datore di Lavoro

gestione dei rapporti commerciali con particolare riferimento alle transazioni finanziarie
negoziazione, stipula e/o esecuzione di contratti, convenzioni, concessioni con soggetti pubblici ai quali si perviene mediante procedure negoziate (affidamento diretto o trattative private) ovvero mediante procedure ad evidenza pubblica (aperte o ristrette); Per tali processi diventa centrale la corretta applicazione del d.lgs. 50/2016 (c.d. Codice dei contratti pubblici)

Sarà compito del Responsabile della Prevenzione della Corruzione approfondire la mappatura dei rischi ed eventualmente proporre implementazioni nel corso della sua attività di verifica e di controllo.

9.5 Misure per la gestione del rischio

9.5.1 Regolamenti e direttive

Le misure primarie per la prevenzione del rischio di corruzione sono contenute nella normativa interna alla Società, e in particolare nei seguenti atti che ciascun dipendente è tenuto a conoscere e a rispettare:

- Statuto
- Codice etico
- Modello Organizzativo
- Regolamento interno

9.5.2 Procedure

In Sito S.p.A sono già operative una serie di procedure idonee a contrastare o a prevenire eventuali fenomeni corruttivi:

- organigramma
- mansionario
- P_01 Contabilità e bilancio
- P_02 Operazioni monetarie e finanziarie
- P_03 Finanziamenti pubblici
- P_04 Omaggi e liberalità
- P_05 Selezione ed assunzione del personale
- P_06 Operazioni societarie straordinarie
- P_07 Trattamento delle informazioni riservate
- P_08 Affidamento e contratti di appalto
- P_09 Procedura di esecuzione dei pagamenti
- P_10 Gestione amministrativa dei rapporti commerciali
- P_11 Benefits

Saranno, inoltre, formalizzate e/o incrementate tutte quelle prassi aziendali che consentono – nelle singole aree di rischio individuate nel presente PTPC – una specifica forma di prevenzione di qualsivoglia fenomeno corruttivo.

Particolare attenzione merita l'emanazione del nuovo codice appalti anch'esso improntato al contrasto della corruzione nelle procedure di affidamento degli appalti.

9.5.3 Sistemi di controllo

Riguardo ai c.d. **sistemi di controllo,** il Responsabile della prevenzione della corruzione provvederà a monitorare e a prevedere le seguenti attività:

- Definire delle tipologie di controllo e delle tempistiche di effettuazione delle stesse (anche attraverso incontri con le altre funzioni aziendali);
- Prevedere un sistema di raccolta/archiviazione delle segnalazioni o delle criticità riscontrate e un'attività dii *feed-back* all'organo di indirizzo politico;
- Verificare l'evoluzione normativa in materia di anticorruzione e trasparenza.

9.5.4 Incompatibilità e inconferibilità per gli incarichi di amministratore e di dirigente

Particolari adempimenti sono richiesti in riferimento al **conferimento degli incarichi ad amministratori e dirigenti**:

- Verifica della sussistenza di eventuali condizione ostative (inconferibilità o incompatibilità di cui al d.lgs. 39/2013), di situazioni di conflitto di interesse, o di altre cause impeditive;
- Verifica di eventuali precedenti penali.

L'accertamento avviene mediante dichiarazione sostitutiva di certificazione resa dall'interessato nei termini e alle condizioni di cui al D.P.R. 445/2000.

9.5.5 Misure di rotazione

La rotazione del personale prevista dalla normativa anticorruzione e evidenziata anche dal PNA 2016 è considerata quale misura organizzativa preventiva finalizzata a limitare il consolidarsi di relazioni che possano alimentare dinamiche improprie nella gestione amministrativa, conseguenti alla permanenza nel tempo di determinati dipendenti nel medesimo ruolo o funzione. L'alternanza riduce il rischio che un dipendente, occupandosi per lungo tempo dello stesso tipo di attività, servizi, procedimenti e instaurando relazioni sempre con gli stessi utenti, possa essere sottoposto a pressioni esterne o possa instaurare rapporti potenzialmente in grado di attivare dinamiche inadeguate.

In generale la rotazione rappresenta anche un criterio organizzativo che può contribuire alla formazione del personale, accrescendo le conoscenze e la preparazione professionale del lavoratore.

Tuttavia, il PNA 2016 precisa che la rotazione è misura che non sempre si può realizzare, specie nelle realtà come Sito S.p.A.

La Società si impegna comunque ad adottare misure per evitare che il soggetto non sottoposto a rotazione abbia il controllo esclusivo dei processi, specie di quelli più esposti al rischio di corruzione e a sviluppare altre misure

organizzative di prevenzione che sortiscano un effetto analogo a quello della rotazione, a cominciare, ad esempio, da quelle di trasparenza.

In particolare si farà in modo che:

- vi sia sempre un'interlocuzione tra più soggetti nei singoli processi e nelle decisioni conseguenti;
- le attività si sviluppino attraverso una corretta articolazione dei compiti e delle competenze.

9.5.6 Selezione del personale

Per quanto compatibili, Sito S.p.A adotta le misure necessarie ad adeguare la selezione del personale alla norme di legge.

9.6 Gli adempimenti in materia di trasparenza in S.I.T.O S.p.A.

La disciplina della trasparenza – di cui alla L. 190/2012 e al d.lgs. 33/2013 – rappresenta parte essenziale dell'attività di prevenzione della corruzione.

La trasparenza deve essere assicurata sia sull'attività sia sull'organizzazione.

Nel Piano vanno specificate le modalità, i tempi di attuazione, le risorse e gli strumenti di verifica dell'efficacia delle iniziative e degli obblighi in materia di trasparenza.

9.6.1 Principi generali della trasparenza in S.I.TO S.p.A.

In quanto ente di diritto privato in controllo pubblico, S.I.TO SPA è sottoposta alle regole sulla trasparenza di cui alla L. 190/2012 e al d.lgs. 33/2013.

In particolare la Società è tenuta:

- Alla **pubblicazione** dei dati richiesti dal d.lgs. 33/2013 e s.m.i;
- Alla realizzazione e all'aggiornamento della **sezione "Amministrazione/Società trasparente**" nel proprio sito internet;
- Alla previsione di una **funzione di controllo e monitoraggio** dell'assolvimento degli obblighi di pubblicazione (il c.d. Responsabile per la trasparenza);
- All'organizzazione di un sistema che fornisca **risposte tempestive** ai cittadini (c.d. **accesso civico**), anche alla luce delle modifiche apportate dal d.lgs. 97/2016 (c.d. **accesso civico generalizzato**).

Il presente Piano sistematizza le seguenti attività, alla cui realizzazione concorrono, oltre al Responsabile per la trasparenza, tutti gli uffici dell'ente e i relativi responsabili:

- Iniziative previste per garantire un adeguato livello di trasparenza, nonché la legalità e lo sviluppo della cultura dell'integrità;
- Definizione di misure, modi e iniziative volti all'attuazione degli obblighi di pubblicazione;
- Definizione di misure organizzative volte ad assicurare la regolarità e la tempestività dei flussi informativi di cui all'art. 43, comma 3, d.lgs. 33/2013;
- Definizione di specifiche misure di monitoraggio e di vigilanza sull'attuazione degli obblighi di trasparenza.

S.I.T.O. S.p.A. è consapevole che la trasparenza rappresenta un fine, i cui contenuti sono indicati dalla normativa applicabile, ma le cui forme dovranno svolgersi ed evolversi in funzione della concreta attività della Società, delle valutazioni e del monitoraggio sulla effettiva realizzazione degli scopi prefissati.

9.6.2 Ruoli e responsabilità

Il **Responsabile per la trasparenza**, che si identifica nel soggetto che svolge anche il ruolo di Responsabile per la prevenzione della corruzione, viene nominato dall'organo amministrativo.

Il Responsabile della trasparenza:

- controlla che le misure per l'attuazione di un'efficacia trasparenza siano collegate con le misure e gli interventi per la prevenzione della corruzione;
- controlla ed assicura la regolare attuazione dell'accesso civico;
- svolge attività di controllo sull'adempimento degli obblighi di pubblicazione previsti dalla normativa vigente con cadenza semestrale oltreché ad evento attraverso dei controlli interni e dei test a campione;
- assicura la chiarezza e la completezza delle informazioni pubblicate.

Il responsabile della Trasparenza per S.I.TO SPA è la **dott.ssa Laura Molinario nominata in data 23 dicembre 2013 con delibera del Consiglio di Amministrazione**.

L'art. 10 del d.lgs. 33/2013 come riformato dal d.lgs. 97/2016, prevede inoltre l'indicazione, in un'apposita sezione del Piano triennale per la prevenzione della corruzione, dei responsabili della trasmissione e della pubblicazione dei documenti, delle informazioni e dei dati ai sensi del suddetto d.lgs. 33/2013.

Tale funzione in S.I.TO SPA viene svolta dal sig. **Mirabelli Massimiliano.**

9.6.3 Società Trasparente

Per la predisposizione delle misure volte ad una corretta attuazione della trasparenza all'interno della Società, il Responsabile della Trasparenza ha coinvolto i seguenti uffici:

- Ufficio tecnico
- Ufficio Amministrazione

L'obiettivo è quello di adempiere agli obblighi di pubblicazione e aggiornamento dei dati nella sezione "Società trasparente".

In particolare, come anticipato, si individua nella persona del **Sig. Mirabelli Massimiliano**, responsabile informatico, il soggetto che si occupa della pubblicazione e dell'aggiornamento dei dati.

La Società per il tramite del Responsabile della Trasparenza e dei referenti eventualmente individuati pubblica i dati secondo le scadenze previste dalle legge e, laddove non sia presente una scadenza, si attiene al principio di *tempestività* ossia in tempo utile a consentire ai portatori di interesse di esperire tutti i mezzi di tutela riconosciuti dalla legge.

Rimangono ferme le competenze dei singoli responsabili di Area relativamente all'adempimento di pubblicazione previsti dalle normative vigenti. Tuttavia, il Responsabile dell'Area non risponde dell'inadempienza se dimostra al Responsabile della trasparenza che tale inadempimento è dipeso da cause a Lui non imputabili.

a) Dati e informazioni oggetto di pubblicazione

La Società, come anticipato, è tenuta a costituire sul proprio sito web una apposita Sezione, denominata "Società trasparente", in cui pubblicare i dati e le informazioni ai sensi del d.lgs. 33/2013.

Per l'organizzazione dei diversi "link" si fa riferimento alla tabella allegata alla delibera ANAC n. 1310 del 28 dicembre 2016, seppur compatibilmente alla struttura organizzativa e alle attività svolte da S.I.T.O S.p.A.

L'ANAC precisa che il criterio della "compatibilità" va inteso come necessità di trovare adattamenti agli obblighi di pubblicazione in ragione delle peculiarità organizzative e funzionali delle diverse tipologie di enti, e non in relazione alle peculiarità di ogni singolo ente. Diversamente si avrebbe un'applicazione estremamente diversificata e disomogenea della trasparenza, anche all'interno della stessa tipologia di enti, conseguenza non rispondente allo scopo della norma e all'obiettivo di poter effettuare, tra le altre cose, comparazioni e confronti.

Si attendono inoltre Linee guida specifiche in merito ad un corretto adempimento degli obblighi in materia di trasparenza negli enti diversi dalla P.A.

b) Trasparenza e privacy

La trasparenza necessita di un coordinamento e di un bilanciamento con il principio di riservatezza e di protezione dei dati sensibili visto anche ad esempio l'ampliamento, ai sensi dell'art. 5 del d.lgs. 33/2013, come riformato dal d.lgs. 97/2016, della possibilità di consultazione dei dati relativi alle "pubbliche amministrazioni" da parte di cittadini.

Il legislatore ha previsto precisi limiti a tale "accesso civico" (di cui si tratterà più approfonditamente nel prossimo paragrafo) per evitare che i diritti fondamentali alla riservatezza e alla protezione dei dati possano essere gravemente pregiudicati da una diffusione, non adeguatamente regolamentata, di documenti che riportino delicate informazioni personali. Infatti occorre considerare i rischi per la vita privata e per la dignità delle persone interessate che possono derivare da obblighi di pubblicazione sul web di dati personali non sempre indispensabili a fini di trasparenza.

La Società, in conformità ai principi di protezione dei dati, è tenuta a ridurre al minimo l'utilizzazione di dati personali e di dati identificativi ed evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità (cd. "principio di necessità" di cui all'art. 3 co. 1 del Codice Privacy). Pertanto, anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d.lgs. 33/2013, i soggetti chiamati a darvi attuazione non possono comunque rendere intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

Deve, pertanto, ritenersi consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza" di cui all'art. 11 co. 1 lett. d) del Codice Privacy). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di

pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.

9.6.4 Accesso civico

La disciplina relativa all'accesso civico prevede tale istituto allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche nonché di promuovere la partecipazione al dibattito pubblico; per questi motivi prevede che chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del d.lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-*bis* del d.lgs. 33/2013 stesso.

Per tale ragione, la Società mette a disposizione il seguente indirizzo mail pubblicato sull'apposita sezione del proprio sito internet: **sitospa@pec.it**

L'art. 5 come riformato dal d.lgs. 97/2016 prevede che chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del d.lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-*bis*.

Per quanto riguarda i limiti all'accesso civico, il legislatore al sopracitato art. 5-*bis* d.lgs. 33/2013 prevede che, fatti salvi i casi di pubblicazione obbligatoria, l'amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati (ai sensi dell'articolo 5-*bis*, comma 2) è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso.

Inoltre l'accesso civico di cui all'articolo 5, comma 2, è rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici inerenti a:

a) la sicurezza pubblica e l'ordine pubblico;

b) la sicurezza nazionale;

c) la difesa e le questioni militari;

d) le relazioni internazionali;

e) la politica e la stabilità finanziaria ed economica dello Stato;

f) la conduzione di indagini sui reati e il loro perseguimento;

g) il regolare svolgimento di attività ispettive.

L'accesso è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia;

b) la libertà e la segretezza della corrispondenza;

c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

È escluso altresì nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge.

La normativa prevede comunque che se i suddetti limiti riguardano soltanto alcuni dati o alcune parti del documento richiesto, deve essere consentito l'accesso agli altri dati o alle altre parti.

L'esercizio del diritto non è sottoposto invece ad alcuna limitazione dal punto di vista soggettivo del richiedente. L'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti e non richiede motivazione.

Il procedimento di accesso civico deve concludersi con una motivazione espressa da comunicarsi al richiedente e agli eventuali controinteressati nel termine di trenta giorni dalla presentazione dell'istanza.

9.7 Codice di comportamento

In relazione al Codice di comportamento previsto dalla normativa, è possibile fare riferimento al Codice Etico adottato dalla Società. Questo sarà monitorato ed eventualmente integrato alla luce della disciplina in materia di prevenzione della corruzione.

9.8 Formazione

Al fine di garantire una generale diffusione della cultura della legalità, S.I.TO S.p.A. assicura specifiche attività formative rivolte al personale dipendente, anche a tempo determinato o avente incarichi di natura occasionale, in materia di trasparenza, pubblicità, integrità e legalità.

Sotto questo profilo, l'attività formativa verrà svolta di intesa con il Responsabile della Prevenzione della Corruzione e con l'Organismo di Vigilanza. I relatori potranno essere gli stessi componenti dell'Organismo di Vigilanza, il Responsabile della Prevenzione della Corruzione e professionisti o docenti esterni. La formazione, adeguatamente documentata con firme di presenza, avverrà con incontri collettivi e per singole aree di attività. Oggetto della formazione saranno le seguenti materie:

- i reati contro la pubblica amministrazione (elemento oggettivo, dolo e colpa, cause di giustificazione, sanzioni);
- le disposizioni per la prevenzione della corruzione e dell'illegalità nella pubblica amministrazione;
- le interazioni tra la disciplina della prevenzione della corruzione (L. 190/12) e la disciplina in materia di responsabilità amministrativa degli enti (d.lgs. 231/2001);
- il Modello di Organizzazione e di Gestione ex d.lgs. 231/2001, le procedure ed il Piano di Prevenzione della Corruzione;
- il Codice Etico;
- il Codice dei contratti Pubblici (d.lgs. 50/2016), in particolare per l'Ufficio Tecnico;
- norme sulla trasparenza;
- il processo di accertamento dei reati e la disciplina di tutela del dipendente che segnala illeciti di cui è a conoscenza.

Sarà compito del RPCT pianificare tale attività formativa: contenuti, tempistica, destinatari, verifiche ed eventuale programmazione di percorsi formativi aggiuntivi obbligatori per il personale allocato in aree/servizi esposti a maggiore rischio di corruzione.

In particolare, in sede di prima attuazione e ogniqualvolta si rendesse necessario, detti interventi formativi saranno finalizzati a far conseguire ai destinatari una piena conoscenza di quanto previsto dal PTPC.

Un'attenzione primaria deve, inoltre, essere dedicata alla formazione del RPCT stesso, nonché di quei soggetti competenti per le attività maggiormente esposte al rischio di corruzione.

Nei contratti con i fornitori, consulenti e collaboratori sarà prevista apposita clausola di presa visione e condivisione dei principi contenuti nel Piano stesso.

9.9 Flussi informativi e tutela dei "whistleblowers"

Al Responsabile della Prevenzione della Corruzione, per quanto di sua competenza, si estendono gli stessi ed autonomi poteri di iniziativa e controllo previsti nel Modello di Organizzazione e Gestione per l'Organismo di Vigilanza.

Il Responsabile della Prevenzione della Corruzione può partecipare alle sedute dell'Organismo di Vigilanza e svolgere i controlli e le attività di sua competenza di concerto con l'Organismo di Vigilanza, ferme restando le sue esclusive responsabilità discendenti dalla Legge 190/2012.

Pertanto gli obblighi di informazione verso l'Organismo di Vigilanza si estendono a favore del Responsabile della Prevenzione della Corruzione.

L'Organismo di Vigilanza e il Responsabile della Prevenzione della Corruzione e il Collegio Sindacale devono tra loro coordinarsi, trasmettendosi reciprocamente verbali, documenti e informazioni acquisite, nonché svolgere verifiche congiuntamente.

Il Responsabile della Prevenzione della Corruzione è tenuto inoltre a trasmettere a Finpiemonte Partecipazioni S.p.A, nella persona del Responsabile della Prevenzione della Corruzione, le informazioni richieste aventi ad oggetto l'applicazione del PTPC.

Con particolare riferimento al fenomeno del c.d. "***whistleblowing*", l'art. 54-bis del decreto legislativo 165/2001 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche), prevede che: «fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile, il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia».

La tutela del dipendente pubblico che segnala illeciti è stata introdotta nel nostro ordinamento quale misura di prevenzione della corruzione, imponendo peraltro alle amministrazioni di individuare una procedura finalizzata a garantire tale tutela e a stimolare le segnalazioni da parte del dipendente.

A tal proposito è visto con favore da parte dell'ANAC l'inserimento di misure che vadano nella prospettiva di riforma dell'istituto. In particolare per colmare le lacune della norma e indirizzare gli enti nell'utilizzo di tale strumento di prevenzione della corruzione l'ANAC ha adottato la determinazione n. 6 del 28 aprile 2015 *«Linee guida in materia di tutela del dipendente pubblico che segnala illeciti»*.

L'ANAC sottolinea la necessità che la segnalazione, ovvero la denuncia, sia "in buona fede": la segnalazione deve essere effettuata nell'interesse dell'integrità dell'ente; l'istituto, quindi, non deve essere utilizzato per esigenze individuali, ma finalizzato a promuovere l'etica e l'integrità nell'ente.

Particolare attenzione deve essere posta inoltre dai vertici dell'amministrazione e dal RPCT affinché non si radichino, in conseguenza dell'attività svolta dal RPCT, comportamenti discriminatori.

Il PNA 2016 evidenzia altresì che non vi è una gerarchia fra i canali di segnalazione previsti dal legislatore, non dovendosi, quindi, sanzionare (disciplinarmente) il dipendente che non si rivolge all'interno della propria amministrazione per denunciare situazioni di *maladministration*.

Qualora le segnalazioni riguardino il Responsabile della prevenzione della corruzione gli interessati possono inviare le stesse direttamente all'ANAC.

Si ricorda che l'ANAC si sta dotando di una piattaforma *Open Source* basata su componenti tecnologiche stabili e ampiamente diffuse: si tratta di un sistema in grado di garantire, attraverso l'utilizzazione di tecnologie di crittografia moderne e standard, la tutela della confidenzialità dei questionari e degli allegati, nonché la riservatezza dell'identità dei segnalanti.

9.11 Sistema disciplinare

Il sistema disciplinare previsto nel presente Modello si applica anche alle violazioni del Piano triennale per la prevenzione della corruzione.

9.12 Programmazione triennale

2017	• Aggiornamento PTPC • Verifica e implementazione delle misure anticorruzione • Verifica e Implementazione delle procedure interne • Coordinamento RPCT e OdV • Predisposizione della relazione del RPCT • Formazione specifica • Verifica/implementazione della sezione "Società trasparente" sul sito web di S.I.TO SPA (sia da un punto di vista sostanziale – dati richiesti; sia da un punto di vista formale – link, accessibilità del sistema) • Definizione delle procedure di monitoraggio sull'adempimento degli obblighi di pubblicazione • Definizione di un sistema di "accesso civico generalizzato"
2018	• Valutazione operato del 2017 in materia di trasparenza e di prevenzione della corruzione • Verifica e implementazione delle misure anticorruzione • Verifica e Implementazione delle procedure interne • Coordinamento RPCT e OdV • Valutazione dell'accessibilità del sistema • Aggiornamento della sezione del sito web in tema di trasparenza • Predisposizione della relazione del RPCT • Formazione specifica

2019	• Valutazione operato del 2018 in materia di trasparenza e di prevenzione della corruzione • Verifica e implementazione delle misure anticorruzione • Verifica e Implementazione delle procedure interne • Coordinamento RPCT e OdV • Aggiornamento della sezione del sito web in tema di trasparenza • Predisposizione della relazione del RPCT • Formazione specifica