




# MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

**secondo il D.Lgs. 231/01 e ss.mm. e ii.**

Rev.	Data	Descrizione revisione
-	31/10/2014	Versione per commenti
0	29/04/2015	Prima emissione
1	14/07/2017	Revisione generale
2	28/03/2018	Modifiche ai par. 7.4 e 8.2 per riforma in tema di whistleblowing
3	07/06/2018	Revisione per introduzione nuovi reati richiamati dal D.Lgs. 231 (razzismo e xenofobia, immigrazione clandestina)
4	04/04/2019	Modifica al par. 4.2 per introduzione del reato contro le P.A. legato al traffico di influenze illecite
5	23/06/2020	Revisione per introduzione nuovi reati richiamati dal D.Lgs. 231 (frode in competizioni sportive ed esercizio abusivo del gioco d'azzardo, reati tributari, violazione del perimetro di sicurezza nazionale cibernetica)
6	25/09/2020	Revisione per introduzione nuovi reati richiamati dal D.Lgs. 231 (nuovi reati di contrabbando, integrazione reati contro le PA e tributari)
7	28/06/2022	Revisione per introduzione nuovi reati richiamati dal D.Lgs. 231 (reati in strumenti di pagamento, reati contro il patrimonio culturale)
8	06/04/2023	Integrazione di dettagli sul processo di segnalazione di violazioni del modello in accordo alla normativa del Whistleblowing
9	12/12/2023	Modifiche generali al Cap. 7.4 "Flussi informativi"
10	15/05/2024	Modifiche al Cap. 4.2 per aggiornamento di tutti i key officers
11	03/09/2025	Inserimento di nuovo reato (art.25 undevicies)
Redazione		Verifica
Funzione: RSGI		Funzione: AD
Firma: 		Firma: 
		Approvazione
		Funzione: AD (Delibera CdA)
		Firma: 

## Sommario

<b>1. INTRODUZIONE .....</b>	<b>3</b>
1.1 La Società .....	3
1.2 Sistema di <i>governance</i> .....	4
1.3 La struttura organizzativa .....	5
1.4 I Sistemi di Gestione .....	5
1.5 Rapporti con società collegate.....	5
<b>2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI SILOMAR .....</b>	<b>6</b>
2.1 Implementazione del Modello .....	7
2.2 Adozione, modifiche ed integrazioni del Modello .....	7
<b>3. METODOLOGIA DI VALUTAZIONE DEI RISCHI .....</b>	<b>8</b>
<b>4. ATTIVITÀ NEL CUI AMBITO POSSONO ESSERE COMMESSI REATI.....</b>	<b>9</b>
4.1 Individuazione dei reati applicabili all'Organizzazione .....	9
4.2 Individuazione dei processi coinvolti, delle attività sensibili e dei key officers .....	12
<b>5. SISTEMI DI CONTROLLO.....</b>	<b>17</b>
5.1 Struttura dei sistemi di controllo (standard) .....	17
5.2 Standard di controllo in Silomar.....	18
5.3 Il sistema documentale aziendale .....	19
<b>6. MAPPATURA DELLE AREE DI ATTIVITÀ A RISCHIO .....</b>	<b>19</b>
<b>7. ORGANISMO DI VIGILANZA.....</b>	<b>20</b>
7.1 Individuazione dell'organo di controllo interno (OdV).....	20
7.2 Responsabilità e compiti dell'Organismo di Vigilanza (OdV) .....	21
7.3 Nomina dell'OdV .....	22
7.4 Flussi informativi .....	23
7.5 Attività di vigilanza e auditing.....	24
7.6 Risorse a disposizione dell'Organismo di Vigilanza .....	24
<b>8. SISTEMA DISCIPLINARE E SANZIONATORIO .....</b>	<b>25</b>
8.1 Funzione del sistema disciplinare .....	25
8.2 Violazione del Modello 231.....	25
8.3 Misure nei confronti di quadri, impiegati e operai .....	25
8.4 Misure nei confronti dei dirigenti .....	26
8.5 Misure nei confronti degli Amministratori.....	26
8.6 Misure nei confronti dei Sindaci .....	26
<b>9. FORMAZIONE E COMUNICAZIONE.....</b>	<b>26</b>
9.1 Comunicazione ai componenti degli organi sociali .....	27
9.2 Formazione e comunicazione ai dirigenti, ai responsabili di servizio .....	27
9.3 Comunicazione per quadri, impiegati e operai.....	27
9.4 Formazione e comunicazione mediante strumenti informatici .....	27
9.5 Comunicazione a terzi .....	27
<b>10. ALLEGATI .....</b>	<b>27</b>

## 1. INTRODUZIONE

Il presente Modello di Organizzazione, Gestione e Controllo è stato implementato da Silomar al fine di rispondere ai requisiti Mediante del D.Lgs. 231/2001, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni". In particolare si riferisce alle disposizioni aziendali al fine di prevenire i seguenti reati:

- artt. 24 e 25 – reati commessi nei rapporti con la Pubblica Amministrazione
- art. 24 bis – delitti informatici e trattamento illecito dei dati, di violazione del perimetro di sicurezza nazionale cibernetica
- art. 24 ter – delitti di criminalità organizzata,
- art. 25 bis – reati di falsità in monete, in carte di pubblico credito e in valori di bollo e in strumenti o segni di riconoscimento,
- art. 25 bis 1 – delitti contro l'industria e il commercio,
- art. 25 ter – reati societari,
- art. 25 quater – delitti aventi finalità di terrorismo o di eversione dell'ordine democratico,
- 25 quater. 1 – pratiche di mutilazione degli organi genitali femminili.
- art. 25 quinquies – delitti contro la personalità individuale,
- 25 sexies – abusi di mercato, in relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato,
- 25 septies – omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro,
- 25 octies – ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio,
- 25 octies.1 – delitti in materia di strumenti di pagamento diversi dai contanti
- 25 novies – delitti in materia di violazione del diritto d'autore,
- 25 decies – dichiarazioni mendaci a autorità giudiziaria,
- 25 undecies – reati ambientali,
- 25 duodecies – impiego di cittadini di paesi terzi il cui soggiorno è irregolare ed immigrazione clandestina,
- 25 terdecies – razzismo e Xenofobia,
- 25 quaterdecies – frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati
- 25 quinquiesdecies – reati tributari
- 25 sexiesdecies – reati di contrabbando
- 25 septiesdecies – delitti contro il patrimonio culturale
- 25 duodevicies – riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici
- 25 undevicies - delitti contro gli animali
- reati transnazionali.

### 1.1 La Società

L'attività di impresa di Silomar S.p.A. si rivolge all'esercizio di imprese marittime per lo sbarco e l'imbarco di oli e grassi vegetali, minerali e animali, melassi, lattici, prodotti chimici e petrolchimici, carburanti e affini. La Società può altresì acquistare, gestire e noleggiare galleggianti e navi per conto proprio o per conto terzi, nonché acquistare, costruire e gestire silos, nell'ambito portuale, costiero e all'interno, per il deposito delle merci come sopra specificate.

Inoltre, l'attività di Silomar S.p.A. può riguardare qualsiasi operazione connessa a quelle suesposte, ivi

compreso il trasporto, anche via terra, delle merci sopra dette.

Infine, Silomar S.p.A. può assumere interessenze e partecipazioni in altre società od imprese, aventi oggetto simile al proprio.

Le informazioni di carattere generale relative alla società Silomar S.p.A. sono riportate nella tabella seguente.

Denominazione	Silomar S.p.A.
Sede Legale	Genova, Porto Ponte Etiopia
Sede Operativa	Genova, Porto Ponte Etiopia
Registro Imprese	T223165172
Numero REA	GE - 111753
Capitale Sociale	6.444.000,00 Euro
C.F.	00246590103
CCNL applicato	Contratto aziendale
Posizione INPS	3400596740
Posizione INAIL	Operai 046019621/14 - Impiegati 046200357/77
Sito web	www.silomar.it

## 1.2 Sistema di governance

Il sistema di amministrazione adottato da Silomar S.p.A. è quello ordinario.

La Società è amministrata da un Consiglio di Amministrazione composto da nove amministratori.

Le funzioni di controllo sono esercitate dal Collegio Sindacale, composto da cinque membri, di cui tre effettivi e due supplenti.

La legale rappresentanza della Società è attribuita al Presidente del Consiglio di Amministrazione e all'Amministratore Delegato. All'Amministratore Delegato spettano altresì tutti i poteri di ordinaria e straordinaria amministrazione della Società, esclusi quelli non delegabili per legge o Statuto. All'Amministratore Delegato sono stati conferiti in via esclusiva i poteri e doveri del "datore di lavoro" e del "committente" in materia di sicurezza ed igiene sul lavoro, nonché del "legale rappresentante" e "gestore" in materia di tutela dell'ambiente e del "gestore" in materia di prevenzione incidenti rilevanti.

All'interno del Consiglio di Amministrazione si evidenziano, a titolo esemplificativo, i seguenti poteri:

- uno dei membri del CdA è titolare del potere di rappresentanza della Società nei confronti degli Uffici Finanziari della Dogana, dell'Ufficio Tecnico di Finanza e della Direzione Regionale delle Entrate per la Liguria.
- uno dei membri del CdA è delegato dal Consiglio per lo sviluppo commerciale della società (Business Development)
- uno dei membri del CdA è delegato dal Consiglio per compiere alcuni atti di ordinaria amministrazione della Società, i quali possono individuarsi, a titolo esemplificativo e non esaustivo, come segue:
  - effettuare incassi e pagamenti, anche mediante l'emissione di assegni o bonifici bancari, nei limiti degli affidamenti concessi dagli istituti di credito della Società, nonché esigere ed incassare crediti della Società, rilasciandone quietanza;
  - effettuare e sottoscrivere comunicazioni e denunce agli enti preposti, relativamente agli adempimenti riguardanti il personale dipendente, le operazioni doganali e la normale attività, ivi comprese eventuali comunicazioni o denunce inerenti gli obblighi tributari;
  - effettuare e sottoscrivere ordini di acquisto di beni e servizi sino al limite di euro 10.000,00.

È inoltre incaricato con delega del CdA il Direttore Tecnico di Silomar, avente i seguenti poteri:

- effettuare e sottoscrivere ordini di acquisto di beni e servizi sino al limite di euro 25.000,00.

### 1.3 La struttura organizzativa

Al fine di rendere immediatamente evidente il ruolo e le responsabilità di ciascuno nell'ambito del processo decisionale aziendale, Silomar S.p.A. ha messo a punto un prospetto sintetico nel quale è schematizzata la sua struttura organizzativa.

Nell'Organigramma, in particolare, sono specificate:

- le aree in cui si suddivide l'attività aziendale;
- le linee di dipendenza gerarchica;
- i soggetti che operano nelle singole aree ed il relativo ruolo organizzativo.

Oltre all'organigramma, la struttura organizzativa aziendale è costituita anche dai mansionari aziendali, che contengono la descrizione di compiti e skills per ciascun ruolo aziendale citato nell'organigramma.

La struttura organizzativa così costituita, è divulgata all'interno dell'Organizzazione tramite:

- affissione dell'Organigramma presso luoghi accessibili a tutto il personale della Società;
- illustrazione, condivisione e consegna dei mansionari aziendali ai dipendenti in occasione di corsi di formazione interni.

La struttura organizzativa è puntualmente aggiornata in funzione dei cambiamenti che intervengono all'assetto organizzativo della società (modifiche ai ruoli aziendali, alle competenze, al personale che ricopre i ruoli aziendali).

### 1.4 I Sistemi di Gestione

Silomar S.p.A. persegue l'obiettivo di offrire un servizio adeguato alle esigenze dei suoi Clienti, assicurando nel contempo la tutela ambientale e della salute e sicurezza dei lavoratori. Pertanto, adotta un sistema di gestione integrato Qualità, Sicurezza e Ambiente, certificato secondo le normative UNI EN ISO 9001, UNI EN ISO 45001, e UNI EN ISO 14001, quale strumento finalizzato a garantire l'affidabilità del sistema di controllo interno nell'ambito di specifici processi.

### 1.5 Rapporti con società collegate

Silomar S.p.A. possiede partecipazioni nelle seguenti società, ognuna delle quali svolge attività analoghe alle proprie:

- SAAR Depositi Portuali S.p.A., nella quale Silomar ha una partecipazione pari al 40% del capitale sociale;
- Depositi Costieri di Savona S.p.A., di cui Silomar possiede il 73% del capitale sociale;
- Genoa Oil Trading S.r.l., nella quale Silomar ha una partecipazione pari all'8% del capitale sociale.

I rapporti intercorrenti tra Silomar S.p.A. e le società sopra elencate sono originati da contratto scritto.

SIGLE UTILIZZATE NEL PRESENTE DOCUMENTO:

SIGLA	DESCRIZIONE
AD	Amministratore Delegato
DT	Direttore Tecnico
RSGI	Responsabile Sistema di Gestione Integrato
SIGI	Sistema di Gestione Integrato
RPER	Responsabile del Personale / Risorse Umane
CDA	Consiglio di Amministrazione
DdL	Datore di Lavoro
ASPP	Addetto al Servizio di Prevenzione e Protezione
RSPP	Resp. Servizio di Prevenzione e Protezione

## 2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI SILOMAR

Silomar, sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, nonché consapevole dell'importanza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della posizione e dell'immagine propria, delle aspettative dei propri azionisti e del lavoro del personale che opera al suo interno e per la società, sotto qualunque forma contrattuale, ha ritenuto conforme alle proprie politiche aziendali procedere all'adozione del Modello di organizzazione, gestione e controllo previsto dal Decreto Legislativo 231/2001.

Tale iniziativa, sebbene non imposta dalle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio, si propone altresì di sensibilizzare tutti coloro che operano in nome e per conto di Silomar, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto stesso.

Il Modello (ispirato alle "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001" di Confindustria) che persegue l'obiettivo di configurare di un sistema strutturato e organico di regole aziendali volto a prevenire la commissione delle diverse tipologie di reati contemplate dal Decreto, si basa principalmente sui seguenti principi:

- Valutazione degli esiti del processo di Risk Assessment condotto propedeuticamente alla predisposizione del Modello, finalizzato alla valutazione dei rischi connessi con la commissione dei reati di cui agli Artt. 24 e 25 del D.Lgs. 231/01 e s.m.i, nell'ambito delle Attività Sensibili (aree a rischio) dell'organizzazione; (Cap.3)
- mappatura delle "aree di attività a rischio" dell'azienda, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati; (Cap.4)
- la definizione di regole aziendali (processi/procedure/norme comportamentali) per la gestione e il controllo delle "aree di attività a rischio" individuate; (Cap.5)
- la definizione della struttura organizzativa dell'azienda che preveda una chiara attribuzione di responsabilità e autorità alle diverse figure aziendali in relazione ai processi aziendali e alle relative attività compreso il sistema di deleghe;<sup>1</sup> (mansionari aziendali, organigramma)
- la definizione dei requisiti minimi previsti per il personale che ricopre posizioni professionali relativi all'applicazione del Decreto per le figure chiave; (Mansionari aziendali)
- la diffusione a tutto il personale aziendale delle regole aziendali stabilite e della struttura organizzativa, al fine di determinare, in tutti coloro che operano in nome e per conto di Silomar nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;
- il monitoraggio sulle "aree di attività a rischio", di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi, principalmente attraverso l'istituzione dell'Organismo di Vigilanza (OdV) con specifici compiti di controllo sull'efficace e corretto funzionamento del Modello; (Cap. 7)
- la verifica ex post dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico.

Tale Modello organizzativo viene completato dal Codice Etico che contiene l'insieme dei diritti, dei doveri e delle responsabilità di Silomar nei confronti dei "portatori d'interesse" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.). Il Codice Etico SILOMAR è riportato integralmente in Allegato 2.

<sup>1</sup> Nella definizione di responsabilità e autorità è prevista l'applicazione del principio della separazione delle funzioni, in base al quale nessuno può gestire in autonomia un intero processo;





Fig.1 – Esempificazione del funzionamento di un Modello organizzativo ex D.Lgs.231/01

## 2.1 Implementazione del Modello

Il presente documento descrive:

- le diverse tipologie di reato previste dal Decreto applicabili all'Azienda,
- le relative attività sensibili nell'ambito delle quali si possano commettere le varie fattispecie di reato,
- gli strumenti e i documenti adottati da Silomar per prevenire, vigilare e contrastare la commissione dei reati stessi,
- le principali aree di rischio riscontrate.

Il Modello è implementato attraverso l'applicazione di regole aziendali stabilite e documentate all'interno del sistema di gestione aziendale sviluppato in conformità ai requisiti delle norme ISO 9001, ISO 14001, ISO 45001 e del D.lgs 231/2001.

Secondo il principio del miglioramento continuo del Sistema di Gestione, la Struttura Documentale è in continuo aggiornamento a cura di RSGL, al fine, anche, di assicurare il miglioramento dei presidi di controllo sulle attività sensibili del Modello, e adeguarlo alle evoluzioni tecnico-organizzative aziendali.

La modifica e le integrazioni delle regole aziendali (processi/procedure/norme comportamentali) seguono modalità e responsabilità stabilite nella procedura di riferimento P1.1 Gestione documenti e registrazioni.

## 2.2 Adozione, modifiche ed integrazioni del Modello

Come sancito dal Decreto, l'adozione del Modello è "atto di emanazione dell'organo dirigente" (art. 6, comma 1, lett. a) del Decreto), di conseguenza, il presente documento è approvato dal Consiglio di Amministrazione di Silomar SpA.

Le successive modifiche nonché le integrazioni del presente documento sono rimesse alla competenza del Consiglio d'Amministrazione di Silomar.

### 3. METODOLOGIA DI VALUTAZIONE DEI RISCHI

Il processo di Risk Assessment propedeutico alla realizzazione del presente Modello si è sviluppato attraverso l'applicazione, fase per fase, del seguente criterio di analisi:

#### 1. INDIVIDUAZIONE DEI REATI APPLICABILI

Lettura critica dei reati citati dal D.Lgs.231/01 come individuati nel documento Risk Assessment e Elenco Reati D.lgs. 231/01, allegato 1 alla presente Parte Generale, in riferimento alla loro potenziale configurabilità nell'ambito della realtà aziendale di SILOMAR.

In questo contesto si è sempre tenuto a mente il fatto che la valutazione in commento non possa basarsi esclusivamente sul concetto di "rischio accettabile" come inteso normalmente nel contesto economico-societario.

Infatti, dal punto di vista economico il rischio è considerato "accettabile" quando i controlli aggiuntivi "costano" più della risorsa da proteggere.

Ovviamente tale percorso logico non è sufficiente per soddisfare i principi previsti dal Decreto 231. Tuttavia, è fondamentale individuare una soglia di rischio, posto che altrimenti la quantità di controlli preventivi diventerebbe virtualmente infinita, con le evidenti conseguenze da un lato sulla effettività del Modello, dall'altro sulla continuità operativa della Società.

Con riferimento alle fattispecie dolose si ritiene che il rischio sia adeguatamente fronteggiato quando il sistema di controllo preventivo è tale da non poter essere aggirato se non in modo fraudolento, così aderendo al dettato normativo del Decreto 231.

Quanto, invece, ai reati colposi, la soglia concettuale di accettabilità è rappresentata dalla realizzazione di una condotta, ovviamente connotata da involontarietà e non conforme ai principi ed alle regole previste dal Modello, nonostante la previsione di protocolli specifici e la puntuale osservanza degli obblighi di vigilanza previsti dal Decreto da parte dell'apposito Organismo di Vigilanza.

Pertanto, posto che il Modello deve fronteggiare sia ipotesi dolose sia ipotesi colpose, il primo obiettivo da perseguire è la regolamentazione ed il presidio delle attività che comportano un rischio di reato al fine di evitarne la commissione.

Su questo presupposto logico si è provveduto a mappare le aree potenzialmente esposte a rischio di reato, avendo come punto di riferimento le *best practices* e le indicazioni fornite dalle linee guida di Confindustria.

#### 2. INDIVIDUAZIONE DEI PROCESSI COINVOLTI, DELLE ATTIVITA' SENSIBILI E DEI KEY OFFICERS

Individuazione delle attività aziendali rilevanti ove può essere presente il rischio di commissione dei reati previsti dal D.Lgs. n. 231/01 (di seguito "Attività Sensibili"), e analisi dei processi aziendali. Per ogni processo e attività sensibile individuati, sono stati quindi identificati i referenti del singolo processo aziendale ("Key Officer").

#### 3. ATTRIBUZIONE DEL LIVELLO DI RISCHIO

La classificazione del rischio, utilizzata al fine della presente mappatura, è la seguente:

- Rischio SPECIFICO: direttamente collegato dipendente dall'attività concretamente svolta da SILOMAR;
- Rischio RESIDUALE: associabile ad alcune attività di SILOMAR, o comunque propria, almeno astrattamente, a qualsiasi realtà aziendale;
- Rischio REMOTO: minimo, se non assente, rispetto all'attività d'impresa della Società.

#### 4. DEFINIZIONE DEL PIANO D'AZIONE FINALIZZATO ALL'ADOZIONE DEL MODELLO ORGANIZZATIVO

A fronte dell'analisi complessiva condotta durante le fasi precedenti, è stato definito un piano d'azione, adottato dall'organizzazione per rendere il Modello Organizzativo adeguato ed efficace nella prevenzione di tutti i reati



di cui al D.Lgs.231.

Tutte le risultanze delle fasi di cui sopra sono state riportate all'interno del documento in allegato 1 "Risk Assessment e Elenco Reati", il quale ha costituito base per l'adeguamento del sistema documentale dell'Organizzazione avvenuto propedeuticamente all'emissione del presente Modello.

## 4. ATTIVITÀ NEL CUI AMBITO POSSONO ESSERE COMMESSI REATI

### 4.1 Individuazione dei reati applicabili all'Organizzazione

In relazione all'analisi dell'operatività e dell'organizzazione aziendale, sono stati individuati tutti i reati potenzialmente verificabili in azienda a suo vantaggio, riportati di seguito:

Rif. D.Lgs.231/01	Fattispecie di reato	Livello di rischio	Motivazioni
Art. 24	Reati contro le Pubbliche Amministrazioni	<b>SPECIFICO</b>	Il rischio di commissione di reati contro le PP.AA. si manifesta nelle attività sensibili elencate nel Risk Assessment cui si rimanda (vedi All. 1)
Art. 24 bis	Delitti informatici e trattamento illecito dati	<b>RESIDUALE</b>	La Società dispone di Sistemi Informatici propri e di postazioni informatiche.
	Violazione del perimetro di sicurezza nazionale cibernetica	<b>REMOTO</b>	Data l'attività svolta non vi sono elementi per ritenere astrattamente realizzabili tale ipotesi di reato.
Art. 24 ter	Delitti di criminalità organizzata	<b>REMOTO</b>	Data l'attività svolta non vi sono elementi per ritenere astrattamente realizzabili tale ipotesi di reato.
Art. 25	Reati contro le Pubbliche Amministrazioni: concussione e corruzione	<b>SPECIFICO</b>	Il rischio di commissione di reati contro le PP.AA. si manifesta nelle attività sensibili elencate nel Risk Assessment cui si rimanda (vedi All. 1)
Art. 25 bis	Falsità in monete, strumenti o segni di riconoscimento	<b>REMOTO</b>	La Società non dispone né direttamente né indirettamente dei mezzi tecnici idonei per la commissione di detti reati
Art. 25 bis 1	Delitti contro l'industria e il commercio	<b>RESIDUALE</b>	Data l'attività svolta da Silomar, non vi sono elementi per ritenere astrattamente realizzabili tale ipotesi di reato.
Art. 25 ter	Reati societari (inclusa la corruzione tra privati secondo l'art. 25 ter, lett. s bis)	<b>SPECIFICO</b>	Il rischio di commissione di reati societari si manifesta nelle attività sensibili elencate nel Risk Assessment cui si rimanda (vedi All. 1)

Rif. D.Lgs.231/01	Fattispecie di reato	Livello di rischio	Motivazioni
Art. 25 quater	Reati di terrorismo o eversione dell'ordine democratico	<b>RESIDUALE</b>	Si ritiene che i presidi posti dall'impianto procedurale adottato dalla Società siano idonei a prevenire la realizzazione di tali fattispecie di reato.
Art. 25 quater 1	Mutilazione degli organi genitali femminili	<b>REMOTO</b>	Tali fattispecie non risultano al momento essere astrattamente ipotizzabili nel contesto della Società alla luce dell'attività svolta dalla stessa.
Art. 25 quinquies	Delitti contro la personalità individuale	<b>REMOTO</b>	Alla luce dell'operatività della Società, non risultano profili di rischio che rendano ragionevolmente fondata la possibilità della commissione di tali reati nell'interesse o a vantaggio della stessa.
Art. 25 sexies	Reati di abusi di mercato (market abuse)	<b>REMOTO</b>	La Società non è quotata in borsa. Non sono state ravvisate attività sensibili.
Art. 25 septies	Reati di omicidio e lesioni con violazione delle norme antinfortunistiche	<b>SPECIFICO</b>	Sono attività sensibili tutti gli adempimenti in materia di salute e sicurezza sul lavoro elencati dall'art. 30 D.Lgs. 81/08.
Art. 25 octies	Ricettazione, riciclaggio, impiego di beni di provenienza illecita, nonché autoriciclaggio	<b>RESIDUALE</b>	Si ritiene che l'impianto procedurale consenta di verificare costantemente le modalità di acquisizione e gestione del denaro, nonché per la prevenzione del delitto di autoriciclaggio.
Art. 25 octies 1	Delitti in materia di strumenti di pagamento diversi dai contanti	<b>RESIDUALE</b>	Si ritiene che l'impianto procedurale consenta di verificare costantemente le modalità di pagamento non in contante.
Art. 25 novies	Violazione dei diritti d'autore	<b>REMOTO</b>	Data l'attività svolta da Silomar, tali fattispecie non risultano essere astrattamente ipotizzabili.
Art. 25 decies	Dichiarazioni mendaci a autorità giudiziaria	<b>REMOTO</b>	Allo stato attuale non vi sono elementi per ritenere che la Società possa essere sottoposta al rischio connesso con la fattispecie di cui all'art. 377-bis.
Art. 25 undecies	Reati ambientali	<b>SPECIFICO</b>	Il rischio di commissione di reati ambientali si manifesta nelle attività sensibili elencate nel Risk Assessment cui si rimanda (vedi All. 1)

Rif. D.Lgs.231/01	Fattispecie di reato	Livello di rischio	Motivazioni
Art. 25 duodecies	Cittadini di paesi terzi con soggiorno irregolare ed immigrazione clandestina	<b>SPECIFICO</b>	L'attività sensibile in relazione a tale fattispecie di reato è individuabile nella gestione del personale di nazionalità di un Paese terzo rispetto all'Unione Europea.
Art. 25 terdecies	Razzismo e Xenofobia	<b>REMOTO</b>	Allo stato attuale non vi sono elementi per ritenere che la Società possa essere esposta al rischio connesso a tali fattispecie.
Art. 25 quaterdecies	Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati	<b>REMOTO</b>	Tali fattispecie non risultano al momento essere astrattamente ipotizzabili nel contesto della Società alla luce dell'attività svolta dalla stessa.
Art.25 quinquiesdecies	Reati tributari	<b>SPECIFICO</b>	Il rischio di commissione di reati tributari si manifesta nelle attività sensibili elencate nel Risk Assessment cui si rimanda (vedi All. 1)
Art.25 sexiesdecies	Contrabbando	<b>RESIDUALE</b>	Si ritiene che l'impianto procedurale consenta di verificare costantemente le modalità di gestione della merce in deposito, per la prevenzione del delitto di contrabbando
Art.25 septiesdecies	Delitti contro il patrimonio culturale	<b>REMOTO</b>	Tale fattispecie non risulta al momento essere astrattamente ipotizzabile (non previsti acquisti di opere d'arte, attività svolta in passato)
Art.25 duodevicies	Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici	<b>REMOTO</b>	Tale fattispecie non risulta al momento essere astrattamente ipotizzabile (non previsti acquisti di opere d'arte, attività svolta in passato)
Art.25 undevicies	Delitti contro gli animali	<b>REMOTO</b>	Tale fattispecie non risulta al momento essere astrattamente ipotizzabile (non vengono gestiti animali e gli stessi non rientrano nella filiera direttamente legata Silomar)
-	Reati transnazionali	<b>REMOTO</b>	Tale fattispecie di reato non è astrattamente realizzabile nell'ambito della Società, in quanto Silomar non ha sedi all'estero.

## 4.2 Individuazione dei processi coinvolti, delle attività sensibili e dei key officers

Ogni fattispecie di reato per cui è stata sancita la potenziale applicabilità all'Azienda, è stata quindi contestualizzata alla realtà Silomar, in modo da individuare nel dettaglio i processi aziendali che potrebbero generare il reato, definire le singole attività sensibili nell'ambito del processo, identificare le relative responsabilità. Di seguito si riportano le Attività Sensibili individuate in Silomar riferite ad ogni fattispecie di reato, e i relativi key officers:

Classe di Reato	Processo/attività sensibile	Key Officer
<b>Delitti con finalità di terrorismo, di eversione dell'ordine democratico e di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio</b>	1. Acquisto di beni/servizi con controparti considerate a rischio	AD-DT
	2. Selezione dei partner commerciali/finanziari e gestione dei relativi rapporti con controparti considerate a rischio	CDA-AD-RESP. AMMINISTRAZIONE-DT
	3. Realizzazione di investimenti - ivi compresi i progetti di sviluppo - con controparti considerate a rischio (es. progetti di partnership con depositi siti in Paesi considerati a rischio)	CDA-AD
	4. Negoziazione e stipulazione di contratti di intermediazione con controparti considerate a rischio (es. contratti con spedizionieri)	AD-DT
	5. Stipulazione di contratti con altri depositi per servizi di stoccaggio a propri Clienti	CDA-AD
	6. Realizzazione e gestione di iniziative umanitarie e di solidarietà (es. donazioni o altre liberalità), sponsorizzazioni, spese di rappresentanza e omaggi, condotte in Paesi ed/o Organizzazioni considerati a rischio	CDA-AD-RESP. CONTABILITÀ-RESP. AMMINISTRAZIONE
	7. Gestione di server della Società o di siti internet (inserimento o divulgazione di informazioni)	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	8. Assunzione di personale	RPER-AD-DT
	9. Consulenze e prestazioni professionali	AD-DT-RPER
	10. Gestione delle transazioni finanziarie (pagamenti/incassi/piccola cassa), e uso di carte di credito	AD-RPER-RESP. CONTABILITÀ-RESP. AMMINISTRAZIONE
	11. Accessi al deposito	AD-DT-LOGISTICA
<b>Reati contro la personalità individuale</b>	1. Attività che prevedono il ricorso diretto o indiretto a manodopera (es. affidamenti di appalti)	DT-RPER
	2. Realizzazione e gestione di iniziative umanitarie e di solidarietà (es. donazioni o altre liberalità), sponsorizzazioni, spese di rappresentanza e omaggi	CDA-AD-RESP. CONTABILITÀ-RESP. AMMINISTRAZIONE
	3. Gestione di server della Società o di siti internet (inserimento di informazioni)	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	4. Assunzione di personale	RPER-AD-DT
<b>Market abuse</b> (illeciti di abuso di informazioni privilegiate e manipolazione del mercato)	1. Gestione delle comunicazioni al mercato/comunità finanziaria e della riservatezza delle informazioni privilegiate che possono essere diffuse e/o utilizzate per l'acquisto, la vendita o altre operazioni sugli strumenti finanziari	CDA-AD

Classe di Reato	Processo/attività sensibile	Key Officer
	2. Acquisizione di contratti con Clienti in condizioni concorrenziali (es. caso di manipolazione dei prezzi, diffusione di notizie false)	CDA-AD
<b>Falsità in strumenti o segni di riconoscimento, nonché contro l'industria e il commercio</b>	1. Realizzazione e sviluppo di nuove soluzioni / tecnologie di servizio e strumenti	AD-DT
	2. Erogazione del servizio secondo procedure e istruzioni definite	DT-LOGISTICA- REPARTO OPERATIVO
	3. Acquisto e/o cessione di beni/servizi	AD-DT
	4. Gestione delle attività promozionali e pubblicitarie	AD
	5. Sviluppo e attuazione delle politiche commerciali	CDA-AD-DT
	6. Utilizzo di software sottoposti a licenza	AD-RPER-RESP. AMMINISTRAZIONE- RESP.CONTABILITÀ
	7. Vendita di servizi	CDA-AD-DT
	8. Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali	CDA-AD-DT
	9. Negoziazione/stipulazione di contratti ai quali si perviene mediante la partecipazione a procedure competitive ( <i>attualmente non applicabile, ma potenzialmente verificabile in futuro</i> )	AD-DT
<b>Violazione del diritto d'autore</b>	1. Gestione delle modalità di accesso al sistema informatico degli utenti interni ed esterni, gestione dei profili utente e del processo di autenticazione	AMMINISTRATORE DI SISTEMA (società esterna incaricata) - RPER
	2. Gestione e protezione dei software, dei contenuti, delle reti, delle comunicazioni	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	3. Gestione delle attività di inventariazione dei beni (licenze informatiche)	RESP. CONTABILITÀ
	4. Gestione della comunicazione esterna ed interna che prevede l'utilizzo di materiale coperto da diritto d'autore	CDA-AD
	5. Gestione delle attività promozionali e pubblicitarie	AD
	6. Gestione delle attività formative / ricreative che prevedono l'utilizzo di materiale coperto da diritto d'autore	DT-RPER
<b>Cittadini di paesi terzi con soggiorno irregolare ed immigrazione clandestina</b>	1. Assunzione di personale	RPER -AD-DT
<b>Omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro</b>	1. Pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro	AD(DL)-RSPP-RSGI
	2. Sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro	AD(DL)-DIRIGENTE SICUREZZA
	3. Individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro	AD(DL)-RSPP
	4. Attività di informazione formazione e addestramento in tema di salute, sicurezza e igiene sul lavoro	AD(DL)-DIRIGENTE SICUREZZA-RSGI- RPER
	5. Rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro	DT-RSGI-RSPP

Classe di Reato	Processo/attività sensibile	Key Officer
	6. Gestione degli asset aziendali con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro	DT-RSPP
	7. Controllo e azioni correttive con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro	RSGI
	8. Riesame della Direzione con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro	AD-RSGI
	9. Gestione dei rapporti con soggetti pubblici in occasione di ispezioni	AD(DL)-RSPP-DT
<b>Reati ambientali</b>	1. Acquisizione e/o cessione di asset in relazione ai quali insistono obblighi ambientali	AD(ANCHE IN QUALITÀ DI GESTORE)-DT
	2. Realizzazione, esercizio, gestione e/o modifica di asset in relazione ai quali insistono obblighi in materia ambientale in capo all'ente	AD(GESTORE)-DT
	3. Gestione degli scarichi idrici	AD(GESTORE)-DT-REPARTO OPERATIVO
	4. Gestione delle attività di carico/scarico nave	DT-REPARTO OPERATIVO
	5. Gestione degli adempimenti e delle attività connessi alla bonifica, a seguito di un evento che sia potenzialmente in grado di contaminare il suolo, il sottosuolo, le acque superficiali e/o le acque sotterranee	AD(GESTORE)-DT-CAPISQUADRA
	6. Caratterizzazione e classificazione rifiuti	DT-RSGI
	7. Gestione delle attività di raccolta e deposito temporaneo dei rifiuti, e avvio delle operazioni di recupero o smaltimento dei rifiuti raccolti, in linea con il criterio di deposito temporaneo scelto, nei limiti previsti dalla normativa vigente	DT-RSGI-ADDETTO SGI
	8. Gestione delle attività di trasporto, smaltimento dei rifiuti e relativa attività di intermediazione	DT-RSGI-ADDETTO SGI
	9. Gestione delle emissioni atmosferiche	AD(GESTORE)-DT
	10. Gestione delle sostanze lesive dell'ozono	DT-RSGI
	11. Gestione dei rapporti con soggetti pubblici per ottenimento di autorizzazioni ambientali, e in occasione di ispezioni da parte degli Organismi Competenti	AD(GESTORE)-DT
<b>Reati societari</b>	1. Predisposizione del bilancio annuale	AD-RESP. CONTABILITÀ
	2. Predisposizione di relazioni, altre comunicazioni sociali, o bilanci provvisori infrannuali, dirette al socio o al pubblico, nonché nel caso di rilascio di attestazioni richieste dalla legge	AD-RESP. CONTABILITÀ
	3. Gestione rapporti con soci, società di revisione, collegio sindacale	CDA-AD-RESP. CONTABILITÀ
	4. Operazioni sul capitale e destinazione dell'utile: restituzione dei conferimenti, ripartizione degli utili o delle riserve, operazioni sulle azioni, formazione del capitale, altre operazioni sul capitale sociale	CDA
	5. Comunicazione, svolgimento e verbalizzazione Assemblee	CDA



Classe di Reato	Processo/attività sensibile	Key Officer
<b>Delitti informatici e trattamento illecito dei dati</b>	1. Pianificazione generale delle misure da adottare in materia di sicurezza del sistema informatico e telematico, classificazione e trattamento di dati e informazioni	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	2. Gestione delle modalità di accesso al sistema informatico degli utenti interni ed esterni, gestione dei profili utente e del processo di autenticazione;	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	3. Gestione delle attività di inventariazione dei beni	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	4. Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	5. Gestione e protezione della postazione di lavoro	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	6. Gestione e protezione dei software, dei contenuti, delle reti, delle comunicazioni	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	7. Gestione degli aspetti inerenti alla sicurezza fisica (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.)	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	8. Gestione delle attività di acquisizione e sviluppo di apparecchiature, dispositivi (anche di rilevazione) o programmi informatici e di servizi di installazione, manutenzione, connessione o di altra natura relativi a hardware, software e reti e relative componenti tecniche connesse con il sistema	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	9. Monitoraggio / verifica periodica del sistema informatico in tema di sicurezza	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
	10. Gestione degli incidenti e dei problemi di sicurezza informatica.	AMMINISTRATORE DI SISTEMA (società esterna incaricata)
<b>Reati contro le Pubbliche Amministrazioni, corruzione, concussione e traffico di influenze illecite</b>	1. Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni, licenze, concessioni per l'esercizio delle attività aziendali	AD-AMMINISTRATORI CON POTERI DI FIRMA
	2. Gestione dei rapporti con i soggetti pubblici relativi all'assunzione e gestione di personale (anche appartenente a categorie protette o la cui assunzione è agevolata)	AD- RPER
	3. Gestione dei rapporti con organismi di vigilanza relativi allo svolgimento di attività regolate dalla legge	AD (GESTORE, DL) - DT
	4. Richiesta di provvedimenti amministrativi occasionali / ad hoc necessari allo svolgimento di attività strumentali a quelle tipiche aziendali (es. DIA, SCIA, permessi di costruire)	AD (GESTORE, DL) - DT
	5. Predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere	AD-RESP. CONTABILITÀ-RESP. AMMINISTRAZIONE
	6. Gestione di procedimenti giudiziali o arbitrali (contenziosi)	AD-AMMINISTRATORI CON POTERI DI FIRMA

Classe di Reato	Processo/attività sensibile	Key Officer
	7. Utilizzo di siti web o software della pubblica amministrazione	AD-RPER-DT-RESP. ADEMPIMENTI FISCALI DOGANALI- ADDETTI UFF.AMM.
<b>Criminalità organizzata, reati transnazionali e di intralcio alla giustizia</b>	1. Approvvigionamento di beni o servizi (anche transnazionali)	AD-DT
	2. Realizzazione e gestione di iniziative umanitarie e di solidarietà (es. donazioni o altre liberalità), sponsorizzazioni, spese di rappresentanza e omaggi	CDA-AD-RESP. AMMINISTRAZIONE
	3. Realizzazione di investimenti - ivi compresi i progetti di sviluppo	CDA-AD-DT
	4. Gestione di vendita di servizi	CDA-AD-DT
	5. Designazione degli organi sociali e del management di consociate nonché del management della Società;	CDA-AD
	6. Gestione dei rapporti con amministratori, dipendenti o terzi coinvolti in procedimenti giudiziari	AD- AMMINISTRATORI CON POTERI DI FIRMA
	7. Negoziazione e stipulazione di contratti di intermediazione (es. contratti con spedizionieri)	AD-DT
	8. Selezione ed assunzione del personale	RPER -AD-DT
	9. Selezione dei partner commerciali/finanziari e gestione dei relativi rapporti con controparti considerate a rischio	CDA-AD-DT
	10. Autorizzazione e vigilanza sugli accessi fisici agli uffici e al deposito	DT-UFFICIO OPERATIVO
	11. Gestione delle armi nell'ambito delle attività di vigilanza (attività indiretta)	AD
	12. Consulenze e prestazioni professionali	AD-DT- RPER - RESP.CONTABILITA'
	13. Uso di carta di credito	AD- RPER - RESP.CONTABILITA'
<b>Razzismo e Xenofobia</b>	1. Interfaccia con autisti	REPARTO LOGISTICA
	2. Attribuzione di ruoli e incarichi in azienda; assunzione del personale	RPER-AD-DT
<b>Reati tributari</b>	1. Acquisto di beni/servizi	AD-DT
	2. Gestione della contabilità e del debito ai fornitori	AD-DT-RPER- RESP.CONTABILITA'
	3. Gestione spese di rappresentanza e note spese	AD-RESP. AMMINISTRAZIONE- RPER- RESP.CONTABILITA'
	4. Rapporti con l'Amministrazione Finanziaria	AD-RESP. AMMINISTRAZIONE- RPER- RESP.CONTABILITA'
	5. Gestione della tesoreria	AD-RESP. AMMINISTRAZIONE- RPER- RESP.CONTABILITA'
	6. Gestione della contabilità e del credito commerciale	AD-RESP. AMMINISTRAZIONE- RPER- RESP.CONTABILITA'

Classe di Reato	Processo/attività sensibile	Key Officer
	7. Gestione della contabilità e della relativa archiviazione	AD-RESP. CONTABILITÀ
	8. Dismissione di cespiti e operazioni straordinarie	AD-CDA-RESP. AMMINISTRAZIONE - RESP. CONTABILITÀ
	9. Predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere	AD-RESP. CONTABILITÀ-RESP. AMMINISTRAZIONE
	10. Gestione del processo di contabilità e bilancio (reati connessi con gravi frodi IVA, indebite compensazioni, dichiarazioni infedeli/omesse)	AD-RESP. CONTABILITÀ
<b>Reati di contrabbando</b>	1. Gestione fiscale/doganale del deposito	AD-DT
<b>Reati in materia di strumenti di pagamento diversi dai contanti</b>	1. Pagamenti tramite carte di credito aziendali, bonifici, assegni	AD-RESP. CONTABILITÀ-RPER
	2. Utilizzo di sistemi informatici per pagamenti vari (remote banking)	AD-RESP. CONTABILITÀ-RPER
	3. Trasferimento di valori da/verso conti Silomar	AD-RESP. CONTABILITÀ-RPER-RESP. AMMINISTRAZIONE
<b>Reati contro il patrimonio culturale</b>	1. Acquisto di opere d'arte	AD-CDA

## 5. SISTEMI DI CONTROLLO

### 5.1 Struttura dei sistemi di controllo (standard)

I presidi finalizzati alla prevenzione del rischio di commissione dei reati previsti dal D.Lgs. n. 231 del 2001 affiancano l'osservanza del Codice Etico Silomar (allegato 2), principio generale non derogabile del Modello 231, e sono strutturati su due livelli di controllo:

- standard generali di trasparenza delle attività**, che devono essere sempre presenti in tutte le Attività Sensibili prese in considerazione dal Modello 231;
- ulteriori standard di controllo specifici**, che prevedono disposizioni particolari volte a disciplinare gli aspetti peculiari delle Attività Sensibili e che devono essere contenuti nelle procedure aziendali di riferimento.

Tali standard sono definiti come di seguito:

STANDARD GENERALI DI TRASPARENZA DELLE ATTIVITÀ'	DEFINIZIONE
<b>1. SEGREGAZIONE</b>	Si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla <sup>2</sup>

<sup>2</sup> È attribuita allo standard la seguente qualificazione:

- il principio della segregazione deve sussistere considerando l'attività sensibile nel contesto dello specifico processo di appartenenza;
- la segregazione sussiste in presenza di sistemi codificati, complessi e strutturati ove le singole fasi siano coerentemente individuate e disciplinate nella gestione, con conseguente limitazione di discrezionalità applicativa, nonché tracciate nelle decisioni assunte.

STANDARD GENERALI DI TRASPARENZA DELLE ATTIVITA'	DEFINIZIONE
<b>2. NORME</b>	Esistenza di procedure/protocolli/norme/circolari: devono esistere disposizioni aziendali e/o di gruppo e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
<b>3. POTERI</b>	Poteri autorizzativi e di firma: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società.
<b>4. TRACCIABILITA'</b>	Ogni operazione relativa all'Attività Sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile <i>ex post</i> , anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.
<b>STANDARD DI CONTROLLO SPECIFICI:</b>	Ogni sistema di controllo intrapreso dall'Azienda aggiuntivo ai quattro standard succitati. Il sistema di controllo interno può essere definito come un insieme di meccanismi, procedure e strumenti predisposti dalla direzione per assicurare il conseguimento degli obiettivi di efficienza delle operazioni aziendali, affidabilità delle informazioni finanziarie, rispetto delle leggi e dei regolamenti e salvaguardia dei beni aziendali.

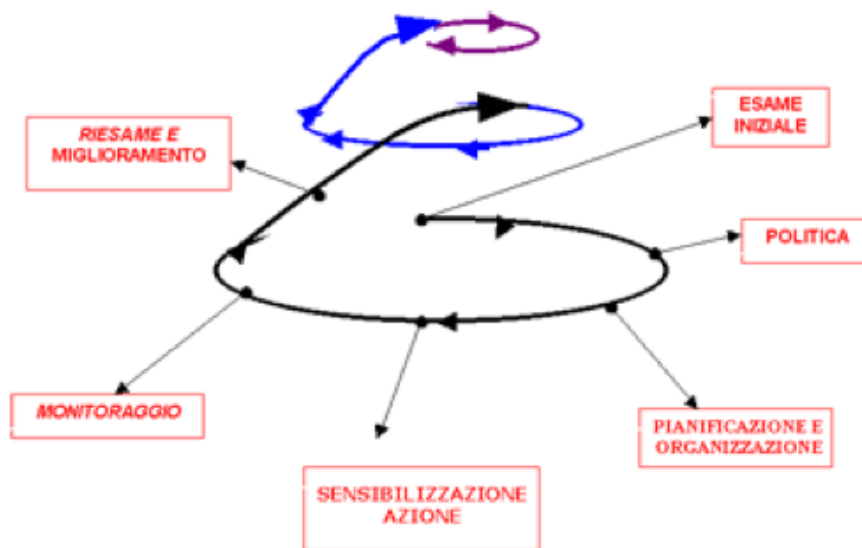


Fig. 2 – Schema riassuntivo dei principi di controllo (fonte: Linee Guida Confindustria)

## 5.2 Standard di controllo in Silomar

Ogni Attività Sensibile identificata (vedi par. 3.2) è controllata tramite l'applicazione dei quattro standard generali di trasparenza delle attività, e da eventuali ulteriori standard di controllo specifici, indicati all'interno dell'Allegato 1 "Risk Assessment e Elenco Reati".

Le funzioni competenti assicurano il recepimento nelle procedure aziendali degli standard generali di trasparenza e specifici con riferimento a tutte le Attività Sensibili. Le procedure aziendali sono comunicate e diffuse all'interno dell'organizzazione in applicazione al documento P1.1 Gestione documenti e registrazioni.

Il management e i dipendenti di Silomar S.p.A. sono tenuti all'osservanza delle procedure aziendali. Attività Sensibili e Standard di controllo specifici del Modello 231 (contenuti in Allegato 2) sono comunicati ai primi riporti dell'Amministratore Delegato da parte dell'Organismo di Vigilanza.

### 5.3 Il sistema documentale aziendale

Tutti i documenti del sistema di gestione integrato sono elencati all'interno del modulo P1.1 MO.01 Gestore documentale. Si evidenzia che l'attuale struttura documentale, suddivisa in n.14 processi aziendali, è frutto di una radicale riedizione di tutto il sistema, avvenuta nel corso dell'ultimo anno a cura di RSGI.

## 6. MAPPATURA DELLE AREE DI ATTIVITÀ A RISCHIO

Considerate tutte le attività sensibili mappate al Cap.5, e i relativi sistemi di controllo in atto mappati al cap. 6, si individuano le seguenti aree di attività considerate a rischio (RISCHIO SPECIFICO), ovvero quelle degne di particolare attenzione durante le attività di vigilanza da parte dell'OdV:

Processo/attività considerata a rischio	CLASSE DI REATO A RISCHIO SPECIFICO				
	Contro PP.AA.	Societari	Amb.	SSL	Tributari
Processo P2 "Operatività del deposito", con particolare riferimento al controllo sulla prevenzione di reati ambientali e di violazione delle norme antinfortunistiche, e al controllo delle attività fiscali-doganali			X	X	
Processo P3.1 "Approvvigionamento di beni e servizi", e gestione dei rapporti con i fornitori		X	X	X	X
Processo P4.1 "Gestione del processo commerciale", con riferimento ai rapporti contrattuali coi Clienti		X			X
Processo P5 "Manutenzione e ispezione", e documentazione correlata			X	X	
Processo P6 "Gestione del personale", in riferimento alle modalità di assunzione e alla formazione del personale sui temi ambiente e sicurezza			X	X	
Processo P8 "Gestione ambientale", e documentazione correlata			X		
Processo P9 "Gestione Salute, Sicurezza e Prevenzione Incidenti Rilevanti", e documentazione correlata				X	
Processo P10 "Miglioramento continuo", in riferimento alle aree ambiente e sicurezza			X	X	
Processo P14.1 "Gestione contabilità e bilancio", e documentazione correlata		X			X
Processo P14.2 "Gestione dei rapporti ordinari con le PP.AA."	X		X	X	X
Processo P14.3 "Gestione dei flussi di cassa", in relazione al controllo delle transazioni finanziarie e sull'uso delle carte di credito		X			X
Processo P14.4 "Omaggi e liberalità"		X			X

Processo/attività considerata a rischio	CLASSE DI REATO A RISCHIO SPECIFICO				
	Contro PP.AA.	Societari	Amb.	SSL	Tributari
Processo P14.6 "Gestione fatturazione"		X			X
Processo P14.7 "Gestione degli accertamenti e delle ispezioni da parte delle PP.AA."	X		X	X	X
Sistema di deleghe, mansionari aziendali, ruoli e responsabilità nell'organizzazione, con particolare riferimento all'ambiente e alla sicurezza e salute dei lavoratori			X	X	
Designazione degli organi sociali e del management di consociate nonché del management della Società		X			
Gestione rapporti con soci e Collegio Sindacale		X			X
Comunicazione, svolgimento e verbalizzazione Assemblee		X			X
Operazioni sul capitale e destinazione dell'utile: restituzione dei conferimenti, ripartizione degli utili o delle riserve, operazioni sulle azioni, formazione del capitale, altre operazioni sul capitale sociale		X			
Richiesta di provvedimenti amministrativi occasionali / ad hoc necessari allo svolgimento di attività strumentali a quelle tipiche aziendali (es. DIA, SCIA, permessi di costruire)	X	X			
Predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere		X			X
Gestione di procedimenti giudiziali o arbitrali (contenziosi)		X			
Utilizzo di siti web o software della pubblica amministrazione	X				

## 7. ORGANISMO DI VIGILANZA

### 7.1 Individuazione dell'organo di controllo interno (OdV)

Contestualmente all'adozione del Modello, il Consiglio di Amministrazione conferisce ad un organo collegiale (*Organismo di Vigilanza - OdV*) composto da almeno due membri, l'incarico di assumere le funzioni di controllo interno, con il compito di vigilare sull'osservanza, sull'applicazione e sull'efficacia del Modello, nonché di curarne l'aggiornamento e di partecipare alla predisposizione delle regole aziendali (processi/procedure/norme comportamentali) idonee a garantirne il più corretto funzionamento, per quanto di competenza.

Per Silomar l'Organismo di Vigilanza, in relazione ai compiti che è chiamato a svolgere, viene definito in modo da rispondere, nel suo complesso, alle seguenti caratteristiche:

- ✓ **autonomia e indipendenza:** l'OdV è collocato come unità di staff in elevata posizione gerarchica e ai relativi membri non sono attribuiti compiti operativi in modo da non minare l'obiettività di giudizio;



- ✓ **professionalità:** Il bagaglio di conoscenze, strumenti e di tecniche di cui i membri dell'OdV devono essere dotati per poter svolgere efficacemente l'attività assegnata è assicurato da un'accurata definizione dei requisiti minimi che devono essere soddisfatti per poter ricoprire il ruolo di membro dell'OdV;
- ✓ **continuità di azione:** per poter dare la garanzia di efficace e costante attuazione del modello viene stabilito che i Responsabili di Funzione, in particolare il Responsabile del Sistema di Gestione Aziendale, supportino l'OdV nell'attività di monitoraggio e di verifica periodica;
- ✓ **poteri di modifica e di iniziativa:** l'OdV ha il potere/dovere di intraprendere le iniziative necessarie per adeguare il modello alle esigenze connesse al verificarsi di deviazioni o violazioni rispetto alle norme previste nel modello stesso o alle esigenze concrete dell'organizzazione,

che si possono sintetizzare come di seguito:

REQUISITO	CHE COSA SIGNIFICA
<b>AUTONOMIA E INDIPENDENZA</b>	<p>Evitare che all'Organismo di vigilanza complessivamente inteso siano affidati compiti operativi. Non deve esserci identità tra controllato e controllante.</p> <p>Eliminare ingerenze e condizionamenti di tipo economico o personale da parte degli organi di vertice.</p> <p>Prevedere nel Modello cause effettive di ineleggibilità e decadenza dal ruolo di membri dell'Organismo di vigilanza, che garantiscano onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.</p>
<b>PROFESSIONALITÀ</b>	<p>Nominare soggetti competenti in materia ispettiva e consulenziale, in grado di compiere attività di campionamento statistico, di analisi, valutazione e contenimento dei rischi, di elaborazione e valutazione dei questionari.</p> <p>È opportuno che almeno taluno tra i membri dell'Organismo di vigilanza abbia competenze giuridiche.</p>
<b>CONTINUITÀ</b>	<p>Predisporre una struttura dedicata all'attività di vigilanza sul modello.</p> <p>Curare la documentazione dell'attività svolta.</p>

I Membri dell'Organismo di Vigilanza di Silomar S.p.A. sono costituiti dalle seguenti figure:

- un membro esterno: consulente Legale-Finanziario
- un membro esterno: consulente tecnico esperto in organizzazione aziendale, con competenze esplicite in ambiente e sicurezza

L'OdV si riunisce almeno due volte all'anno o, comunque, nel caso se ne verificasse la necessità a seguito di segnalazioni o eventi critici.

## 7.2 Responsabilità e compiti dell'Organismo di Vigilanza (OdV)

All'OdV è conferita la responsabilità di vigilare:

1. sull'osservanza delle prescrizioni del Modello, in relazione alle diverse tipologie di reati contemplate dal Decreto;
2. sull'efficacia del Modello in relazione alla struttura aziendale ed all'effettiva capacità di prevenire la commissione dei reati;
3. sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione alle mutate condizioni aziendali.

Per questo all'OdV sono affidati i seguenti compiti:

- ✓ attuare direttamente, ove necessario, periodici controlli, oltre a quelli previsti per il management operativo, nell'ambito delle aree di attività a rischio. Le evidenze di tali attività devono essere raccolte, elaborate e conservate in conformità a quanto stabilito dalla procedura P10.3 "Audit Interni";

- ✓ controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione cartacea/informativa a supporto delle attività rilevanti a norma del Decreto in conformità a quanto stabilito dalla procedura P1.1 "Gestione documenti e registrazioni";
- ✓ promuovere e monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello coordinandosi con le funzioni competenti (RPER, RSGI) al personale direttivo e con funzioni di rappresentanza, a tutto il personale compresi i neoassunti e ai Consulenti e Partners;
- ✓ partecipare al processo di erogazione delle sanzioni;
- ✓ interpretare la normativa rilevante e verificare l'adeguatezza del sistema di controllo interno in relazione a tali prescrizioni normative;
- ✓ riesaminare l'adeguatezza del sistema documentale aziendale ai fini di un efficace applicazione del modello;
- ✓ riesaminare periodicamente i processi aziendali e la struttura organizzativa ai fini dell'aggiornamento sia della mappatura delle aree di attività a rischio sia del modello stesso;
- ✓ riferire periodicamente al Presidente, al Consiglio di Amministrazione e al Collegio Sindacale in merito allo stato di attuazione e adeguatezza del Modello.

Tenuto conto della peculiarità delle attribuzioni dell'OdV e dei connessi contenuti professionali, nello svolgimento dei compiti di vigilanza e controllo l'OdV può avvalersi del supporto delle funzioni di staff e di linea che, di volta in volta, si rendessero necessarie anche utilizzando gli strumenti aziendali già regolamentati attraverso il sistema di gestione aziendale.

A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale rilevante e deve essere costantemente informato dal management:

- a) sugli aspetti dell'attività aziendale che possono esporre l'azienda al rischio conseguente alla commissione di uno dei reati previsti dal D. Lgs. 231/2001;
- b) sulla struttura organizzativa e il sistema delle deleghe e delle procure adottato dalla Società;
- c) sui rapporti con Consulenti e Partner;
- d) sui rapporti predisposti dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- e) su ogni informazione proveniente da terzi comprese le segnalazioni aventi ad oggetto ogni violazione o per le quali vi sia il fondato motivo di ritenere che possa essere stata commessa una violazione del Modello, effettuate in forma scritta, orale o telematica;
- f) informazioni relative ad atti ufficiali quali:
  - ✓ i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto e successive estensioni;
  - ✓ le richieste di assistenza legale inoltrate dai Dipendenti, e dagli Amministratori dirigenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
  - ✓ i procedimenti disciplinari comminati e delle eventuali sanzioni irrogate.

L'OdV, per lo svolgimento delle proprie funzioni, oltre all'autonomia citata, deve poter utilizzare le strutture della società, nei limiti in cui queste non debbano essere distolte dalle loro occupazioni ordinarie. L'OdV può essere supportato da un legale esterno, nell'interpretazione degli eventuali casi di più difficile soluzione.

### 7.3 Nomina dell'OdV

L'OdV è nominato dal Consiglio di Amministrazione, al quale è anche data la possibilità di revoca nei casi di infedeltà, inefficienza, negligenza nel suo operato o accertata impossibilità ad adempiere il compito affidato. L'incarico di Organismo di Vigilanza, della durata da uno a tre anni, è affidato con delibera del Consiglio di Amministrazione e conseguente accettazione dei soggetti interessati. Nella stessa delibera il Consiglio di Amministrazione determina la misura del compenso annuo.

È ammessa la revoca anche nei casi in cui, per qualsiasi motivazione, il CDA ritenga siano venuti meno i requisiti di indipendenza, parentela ed assenza di conflitti di interessi.

Costituiscono cause di ineleggibilità e/o di decadenza dell'Organismo di Vigilanza e delle risorse umane dedicate:

- la condanna, con sentenza passata in giudicato, per aver commesso uno dei reati previsti dal D.Lgs.

231/2001; ovvero

- la condanna, con sentenza passata in giudicato, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese. In casi di particolare gravità, anche prima del giudicato, il Consiglio di Amministrazione potrà disporre - sentito il parere del Collegio Sindacale - la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un interim. Fatta salva l'ipotesi di una rivisitazione del ruolo e del posizionamento dell'Organismo di Vigilanza sulla base dell'esperienza di attuazione del Modello, l'eventuale revoca degli specifici poteri propri dell'Organismo di Vigilanza potrà avvenire soltanto per giusta causa, previa delibera del Consiglio di Amministrazione sentito il parere del Collegio Sindacale.

Al fine di sancire compiti, responsabilità e modalità di svolgimento del proprio ruolo all'interno di Silomar, una volta nominato l'OdV si dota di specifico Regolamento Interno.

## 7.4 Flussi informativi

### Reporting dell'Organismo di Vigilanza verso il vertice societario

L'OdV:

- Deve riferire sempre al Presidente del CDA e all'Amministratore Delegato.
- Deve riferire sui risultati, sulla conduzione e implementazione del modello al Collegio Sindacale.
- Deve esporre annualmente al CDA le risultanze della propria attività.
- Deve curare l'aggiornamento del Codice etico e precisare le modalità di segnalazione delle infrazioni.

Il reporting verso il vertice societario ha ad oggetto:

- ✓ l'attività svolta dall'OdV;
- ✓ le eventuali criticità emerse sia in termini di comportamenti o eventi interni a Silomar S.p.A., sia in termini di efficacia del Modello.

Il Consiglio di Amministrazione, il Presidente del Consiglio di Amministrazione e il Collegio Sindacale hanno la facoltà di convocare in qualsiasi momento l'OdV al fine di condividere eventuali criticità evidenziate nell'ambito delle attività di controllo, fermo restando il fatto che comunque una volta all'anno viene svolta una riunione congiunta OdV - Collegio Sindacale.

L'OdV, a sua volta, ha la facoltà di richiedere, per motivi urgenti:

- ✓ attraverso le funzioni o i soggetti competenti, la convocazione del Consiglio di Amministrazione;
- ✓ il coinvolgimento del Collegio Sindacale.

### Flussi informativi verso l'Organismo di Vigilanza, e tutela dell'anonimato del Whistleblower

I Destinatari del Modello sono tenuti a comunicare tempestivamente<sup>3</sup> all'OdV tutte le informazioni di cui venga a conoscenza tra quelle disciplinate all'interno della procedura P12.1 "Comunicazione, consultazione e partecipazione"; a titolo esemplificativo, le informazioni verso l'OdV devono riguardare modifiche alla governance aziendale, provvedimenti disciplinari, situazioni di emergenza, segnalazioni previste dal Codice della Crisi d'Impresa dell'Insolvenza, prescrizioni impartite dagli organi ispettivi, infortuni, criticità durante trattative con clienti o fornitori, assunzioni di personale, ecc.

Tutte le informazioni di cui sopra devono essere fornite, in via diretta oppure tramite il proprio responsabile, via mail all'indirizzo di posta elettronica ***organismovigilanza.silomar@gmail.com***.

Inoltre, ai sensi di quanto disposto dall'art. 6, commi 2 bis, 2 ter e 2 quater, devono essere inviate all'Organismo di Vigilanza segnalazioni circostanziate di condotte illecite ovvero di violazioni delle norme comportamentali del Modello Organizzativo e del Codice Etico, rilevanti ai sensi del D. Lgs. 231/2001, e fondate su elementi di fatto precisi e concordanti. In tali casi, il Segnalante\* si dovrà rivolgere all'OdV in forma anonima, attraverso i canali di comunicazione interna descritti nella P12.1 "Comunicazione, consultazione e partecipazione", cui si rimanda per dettagli.

*\* i segnalanti possono essere tutti quei soggetti che sono a vario titolo coinvolti con l'attività Silomar: collaboratori autonomi, liberi professionisti che prestano consulenza o lavorano per Silomar, volontari e tirocinanti anche non retribuiti, azionisti, amministratori, ex dipendenti, candidati ad una posizione lavorativa*

Silomar infatti, in accordo alla normativa sul *whistleblowing*, assicura la tutela l'anonimato del Segnalante (o Whistleblower), degli eventuali facilitatori (es. associazioni, famiglia del segnalante), dei colleghi che operano all'interno del medesimo contesto lavorativo del segnalante, e degli enti di proprietà del segnalante o in cui il

<sup>3</sup> entro 10 giorni lavorativi

segnalante lavora. In ogni caso è assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in mala fede. I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione.

Il processo di accertamento e gestione della segnalazione anonima ricevuta dall'OdV, verrà attuato in accordo a tempi, metodi e responsabilità indicati nella procedura P12.1 "Comunicazione, consultazione e partecipazione", cui si rimanda per dettagli. Si rende noto che la segnalazione, sia essa effettuata in forma anonima o meno, verrà presa in considerazione solo qualora la stessa risulti, ad esclusivo avviso dell'Organismo di Vigilanza, fondata su elementi di fatto precisi e concordanti, e vengano allegati dati certi ed immediatamente riscontrabili. Sono vietati atti di ritorsione o discriminatori, diretti o indiretti nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione: tutti coloro che commettano atti di ritorsione o discriminatori, saranno sanzionati secondo il successivo Cap. 8.

Si ricorda che l'omissione di comunicazioni all'OdV in merito a informazioni prescritte è considerata inadempimento alle obbligazioni derivanti dal rapporto di lavoro ai sensi dell'art. 2104 c.c. e dell'art. 2106 c.c.

#### **Raccolta e conservazione delle informazioni**

Ogni informazione, segnalazione, report previsti nel Modello sono conservati dall'Organismo di Vigilanza secondo quanto previsto nel proprio Regolamento. I dati e le informazioni conservate nel database sono poste a disposizione di soggetti esterni all'Organismo di Vigilanza previa autorizzazione dell'Organismo di Vigilanza. Quest'ultimo definisce, con apposita disposizione interna, criteri e condizioni di accesso al database.

### **7.5 Attività di vigilanza e auditing**

Il corretto ed efficace svolgimento dei compiti di vigilanza affidati dalla Legge all'OdV sono presupposti indispensabili e assolutamente inderogabili per l'esonero dalla responsabilità, sia che il reato sia stato commesso dai soggetti "apicali" sia che sia stato commesso dai soggetti sottoposti all'altrui direzione. Questo è il senso dell'art. 7, comma 4, del D.Lgs. 231/2001 il quale prevede che l'efficace attuazione del modello richiede, oltre all'istituzione di un sistema disciplinare, una sua verifica periodica, che ragionevolmente può essere attuata solo da parte dell'Organismo a ciò appositamente dedicato. A tale OdV, pur risultando soggetto autonomo ed indipendente da esso, sono attribuiti i compiti di verifica, applicazione ed aggiornamento dei modelli di organizzazione, gestione e controllo.

Pertanto, a cadenza almeno annuale, o comunque ogni volta se ne ravvisi la necessità (es. successivamente da accadimento di eventi, a su segnalazione da parte dei Destinatari, o su richiesta del CdA, ecc.), l'OdV provvede affinché venga effettuata attività di vigilanza sul corretto rispetto del Modello Organizzativo e del Sistema di Gestione aziendale da parte di tutti i soggetti aziendali coinvolti nel modello stesso. Per realizzare la vigilanza periodica, l'Organismo può avvalersi di soggetti esterni competenti ritenuti di volta in volta necessari.

I soggetti delegati alle attività di vigilanza devono essere individuati dall'OdV con atto formale (incarico con specifica tecnica riportante almeno il dettaglio delle attività di vigilanza, le tempistiche, le modalità di conduzione delle interviste, i soggetti destinatari coinvolti, le modalità di rendicontazione).

A seguito delle attività svolte, i soggetti che hanno condotto la vigilanza registrano su opportuni report le evidenze e risultanze della vigilanza svolta. Successivamente a validazione da parte dell'OdV dei report, l'OdV provvede alla divulgazione dei rapporti stessi ai soggetti apicali (CdA, AD, responsabili d'area/funzione).

I destinatari coinvolti nell'eventuale definizione e attuazione di azioni correttive/preventive a seguito di rilievi emersi in sede di Vigilanza, sono obbligati a rendicontare all'OdV la definizione e chiusura delle azioni intraprese, secondo le modalità indicate nella specifica procedura del SGI di gestione delle "Non conformità, Azioni Correttive / Azioni di miglioramento".

Tutte le evidenze relative alle attività di vigilanza, comprese le varie comunicazioni resesi necessarie, sono archiviate a cura dell'OdV.

Le risultanze delle attività annuali di vigilanza sono oggetto di reporting verso il vertice societario (vedi Par. 8.3).

### **7.6 Risorse a disposizione dell'Organismo di Vigilanza**

Con la delibera di nomina, il Consiglio di Amministrazione autorizza l'Organismo di Vigilanza, per tutta la durata dell'incarico, ad avvalersi, in qualsiasi momento, della collaborazione di tutte le funzioni interne della società, nonché dei consulenti esterni e dei revisori.

Il Consiglio d'Amministrazione, nella delibera di nomina, e successivamente con apposita delibera adottata all'inizio di ogni anno, stanza il budget a disposizione dell'Organismo di Vigilanza tale da consentirgli l'efficace espletamento del proprio incarico.

## 8. SISTEMA DISCIPLINARE E SANZIONATORIO

Aspetto essenziale per l'effettività del Modello è la predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole aziendali (processi/procedure/norme comportamentali) previste dal Modello stesso (cfr. art. 6, comma secondo, lett. E, art. 7, comma quarto, lett. B)

Sono soggetti al sistema disciplinare di cui al presente Modello tutti i "Dipendenti", gli Amministratori, i collaboratori esterni e partner di Silomar, nonché tutti coloro che abbiano rapporti contrattuali con la Società. Il procedimento per l'irrogazione delle sanzioni di cui al presente sistema disciplinare tiene conto delle particolarità derivanti dallo status giuridico del soggetto nei cui confronti si procede.

Silomar provvederà direttamente all'applicazione delle sanzioni disciplinari nel caso le violazioni siano state compiute da proprio personale dipendente e/o da consiglieri di amministrazione.

Ai partner e ai consulenti che operano direttamente o con loro dipendenti all'interno di Silomar è richiesto di approvare esplicitamente il sistema disciplinare adottato dalla Società. Nel caso di violazioni compiute da soggetti di cui sopra, le Società e/o i Professionisti si impegnano a mettere in atto le sanzioni disciplinari che saranno indicate da Silomar a seguito del procedimento di infrazione rilevato dall'OdV e sanzionato dal CdA. L'applicazione delle sanzioni disciplinari, riferendosi alla violazione di tali regole, prescinde dal sorgere e dall'esito di un eventuale procedimento penale.<sup>4</sup>

L'OdV deve essere informato circa la gestione dei procedimenti disciplinari.

### 8.1 Funzione del sistema disciplinare

La definizione di sanzioni commisurate alla violazione e applicabili in caso di violazione del Modello 231 ha lo scopo di contribuire: (i) all'efficacia del Modello 231 stesso e (ii) all'efficacia dell'azione di controllo dell'Organismo di Vigilanza.

A tale proposito è predisposto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle prescrizioni indicate nel Modello 231, con riferimento sia ai soggetti in posizione apicale, sia ai soggetti sottoposti ad altrui direzione.

L'applicazione del sistema disciplinare è autonoma rispetto allo svolgimento e all'esito del procedimento eventualmente avviato presso l'Autorità giudiziaria competente.

L'Organismo di Vigilanza segnala alle funzioni competenti la notizia di violazione del Modello 231 e monitora, di concerto con il responsabile della gestione delle risorse umane, l'applicazione delle sanzioni disciplinari.

### 8.2 Violazione del Modello 231

Ai fini dell'ottemperanza della legge, a titolo esemplificativo, costituisce violazione del Modello 231: i) la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello 231 e/o del Codice Etico Silomar (All.2), ovvero l'omissione di azioni o comportamenti prescritti dal Modello 231 e/o dal Codice Etico Silomar, nell'espletamento delle Attività Sensibili; ii) la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello 231 e/o del Codice Etico Silomar, ovvero l'omissione di azioni o comportamenti prescritti dal Modello 231 e/o dal Codice Etico Silomar, nell'espletamento di attività connesse alle Attività Sensibili e/o nei processi di gestione delle provviste, ovvero inosservanza – nell'espletamento delle Attività Sensibili – delle procedure aziendali di riferimento nelle quali sono recepiti i presidi di controllo per le finalità di cui al D.lgs. 231/2001, che:

- a) esponcano la Società a una situazione oggettiva di rischio di commissione di uno dei reati contemplati dal d.lgs. n. 231 del 2001 e/o
- b) siano diretti in modo univoco al compimento di uno o più reati contemplati dal d.lgs. n. 231 del 2001 e/o
- c) tali da determinare l'applicazione a carico della Società di sanzioni previste dal d.lgs. n. 231 del 2001;

Le sanzioni disciplinari si applicano anche nei confronti di chi viola le misure di tutela adottate per le segnalazioni all'Organismo di Vigilanza nonché nei confronti di chi effettua, con dolo o colpa grave, segnalazioni che si rivelano infondate.

### 8.3 Misure nei confronti di quadri, impiegati e operai

A ogni notizia di violazione del Modello 231 comunicata da parte dell'Organismo di Vigilanza, è dato impulso

<sup>4</sup> Peraltro, i principi di tempestività ed immediatezza rendono non soltanto non doveroso, ma altresì sconsigliabile ritardare l'irrogazione della sanzione disciplinare in attesa dell'esito del giudizio eventualmente instaurato davanti all'Autorità Giudiziaria (così Linee Guida Confindustria II, 3).



da parte del responsabile della gestione delle risorse umane alla procedura di accertamento di presunti comportamenti illeciti posti in essere dai dipendenti:

i) nel caso in cui, in seguito all'accertamento delle mancanze ai sensi del contratto applicato, sia accertata la violazione del Modello 231 o del Codice Etico, è individuata ai sensi della procedura succitata e irrogata dal soggetto a ciò abilitato, nei confronti dell'autore della condotta censurata, la sanzione disciplinare prevista dal contratto applicabile;

ii) la sanzione irrogata è proporzionata alla gravità della violazione. Si terrà conto: dell'intenzionalità del comportamento o del grado della colpa; del comportamento complessivo del dipendente con particolare riguardo alla sussistenza o meno di precedenti disciplinari; del livello di responsabilità e autonomia del dipendente autore dell'illecito disciplinare; della gravità degli effetti del medesimo con ciò intendendosi il livello di rischio cui la Società ragionevolmente può essere stata esposta – ai sensi e per gli effetti del D.Lgs. n. 231 del 2001 – a seguito della condotta censurata; delle altre particolari circostanze che accompagnano l'illecito disciplinare.

Le sanzioni disciplinari previste dal Regolamento aziendale Silomar applicato sono:

- richiamo verbale;
- ammonizione scritta;
- sospensione dal lavoro e dalla retribuzione;
- licenziamento per giusta causa.

Per il dettaglio si rimanda al "quadro sanzionatorio" del Regolamento aziendale stesso.

Il Responsabile della gestione del Personale comunica l'irrogazione di tale sanzione, ovvero i provvedimenti di archiviazione con le relative motivazioni, all'Organismo di Vigilanza.

Sono rispettati tutti gli adempimenti di legge e di contratto relativi all'irrogazione della sanzione disciplinare.

## **8.4 Misure nei confronti dei dirigenti**

Alla notizia di una violazione del Modello 231 comunicata da parte dell'Organismo di Vigilanza, nel caso in cui la violazione del Modello 231 da parte di uno o più dirigenti sia accertata ai sensi del precedente paragrafo 8.3 lett. (i), la società adotta nei confronti dell'autore della condotta censurata quanto previsto per legge e per contratto applicabile, tenuto conto dei criteri ex paragrafo 8.3 lett. (ii). Se la violazione del Modello 231 fa venire meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

## **8.5 Misure nei confronti degli Amministratori**

L'Organismo di Vigilanza comunica al Collegio Sindacale e all'Amministratore Delegato la notizia di una violazione del Modello 231 commessa da parte di uno o più componenti del Consiglio di Amministrazione. Il Consiglio di Amministrazione, con l'astensione del soggetto coinvolto, procede agli accertamenti necessari e assume, sentito il Collegio Sindacale, i provvedimenti opportuni, che possono includere la revoca in via cautelare dei poteri eventualmente delegati, nonché la convocazione dell'Assemblea dei soci per disporre l'eventuale sostituzione.

## **8.6 Misure nei confronti dei Sindaci**

L'Organismo di Vigilanza comunica all'Amministratore Delegato del Collegio Sindacale e al Consiglio di Amministrazione la notizia di una violazione del Modello 231 commessa da parte di uno o più Sindaci. Il Collegio Sindacale, con l'astensione del soggetto coinvolto, procede agli accertamenti necessari e assume, sentito il Consiglio di Amministrazione, i provvedimenti opportuni.

# **9. FORMAZIONE E COMUNICAZIONE**

È data ampia divulgazione, all'interno ed all'esterno della struttura, dei principi contenuti nel Modello. La società si impegna a facilitare e promuovere la conoscenza del Modello da parte dei dipendenti, con grado di approfondimento diversificato a seconda della posizione e del ruolo, e il loro contributo costruttivo sui suoi contenuti.



## **9.1 Comunicazione ai componenti degli organi sociali**

Il Modello è comunicato formalmente dall'Organismo di Vigilanza a ciascun componente degli organi sociali.

## **9.2 Formazione e comunicazione ai dirigenti, ai responsabili di servizio**

I principi e i contenuti del Modello sono comunicati formalmente dall'Organismo di Vigilanza a tutti i dirigenti della società (a ruolo e in servizio), ai Responsabili di area/funzione mediante consegna di apposito documento predisposto dall'Organismo di Vigilanza in coordinamento con le funzioni aziendali competenti. I principi e i contenuti del Modello sono, inoltre, divulgati mediante corsi di formazione; i soggetti sopra individuati sono tenuti a partecipare ai corsi di formazione. La struttura dei corsi di formazione è definita dall'Organismo di Vigilanza in coordinamento con le funzioni aziendali competenti.

Gli interventi di formazione sono svolti secondo le modalità indicate all'interno della Procedura P6.2 "Informazione, formazione e addestramento".

## **9.3 Comunicazione per quadri, impiegati e operai**

Il documento informativo sul Modello 231 è affisso nelle bacheche aziendali e i principi e i contenuti del Modello sono comunicati a ciascun dipendente. Sono, inoltre, definite iniziative di informazione mirata per quadri, impiegati e operai (vedi la procedura P6.2 "Informazione, formazione e addestramento").

## **9.4 Formazione e comunicazione mediante strumenti informatici**

Il documento informativo sul Modello 231 è reso disponibile a tutti gli utenti - anche non dipendenti - del sito internet di Silomar. Le iniziative di formazione e informazione mirata possono svolgersi anche a distanza e mediante utilizzo di risorse informatiche.

## **9.5 Comunicazione a terzi**

In coerenza con quanto già previsto per il Codice Etico, il documento informativo sul Modello 231 è portato a conoscenza di tutti coloro con i quali la società intrattiene relazione d'affari. L'impegno al rispetto dei principi di riferimento del Modello da parte dei terzi aventi rapporti contrattuali con la società dovrà essere previsto da apposita clausola del relativo contratto che formerà oggetto di accettazione del terzo contraente.

# **10. ALLEGATI**

Costituiscono parte integrante del presente Modello i seguenti allegati:

- ✓ Allegato 1 – Risk assessment e elenco reati (*in revisione corrente*)
- ✓ Allegato 2 – Codice Etico (*in revisione corrente*).