Sviluppo Investimenti Territorio S.r.l.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Parte Speciale

Adottato dal Consiglio di Amministrazione in data 6 dicembre 2011

Aggiornato dall'Amministratore Unico in data 14 giugno 2017

Adottato dall'Amministratore Unico in data 9 marzo 2021

Sommario

1. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE E L'AUTORITÀ GIUDIZIARIA

a) Aree a rischio

I reati di cui agli artt. 24, 25 e 25-*decies* del Decreto presuppongono l'instaurazione di rapporti con la P.A. o con l'Autorità Giudiziaria.

Tenuto conto della molteplicità dei rapporti che SIT intrattiene con le Pubbliche Amministrazioni e del suo intento di perseguire la *best practice* nell'esercizio della propria attività operativa, **le aree di attività ritenute a rischio**, con riferimento ai reati in parola, sono le seguenti:

- Espletare procedure per l'ottenimento di provvedimenti autorizzativi da parte della P.A. (ad es. concessioni, autorizzazioni e licenze edilizie ed urbanistiche, permessi di costruire ecc.);
- Intrattenere rapporti con esponenti della P.A. che abbiano competenze in processi legislativi, regolamentari o amministrativi riguardanti la Società, quando tali rapporti possano comportare l'ottenimento di vantaggi rilevanti per la SIT stessa, dovendosi escludere l'attività di mera informativa, partecipazione a eventi o momenti istituzionali e scambio di opinioni relativamente a particolari politiche o normative;
- Indire, bandire e gestire procedure di gara o di negoziazione per l'assegnazione di appalti di lavori, di fornitura o di servizi, di concessioni, di partnership, di *asset* (complessi aziendali, partecipazioni, etc.) e operazioni assimilabili;
- Partecipare a procedure di gara o di negoziazione diretta indette da enti pubblici;
- Partecipare a procedure per l'ottenimento di erogazioni, contributi o finanziamenti agevolati da parte di enti pubblici;
- Gestire rapporti con operatori pubblici e privati nell'attività di individuazione delle aree oggetto di intervento da parte di SIT;
- Formalizzare con i Comuni i Protocolli di Intesa e le Convenzioni;
- Formalizzare Contratti di Associazione in Partecipazione con terzi per la realizzazione degli interventi immobiliari;
- Partecipare in associazione agli interventi con *partner* terzi con forme diverse (es.: *joint venture*, ATI, consorzi, ecc.);
- Assegnare, ai fini della indizione delle procedure di gara, incarichi di consulenza o di rappresentanza ad un soggetto terzo;
- Espletare procedure di evidenza pubblica per l'affidamento di servizi/lavori;
- Espletare la procedura ad evidenza pubblica di commercializzazione delle aree industriali;
- Gestire la procedura di commercializzazione delle aree dismesse;
- Gestire la negoziazione finale dell'offerta in forma privata con gli assegnatari dei lotti, secondo i criteri di assegnazione dei lotti indicati nel bando.

In linea generale, **i processi aziendali nei quali si presentano attività sensibili** con riferimento ai reati di cui agli artt. 24, 25 e 25 *decies* del Decreto, sono i seguenti:

- assegnazione lavori, servizi e forniture: prestazioni professionali, appalti e subappalti;
- gestione interventi di iniziativa della Regione Piemonte e per conto proprio: partecipazione (quale committente e/o quale soggetto in gara) a gare ed appalti pubblici ed a trattative; costruzione in proprio; attività immobiliare;
- tesoreria: attività finanziarie relative a gestione dei flussi finanziari, gestione dei fondi aziendali, impiego di disponibilità liquide;

- contabilità generale e bilancio: attività di registrazione, redazione, controllo e conservazione dei documenti contabili ed extracontabili relative, in particolare, a Bilancio e Controllo di gestione;
- processo di gestione dei sistemi informativi: attività supportate da sistemi informatici e telematici per l'elaborazione e la trasmissione di dati contabili, fiscali e gestionali;
- processo di gestione delle risorse umane: attività relative alla selezione, assunzione e gestione del personale dipendente.

b) Norme di condotta.

SIT intende assicurare che tutti i propri organi gestionali, i propri dipendenti in posizione sia apicale sia sottoposta, i propri collaboratori interni ed esterni, i propri consulenti, rappresentanti ed incaricati, per quanto possano essere coinvolti nello svolgimento di attività nelle Aree a Rischio, si attengano a regole di condotta conformi a quanto prescritto dalla stessa SIT.
Il fine perseguito è di prevenire e impedire il verificarsi di reati nei rapporti con la P.A.
Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Destinatari – con riferimento alle rispettive attività – sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- il Codice Etico;
- le procedure/regolamenti interne/i;
- ogni altra normativa relativa al sistema di controllo interno in essere nel Gruppo;
- il sistema disciplinare di cui al CCNL applicabile.

L'assunzione di impegni verso la Pubblica Amministrazione, le Istituzioni Pubbliche ed in genere verso i terzi è riservata esclusivamente all'Amministratore Unico e nel rispetto della più rigorosa osservanza delle disposizioni di legge e regolamentari applicabili. I contratti e le modalità attraverso le quali gli accordi stessi sono trattati e conclusi non devono in alcun modo compromettere l'integrità e la reputazione della Società. Tutta la documentazione relativa alle trattative e ai contatti con la Pubblica Amministrazione deve essere conservata per permettere verifiche da parte dell'Organismo di Vigilanza.
Nella stipulazione di contratti con la Pubblica Amministrazione per conto della Società, è vietato ricorrere a forme di mediazione o ad altra opera di terzi diversi dagli esponenti della stessa SIT, né corrispondere o promettere ad alcuno utilità a titolo di intermediazione, per facilitare o aver facilitato la conclusione o l'esecuzione del contratto.
L'adozione di queste procedure specifiche è finalizzata a:

- conferire trasparenza e riconoscibilità ai processi decisionali e attuativi, mediante la descrizione dei principi di attribuzione delle deleghe e dei poteri aziendali e della relativa loro estensione;
- prevedere meccanismi di controllo interno quali, per esempio, autorizzazioni, verifiche, documentazione delle fasi decisionali maggiormente rilevanti etc.;
- consentire una chiara e definita suddivisione dei compiti e responsabilità, in modo da evitare che vi sia identità fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli;
- evitare di concentrare i poteri decisionali in capo a pochi individui, attuando quanto più possibile il principio della "segregazione funzionale/contrapposizione degli interessi";
- evitare sovrapposizioni di ruoli e di competenze;
- garantire che i documenti riguardanti l'attività di impresa siano archiviati e conservati, a cura della funzione competente, con modalità tali da non permetterne la modificazione successiva, se non con apposita evidenza;
- vietare la corresponsione di compensi, provvigioni, o commissioni a Consulenti esterni, Collaboratori, o Soggetti Pubblici in misura non congrua rispetto alle prestazioni rese in favore di SIT e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe.

Posto che il dipendente pubblico "non chiede, per sé o per altri, né accetta, neanche in occasione di festività, regali o altre utilità salvo quelli d'uso di modico valore, da soggetti che abbiano tratto o comunque possano trarre benefici da

decisioni o attività inerenti all'ufficio", atti di cortesia commerciale, quali omaggi o forme di ospitalità, o qualsiasi altra forma di beneficio (anche sotto forma di liberalità) in favore dei Pubblici Ufficiali ed esponenti della P.A. sono consentiti solo qualora siano:

- di modico valore;
- previsti dalle prassi commerciali (ad esempio presenti natalizi);
- previsti per categorie di destinatari (ad esempio, presenti natalizi per fornitori);
- tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere interpretati, da un osservatore terzo ed imparziale, come atti destinati a garantire vantaggi e favori in modo improprio.

In ogni caso, gli atti di cortesia commerciale verso Pubblici Ufficiali devono essere sempre autorizzati ai sensi delle procedure aziendali.

c) Divieti

La Società stabilisce, in ossequio alle norme ordinamentali, la vigenza dei seguenti divieti, che tutti i Destinatari debbono osservare:

- effettuare elargizioni in denaro a pubblici funzionari o riceverle;
- al di fuori di quanto previsto dalla prassi aziendale, distribuire e/o ricevere omaggi e regali, oppure accordare altri vantaggi di qualsiasi natura, ossia ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici o a loro familiari che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per SIT. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico, culturale o d'immagine. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- quando è in corso una qualsiasi trattativa d'affari, richiesta o rapporto con la Pubblica Amministrazione, cercare di influenzare impropriamente le decisioni della controparte, comprese quelle dei funzionari che trattano o prendono decisioni, per conto della Pubblica Amministrazione;
- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione a titolo personale;
- promettere o dare a Pubblici Ufficiali o a qualsiasi esponente della P.A., direttamente o per interposta persona, denaro o altre utilità per ottenere dallo stesso una violazione del principio di imparzialità, ovvero prestazioni diverse da quelle che siano normalmente accordate o rifiutate ad altri;
- riconoscere compensi o effettuare prestazioni, in favore dei consulenti, rappresentanti, mediatori ed ogni altro genere di collaboratore, che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, di compenso ricevuto, alle caratteristiche del rapporto di *partnership* ed alle prassi vigenti in ambito locale;
- riconoscere compensi in favore di fornitori che non trovino adeguata giustificazione in relazione al tipo di controprestazione;
- presentare dichiarazioni non veritiere al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- chiedere al Pubblico Ufficiale o Incarico di Pubblico Servizio al di fuori di quanto necessario per il legittimo svolgimento dell'attività aziendale: informazioni di cui il P.U. dispone per ragioni di ufficio; comportamenti che ostacolino l'esercizio di diritti di terzi; comportamenti che intralcino l'esercizio della Pubblica Amministrazione;
- promettere o dare a Pubblici Ufficiali o Incaricati di Pubblico Servizio, direttamente o per interposta persona, denaro o altre utilità per ottenere: la trattazione di pratiche con ordini diversi da quello cronologico (o diverso ordine eventualmente previsto dalle norme vigenti); il rifiuto di prestazioni dovute a terzi concorrenti; il non rispetto di standard di qualità e di quantità fissati dalla P.A. nelle apposite carte dei servizi; la non continuità del servizio o la sua interruzione.

d) Obblighi di condotta

Oltre agli espressi divieti di cui sopra, vigono i seguenti obblighi di comportamento:

- i rapporti con ogni P.A. e con altri enti privati a partecipazione pubblica devono essere gestiti con trasparenza, nel rispetto della norme statuali vigenti, del Codice Etico e delle procedure interne;
- gli incarichi conferiti ai Consulenti ed ai Collaboratori devono essere proposti, negoziati, stipulati ed approvati nel rispetto della norme statuali vigenti, del Codice Etico e delle procedure interne;
- i contratti stipulati con i fornitori e i partner, devono essere proposti, negoziati, stipulati ed approvati nel rispetto della norme statuali vigenti, del Codice Etico e delle procedure interne;
- nessun tipo di pagamento può esser effettuato in contanti o in natura, con eccezione delle procedure di piccola cassa;
- le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi e dati veri e controllati ed, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- la gestione dei rapporti con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio devono ispirarsi a criteri di correttezza e trasparenza, in modo da garantire il buon andamento della funzione o del servizio e, quindi, l'imparzialità nello svolgimento degli stessi.
- i rapporti con la Pubblica Amministrazione devono essere gestiti solo dalla funzione aziendale competente o dalle persone specificatamente delegate a questo scopo, in virtù del conferimento di specifici poteri o della funzione esercitata all'interno dell'impresa, come definita negli specifici sistemi di organizzazione e gestione; alle ispezioni tributarie, giudiziarie, amministrative e comunque a qualsiasi attività svolta da soggetti pubblici nei confronti della Società, devono partecipare esclusivamente i soggetti espressamente delegati o incaricati. I soggetti delegati o incaricati di intrattenere rapporti con la P.A. non possono eccedere i limiti delle attribuzioni e competenze ricevute; nel caso le relazioni si sviluppino in modo anomalo o difforme alle prassi normali, deve essere coinvolto il diretto superiore.
- chiunque svolga attività nell'interesse o a vantaggio di SIT è tenuto a fornire alla P.A. dichiarazioni e documentazioni veritiere; il contenuto delle dichiarazioni e delle documentazioni deve essere comunque preventivamente verificato dal soggetto che lo sottoscrive o lo trasmette. La Società conserva copia delle dichiarazioni e dei documenti trasmessi.
- chiunque riceva da Pubblici Ufficiali o da qualsiasi esponente della P.A., direttamente o indirettamente, richieste di denaro, beni o altre utilità in cambio di benefici illeciti, ingiusti o comunque non necessari per il legittimo svolgimento dell'attività aziendale deve immediatamente segnalare il fatto all'Amministratore Unico ed all'Organismo di Vigilanza;
- qualora un Pubblico Ufficiale o un qualsiasi esponente della P.A., senza giustificato motivo, ritardi o affidi ad altri il compimento di attività o l'adozione di decisioni di propria spettanza, chieda per proprio uso privato materiale o attrezzature di cui dovrebbe disporre per ragioni di ufficio, chieda per proprio uso personale linee telefoniche, mezzi di trasporto, servizi o attrezzature della Società o dei suoi esponenti, chieda per uso personale utilità, beni o servizi di qualsiasi natura, deve essere data immediata informazione all'Amministratore Unico ed all'Organismo di Vigilanza, astenendosi dal dar seguito alle richieste.

Per quanto riguarda i rapporti con l'Autorità giudiziaria (reato di cui all'art. 25-*decies*, induzione indebita a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria) che vedano coinvolti esponenti aziendali, è fatto divieto di porre in essere atti di violenza, minaccia o coartazione, e di effettuare o promettere elargizioni in danaro o altre forme di utilità affinché l'indagato, l'imputato o il testimone non collabori con l'Autorità Giudiziaria e non renda dichiarazioni vere, oppure non riferisca in piena libertà la propria rappresentazione dei fatti, esercitando se ritenuto la facoltà di non rispondere, in virtù delle citate forme di condizionamento.

e) Flussi informativi all'Organismo di Vigilanza

Le funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi condotta anomala o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.

L'Organismo di Vigilanza potrà richiedere alle funzioni a vario titolo coinvolte di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.

I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.

L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/processi sensibili, affinché questo provveda ad adeguare conseguentemente il Modello.

2. SALUTE E SICUREZZA SUL LAVORO

a) Aree a rischio

La tutela della salute e della sicurezza sul lavoro è materia che pervade ogni ambito ed attività aziendale. Le aree sensibili sono tutte le attività connesse a garantire: la massima sicurezza tecnica, organizzativa e procedurale possibile nell'ambiente di lavoro; il completo rispetto delle norme vigenti in materia antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro.

In ottemperanza a quanto disposto dalla disciplina in materia di salute e sicurezza sul lavoro (D.Lgs. 81/2008), la Società adotta e tiene aggiornato il "Documento di Valutazione dei Rischi", che contiene:

- la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione (da ora in vanti RSPP), dei rappresentanti dei lavoratori per la sicurezza e dei medici competenti che hanno partecipato alla valutazione del rischio;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

b) Norme di condotta

Nello svolgimento delle attività, tutti i destinatari del Modello sono tenuti ad osservare i principi generali di comportamento che la Società ha individuato in conformità alla normativa in materia di tutela dell'igiene, della salute e della sicurezza dei lavoratori. In particolare, la Società adotta le seguenti misure generali:

- attenta valutazione dei rischi e completa trasposizione degli stessi nel Documento di Valutazione dei Rischi;
- eliminazione dei rischi per la salute e la sicurezza in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non sia possibile, loro riduzione al minimo;
- riduzione dei rischi alla fonte;
- programmazione della prevenzione mirando ad un complesso che integra in modo coerente le condizioni tecniche produttive ed organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro;
- sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
- rispetto dei principi ergonomici nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, anche per attenuare il lavoro monotono e quello ripetitivo;
- limitazione al minimo dei lavoratori che sono, o che possono essere, esposti al rischio;
- utilizzo limitato degli agenti chimici, fisici e biologici, sui luoghi di lavoro;
- controllo sanitario dei lavoratori in funzione dei rischi specifici;
- allontanamento del lavoratore dall'esposizione a rischio, per motivi sanitari inerenti la sua persona;
- misure igieniche;
- misure di protezione collettiva ed individuale;
- misure di emergenza da attuare in caso di pronto soccorso, di incendio, di evacuazione dei lavoratori e di pericolo grave ed immediato;
- uso di segnali di avvertimento e di sicurezza;
- regolare manutenzione di ambienti, attrezzature, macchine ed impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti;
- informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro;
- istruzioni adeguate ai lavoratori.

La SIT riconosce alla tutela della salute e sicurezza sul lavoro un'importanza fondamentale e imprescindibile nell'ambito della organizzazione aziendale, e si impegna a promuoverla avendo come obiettivo il miglioramento continuo delle proprie prestazioni in tema di sicurezza. Gli impegni includono:

- il rispetto della normativa nazionale e comunitaria relativa a salute e sicurezza sul lavoro;
- la predisposizione di un sistema organizzativo per il controllo e il miglioramento delle attività che presentano un potenziale rischio per la salute e sicurezza dei lavoratori.

La SIT si impegna pertanto ad assolvere agli obblighi giuridici relativi:

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

Con specifico riferimento alla **gestione dei cantieri** (artt. 88 e ss. del D.Lgs. 81/2008) che è nella responsabilità del "Committente", si attuano i seguenti processi:

- verifica dell'idoneità tecnico professionale delle imprese in appalto/subappalto e dei lavoratori autonomi;
- pianificazione delle fasi di lavorazione e loro valutazione con particolare riferimento alle interazioni delle attività interferenti anche al contorno del cantiere ed alla eventuale compresenza di attività della Società;
- designazioni di figure di legge (es. Responsabile dei lavori; Coordinatore per la progettazione e per l'esecuzione dei lavori) e predisposizioni dei piani di sicurezza e coordinamento nonché dei documenti di valutazione dei rischi interferenziali;
- esecuzione degli adempimenti tecnico-amministrativi, notifiche e comunicazioni alla pubblica amministrazione;
- coordinamento nell'esecuzione delle attività fra le imprese/lavoratori autonomi e controlli sul rispetto delle misure nel cantiere.

Nei cantieri temporanei o mobili allestiti in unità operative ove sono presenti collaboratori della Società, i rischi derivanti da interferenze tra le due attività sono gestiti dal Committente individuando le specifiche misure di prevenzione, protezione ed emergenza a tutela della salute e sicurezza dei collaboratori, dei clienti e delle imprese appaltatrici e lavoratori autonomi. Tali misure sono indicate nel Piano di Sicurezza e Coordinamento o nel Documento unico di valutazione dei rischi interferenziali (in relazione al rispettivo campo di applicazione) elaborato a cura dei soggetti individuati dal Committente, che può avvalersi anche del supporto della struttura di Prevenzione e Protezione del Datore di Lavoro della Società.

Con specifico riferimento alla **gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione** (art. 26 del D.Lgs. 81/2008) che è nella responsabilità sia del Datore di Lavoro che del Committente, si attuano i seguenti processi:

- verifica, con le modalità previste dalla normativa vigente, dell'idoneità tecnico professionale delle imprese (comprese le eventuali subappaltatrici) e dei lavoratori autonomi;
- informativa alla controparte circa i rischi specifici presenti nei luoghi in cui è chiamata ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla attività oggetto del contratto, nonché, ove previsto dalla normativa, predisposizione del Documento di Valutazione dei Rischi Interferenziali, da inviare all'offerente ai fini della formulazione dell'offerta e parte integrante del contratto, contenente le misure

idonee per eliminare o ridurre i rischi relativi alle interferenze delle attività connesse all'esecuzione del contratto;
- redazione della lettera di invito o del bando;
- predisposizione dell'offerta da parte dell'offerente con indicazione dei costi destinati alla sicurezza, inerenti alle misure per gestire le interferenze, in relazione all'entità e alle caratteristiche del servizio/fornitura offerti nonché contenente dichiarazione di presa di visione dei rischi, presenti nei luoghi ove si svolge l'attività, e delle relative misure per la loro eliminazione/riduzione;
- aggiudicazione del servizio e stipula del contratto;
- esecuzione del servizio/fornitura da parte dell'aggiudicatario e cooperazione e coordinamento con la controparte per la prevenzione dei rischi propri dell'attività oggetto del contratto nonché per gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, anche mediante reciproca informazione al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva ed i rischi insiti nell'eventuale compresenza di personale e collaboratori della Società;
- controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività.

Il Documento di Valutazione dei Rischi (DVR) definisce le responsabilità e le procedure al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato. In particolare, sono state individuate le figure aziendali che rivestono il ruolo, rispettivamente, di "Datore di Lavoro" e "Committente".
Il Rappresentante dei Lavoratori per la Sicurezza collabora attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni. Inoltre, egli, nel rispetto delle norme di legge in materia, può accedere alla documentazione aziendale inerente la valutazione dei rischi e le misure di prevenzione relative e chiedere informazioni al riguardo. Tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente ed il Responsabile del Servizio Prevenzione e Protezione visitano i luoghi di lavoro ove sono presenti lavoratori esposti a rischi specifici ed effettuano a campione sopralluoghi negli altri ambienti.

c) Divieti

È vietata qualsiasi condotta, anche omissiva, tale da mettere a rischio la salute e la sicurezza sul posto di lavoro.
È altresì vietata qualsiasi condotta, anche omissiva, tesa a non rispettare le prescrizioni e/o i divieti stabiliti dalla Società in tema di salute e sicurezza.
La ricerca di vantaggi per la Società, qualora comportino o possano comportare la violazione, dolosa o colposa, alle norme in tema di tutela della sicurezza e salute del lavoro, non è mai giustificata.
Ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni od omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

d) Misure tecniche ed organizzative

Le regole adottate da SIT al fine di prevenire la commissione dei reati di omicidio colposo e lesioni colpose assicurano l'adozione delle misure tecniche e organizzative imposte dal Testo Unico sulla Sicurezza (D.Lgs. 81/2008). Tali misure consistono principalmente nelle seguenti:
- individuazione, all'interno dell'azienda, delle figure che ai sensi di legge rivestono un ruolo di responsabilità in ordine all'applicazione della normativa in esame;
- predisposizione e costante aggiornamento del DVR;
- attuazione della sorveglianza sanitaria dei lavoratori ed eventuale allontanamento degli stessi dall'esposizione al rischio a tutela della loro incolumità;
- adozione nei luoghi di lavoro delle misure e dei requisiti tecnico-strutturali imposti dalla normativa e conseguente svolgimento di una regolare attività di manutenzione avente ad oggetto, oltre ai locali, anche gli impianti, le attrezzature e i dispositivi di sicurezza;
- adozione di adeguate misure di primo soccorso, di prevenzione degli incendi e di lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato e, più in generale, di gestione delle emergenze, designando preventivamente i lavoratori incaricati della loro attuazione;

- realizzazione di un'attività di informazione, formazione e addestramento;
- vigilanza sul rispetto e l'attuazione delle misure di prevenzione e protezione dai rischi;
- attenta scelta dei soggetti incaricati della realizzazione di opere o della fornitura di servizi autonomi;
- perfezionamento dei contratti di appalto, d'opera o di somministrazione secondo le modalità e i requisiti richiesti dalla legge e, in particolar modo, con indicazione in essi dei costi relativi alla sicurezza del lavoro e con la contestuale redazione del Documento Unico di Valutazione dei Rischi da Interferenze.

e) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.
L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.
I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/processi sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

3. REATI SOCIETARI

a) Aree a rischio

In relazione ai reati societari, le **aree ritenute più specificamente a rischio** sono le seguenti:

1. la predisposizione di comunicazioni dirette ai soci ovvero al pubblico in generale riguardo alla situazione economica, patrimoniale e finanziaria della società, anche nel caso in cui si tratti di comunicazioni diverse dalla documentazione contabile periodica (bilancio d'esercizio, relazioni periodiche etc.);
2. la predisposizione di prospetti informativi;
3. la predisposizione e divulgazione verso l'esterno di dati o notizie relativi alla società;
4. la gestione delle transazioni finanziarie;
5. il ciclo fatturazione attiva e passiva;
6. la gestione dei rapporti con revisori, sindaci e soci;
7. il compimento di operazioni endosocietarie o di significativo rilievo concluse sia con soggetti terzi che con parti correlate.

In linea generale, i **processi aziendali nei quali si presentano attività sensibili** con riferimento ai reati societari, sono i seguenti:

- **Processo di contabilità generale e bilancio**: attività di registrazione, redazione, controllo e conservazione dei documenti contabili ed extracontabili relative, in particolare, a Bilancio e Controllo di gestione;
- **Tesoreria**: attività finanziarie relative a gestione dei flussi finanziari, gestione dei fondi aziendali, impiego di disponibilità liquide;
- **Assegnazione lavori, servizi e forniture**: prestazioni professionali, appalti e subappalti;
- **Gestione interventi di iniziativa della Regione Piemonte e per conto proprio**: partecipazione (quale committente e/o quale soggetto in gara) a gare ed appalti pubblici ed a trattative, costruzione in proprio, attività immobiliari.

L'area critica per la commissione del reato di **"false comunicazioni sociali" di cui all'art. 2621 C.C.** riguarda la tenuta della contabilità e la predisposizione o coinvolgimento nella predisposizione (anche parziale da parte di collaborazione e/o consulenza) di comunicazioni sociali destinate al mercato:

a) bilancio d'esercizio;
b) relazioni infrannuali civilistiche;
c) bilanci pro-forma;
d) budget o piani pluriennali;
e) altre informazioni destinate alla Regione Piemonte ed agli altri enti istituzionali, pubblici o privati, che si trovino ad interloquire con SIT.

Rilevano non solo le parti fondamentali di un bilancio e dei documenti obbligatori (stato patrimoniale, conto economico, nota integrativa e relazione sulla gestione), ma anche ogni documento ad essi sottostante, la cui redazione diventa elemento fondamentale per il documento definitivo. Le procedure dovranno accertare che ogni posta di bilancio sia il risultato dell'applicazione di criteri obiettivi facilmente individuabili e, soprattutto, omogenei per ogni singola operazione ivi riportata.

Occasioni per la commissione del reato potrebbero essere: l'inserimento, variazione o cancellazione dei dati di Contabilità Generale nel sistema informatico (fatturazione attiva/passiva, incassi e pagamenti ad agenti, pagamenti a fornitori e dipendenti, gestione della liquidità e delle operazioni non ordinarie di tesoreria); la stima delle poste estimative/valutative di bilancio; la raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione della bozza di bilancio annuale - societario e consolidato - da sottoporre all'approvazione dell'Amministratore Unico; l'approvazione del progetto di Bilancio d'esercizio e consolidato nonché delle situazioni infrannuali.

Relativamente alla fase di raccolta e preparazione dei dati per la predisposizione del bilancio, le procedure/istruzioni interne dovranno specificare i criteri da seguire per la determinazione delle poste valutative/estimative e di altre poste critiche di bilancio. Il flusso di raccolta dati deve essere strutturato, anche in via preventiva nella fase di aggregazione, con indicazione di responsabilità, tempi e modalità di trasmissione e devono essere altresì evidenti le procedure autorizzative per le deviazioni dalle procedure standard con previsione di oneri di motivazione e documentazione.

Al fine di prevenire il reato di **"impedito controllo" ex art. 2625 C.C.** deve essere mantenuta evidenza documentale di tutte le richieste pervenute e di tutte le informazioni/dati/documenti consegnati o resi disponibili al Sindaco Unico, ai soci e agli organi societari di controllo.
Il reato di cui all'art. 2625 C.C. potrebbe trovare occasione nelle seguenti evenienze:

- in occasione di verifiche periodiche, della revisione del bilancio o nella gestione dei rapporti con il Sindaco Unico;
- nella gestione dei rapporti con i soci in occasione di eventuali richieste di esibizione di libri sociali.

Il reato potrebbe essere compiuto, a titolo esemplificativo, mediante le seguenti condotte:

- occultamento di documenti o messa in atto di altri artifici idonei ad impedire od ostacolare il controllo;
- omissione di informazioni, mancata esibizione della documentazione richiesta dal Sindaco Unico e mancata esibizione ai Soci che facciano richiesta del libro soci.

Al fine di prevenire il reato di **"formazione fittizia del capitale" *ex* art. 2632 C.C.** dovrà essere adottata apposita procedura relativa alla gestione delle operazione straordinarie (conferimenti di beni in natura o di crediti o del patrimonio della società in caso di trasformazione) identificando ruoli, responsabilità, criteri e modalità di realizzazione oltre alla procedura per la gestione di operazioni con parti correlate che regolamenti la sottoscrizione reciproca di azioni e quote.
La procedura dovrà prevedere controlli di merito indipendenti sulle valutazioni contenute nelle relazioni di stima in caso di conferimenti in natura o di crediti, realizzate dalle funzioni competenti.
Occasioni per la commissione del reato possono emergere in casi come questi:

- operazioni di emissione di quote proprie su delega dell'Amministratore Unico;
- operazione di conferimento di beni dei soci su delega dell'Amministratore Unico;
- operazioni di trasformazione della società su delega dell'Amministratore Unico.

Al fine di prevenire il reato di **"illecita influenza sull'Assemblea" ex art. 2636 C.C.**, la Società adotterà adeguati flussi autorizzativi strutturati in materia di predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'assemblea.
Al fine di prevenire la commissione del reato in oggetto, chiunque si trovi nella condizione di non poter o dover esercitare il voto, deve darne comunicazione all'organo di controllo.
Occasione di realizzazione della condotta sono tutte le fasi inerenti all'Assemblea, dalla sua convocazione, al deposito, ove previsto, delle partecipazioni presso la sede della società, all'esercizio del diritto di voto e riguarda, essenzialmente, la predisposizione di progetti, prospetti e documentazione da sottoporre all'assemblea per l'approvazione.
Possibili modalità di realizzazione della condotta sono:

- la simulazione o fraudolenta predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'assemblea;
- l'esecuzione di atti simulati o fraudolenti tali da far convergere la maggioranza assembleare verso tesi precostituite.

b) Norme di condotta

Gli organi di *governance*, di controllo ed i dipendenti sono tenuti ad un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società. In particolare, essi sono tenuti a:

1. 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 ordine a tale punto, è fatto divieto di:

a. tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Sindaco Unico o della società di revisione legale o dei soci;
b. porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

2. Osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo. In ordine a tale punto, è fatto divieto di:

a. restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
b. ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
c. acquistare o sottoscrivere azioni della Società o dell'eventuale società controllante fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;
d. effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
e. procedere in ogni modo a formazione o aumento fittizio del capitale sociale;
f. ripartire i beni sociali tra i soci, in fase di liquidazione, prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;
g. porre in essere operazioni simulate o altrimenti fraudolente, nonché diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

È dunque vietato porre in essere o dare causa (anche con mera collaborazione od apporto concausale, anche omissivo) alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato previsti dall'articolo 25-*ter* del D.Lgs. 231/2001: si ribadisce che è espressamente vietato:

1. Tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
2. Esporre fatti materiali rilevanti non rispondenti al vero o omettere fatti materiali rilevanti la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della società, nei bilanci, nelle relazioni e nelle altre comunicazioni sociali dirette ai soci al pubblico previste dalla legge;
3. Illustrare i dati e le informazioni in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti;
4. Restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
5. Ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
6. Acquistare o sottoscrivere azioni della Società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;

7. Effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
8. Procedere a formazione o aumenti fittizi del capitale sociale;
9. 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 Sindaco Unico e dei soci;
10. 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;
11. Omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle autorità di vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;
12. Esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;
13. Porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
14. Porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio e del Sindaco Unico;
15. Non attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione dei bilanci, della relazione semestrale e trimestrale, nelle procedure amministrativo contabili.

c) Scheda riassuntiva delle norme di condotta

1. Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al socio ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
2. Osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3. 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;
4. L'Amministratore Unico deve dare notizia al Sindaco Unico e all'Organismo di Vigilanza di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata.

d) Scheda riassuntiva dei divieti

1. Rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;

2. Omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;
3. Restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
4. Ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
5. Effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
6. Procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale;
7. Porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio e del Sindaco Unico;
8. Omettere od occultare l'eventuale interesse che, per conto proprio o di terzi, l'Amministratore abbia in una determinata operazione della società;
9. Esporre nelle comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società.

e) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.
L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.
I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/processi sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

4. REATI INFORMATICI E REATI COMMESSI CON VIOLAZIONE DELLE NORME IN MATERIA DI DIRITTO D'AUTORE

a) Aree a rischio

Le attività della Società nelle quali possono essere commessi reati informatici, reati in violazione delle norme in materia di diritto d'autore e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.
La Società ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni del Codice della Privacy, per prevenire e controllare i rischi in tema di tecnologia dell'informazione, a tutela del proprio patrimonio informativo e dei dati personali.
In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio sono le seguenti:

- tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;
- gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica;
- gestione dei flussi informativi elettronici con la pubblica amministrazione;
- utilizzo di software e banche dati;
- gestione dei contenuti del sito Internet.

Posto che i rischi riguardano soprattutto l'area dei dati, è dunque possibile ricondurre alle seguenti categorie gli eventi che possono generare danni che comportano rischi per la sicurezza:
1. eventi cagionati dai dipendenti, che possono consistere in: sottrazione di credenziali di autenticazione, carenza di consapevolezza, disattenzione o incuria, comportamenti sleali o fraudolenti;
2. eventi determinati dall'utilizzo di strumenti: azione di virus informatici, *spamming*, malfunzionamento, indisponibilità o degrado degli strumenti, accessi esterni non autorizzati, intercettazione di informazioni in rete;
3. eventi relativi al contesto fisico-ambientale: ingressi non autorizzati a locali/aree ad accesso ristretto, sottrazione di strumenti contenenti dati, eventi distruttivi, naturali o artificiali nonché dolosi, accidentali o dovuti ad incuria, guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.), errori umani nella gestione della sicurezza fisica.

b) Norme di condotta

Considerato che nella storia di SIT non si ravvisano episodi di coinvolgimenti di dipendenti per i reati informatici commessi nell'interesse della società o a suo vantaggio, si ritiene che in relazione alla modestia del rischio rilevato, possa essere individuata quale efficace e sufficiente misura di prevenzione l'osservanza dei principi e delle disposizioni adottate dal Codice Etico. In ogni caso, nella gestione degli adempimenti necessari al fine di prevenire l'accesso abusivo ad una rete informatica ed in linea generale il c.d. danneggiamento informatico si prevede l'utilizzo di procedure aziendali volte a:

- prevedere l'aggiornamento periodico obbligatorio password dei dipendenti;
- stabilire l'obbligo di mantenere la riservatezza della password;
- prevedere corsi di aggiornamento/formazione sui principali pacchetti informativi in dotazione (in particolare sul corretto utilizzo delle mail), e la distribuzione di un breviario sul corretto utilizzo delle dotazioni informatiche a ciascun dipendente;
- limitare l'accesso internet a siti aziendalmente utili e moralmente leciti;
- inibire l'utilizzo delle e-mail *spamming*;
- creare una struttura di esperti informatici che monitorano l'adempimento alle prescrizioni aziendali in materia di sicurezza informatica e si aggiornino i sistemi di sicurezza alla luce delle nuove forme di "invasione";
- prevedere l'aggiornamento del sistema antivirus/antispamming periodico;
- controllare il regolare aggiornamento del Documento programmatico sulla sicurezza;

- stabilire l'assegnazione nominale di PC aziendali.

SIT pertanto si impegna a:

1. Informare adeguatamente il personale dell'importanza di:
   - Mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
   - Utilizzare correttamente i software e banche dati in dotazione;
   - Non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali;
2. Prevedere attività di formazione e addestramento periodico in favore del personale, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
3. Informare il personale della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
4. Impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
5. Limitare gli accessi alle stanze server unicamente al personale autorizzato;
6. Proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
7. Dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
8. Impedire l'installazione e l'utilizzo di software non approvati dalla società e non correlati con l'attività professionale espletata per la stessa;
9. Informare gli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
10. Limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti ad individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;
11. Impedire l'installazione e l'utilizzo, sui sistemi informatici di SIT, di software mediante i quali sia possibile scambiare file con altri soggetti all'interno del web;
12. Qualora per la connessione alla rete internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a SIT, possano illecitamente collegarsi alla rete internet tramite i router della stessa e compiere illeciti ascrivibili al personale;
13. Limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione;
14. Provvedere alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;
15. Prevedere, nei rapporti contrattuali con i fornitori di servizi software e banche dati sviluppati in relazione a specifiche esigenze aziendali, clausole di manleva volte a tenere indenne la società da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi.

Ai sensi dell'art. 34 del Codice in materia di protezione dei dati personali, SIT ha approvato il Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari, che delinea il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali, aggiornato al 16/01/2017.

c) Divieti

Alla luce di quanto esposto, la Società dispone i seguenti divieti:

1. Connettere ai sistemi informatici di SIT, personal computer, periferiche, altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;

2. Procedere ad installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
3. Modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
4. Acquisire, possedere o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero essere adoperati abusivamente per compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le Credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
5. Ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate da SIT;
6. Divulgare, cedere o condividere con personale interno o esterno a SIT le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
7. Accedere abusivamente ad un sistema informatico altrui ovvero nella disponibilità di altri Dipendenti o terzi, nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
8. Manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
9. Sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
10. Acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
11. Accedere abusivamente al sito internet della Società al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili;
12. Comunicare a persone non autorizzate, interne o esterne a SIT, i controlli sui sistemi informativi e le modalità con cui sono utilizzati;
13. Mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
14. Lo *spamming*;
15. Inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi.
16. Utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, *worm*, *trojan*, *spyware*, *dialer*, *keylogger*, *rootkit*, etc…) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

È anche vietato porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:

1. diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;
2. abusivamente duplicare, detenere o diffondere in qualsiasi forma programmi per elaboratore od opere audiovisive o letterarie;
3. detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;
4. riprodurre banche di dati su supporti non contrassegnati dalla SIAE, diffonderle in qualsiasi forma senza l'autorizzazione del titolare del diritto d'autore o in violazione del divieto imposto dal costitutore;
5. rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;
6. importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.

d) **Flussi informativi all'Organismo di Vigilanza**

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.

L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.

I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.

L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/Processi Sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

5. REATI DI RICICLAGGIO E RICETTAZIONE

a) Aree a rischio

In relazione ai reati di riciclaggio e ricettazione, i processi aziendali nei quali si presentano **attività sensibili** sono i seguenti:

- **processo di approvvigionamento di beni e servizi**: ricerca e selezione dei fornitori, identificazione del fabbisogno e predisposizione della proposta d'acquisizione (Richiesta di Acquisto), eventuali richieste d'offerta a fornitori, analisi delle offerte ricevute e conduzione della trattativa d'acquisto formalizzazione del contratto/lettera di conferimento o emissione e trasmissione degli ordini di acquisto ai fornitori con l'indicazione del Codice Identificativo di Gara (CIG);
- **assegnazione lavori, servizi e forniture**: prestazioni professionali, appalti e subappalti;
- **gestione interventi di iniziativa della Regione Piemonte e per conto proprio**: partecipazione (quale committente e/o quale soggetto in gara) a gare ed appalti pubblici ed a trattative; costruzione in proprio; attività immobiliare;
- **tesoreria**: attività finanziarie relative a Gestione dei flussi finanziari, Gestione dei fondi aziendali, Impiego di disponibilità liquide.

b) Norme di condotta

Le operazioni di natura commerciale, finanziaria e societaria derivanti da rapporti continuativi ed occasionali con terzi diversi dagli Intermediari Finanziari devono essere precedute da un'adeguata attività di verifica volta ad accertare l'assenza del rischio di coinvolgimento nella commissione dei reati di riciclaggio, ricettazione ed impiego di denaro, beni o utilità di provenienza illecita, attraverso una chiara identificazione della controparte; dello scopo, natura e struttura legale-fiscale dell'operazione; del valore complessivo ed unitario degli strumenti utilizzati nell'operazione.
Tutti gli incassi e i pagamenti derivanti da rapporti di collaborazione con terzi fornitori, di acquisto o vendita di partecipazioni, di finanziamento a controllate e collegate ed altri rapporti intercompany, aumenti di capitale, incasso dividendi, ecc. sono regolati esclusivamente attraverso il canale bancario, idoneo ad assicurare sicurezza, tracciabilità ed efficienza nelle operazioni di trasferimento di denaro tra operatori economici.
Tutta la documentazione relativa alle operazioni in oggetto devono essere archiviate e conservate dalle funzioni aziendali competenti.

c) Divieti

È vietato effettuare le seguenti operazioni:

- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare conti aperti presso filiali in Paesi esteri ove ciò non sia correlato alla sottostante attività economica/commerciale;
- creare fondi a fronte di pagamenti non giustificati;
- detenere/trasferire denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera per importi, anche frazionati, complessivamente pari o superiori al limite stabilito dalla normativa vigente;
- accettare assegni emessi da soggetti che non sono i reali debitori nei confronti della Società;
- emettere assegni bancari e postali per importi pari o superiori al limite stabilito dalla normativa vigente che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare pagamenti non adeguatamente documentati e autorizzati;
- effettuare pagamenti in contanti, eccetto per le particolari tipologie di acquisto rientranti nella piccola cassa e comunque per importi limitati;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a funzionari della Pubblica Amministrazione a titolo personale, con la finalità di promuovere o favorire interessi della Società o di società controllate, anche a seguito di illecite pressioni;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione in relazione al tipo di incarico svolto;

- accettare pagamenti frazionati se non supportati da accordi commerciali (quali anticipo e saldo alla consegna e pagamenti rateizzati);
- ricevere incassi, trasferimenti di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore al limite stabilito dalla normativa vigente;
- inserire nuovamente nel circuito monetario, banconote o monete evidentemente falsificate, o anche semplicemente sospette di falsità. Tali banconote devono essere trattenute e consegnate ad un istituto di credito.

d) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.
L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.
I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/Processi Sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

6. REATI AMBIENTALI

a) Aree a rischio

In relazione ai reati ambientali, i processi aziendali nei quali si presentano attività sensibili sono i seguenti:

- **assegnazione lavori, servizi e forniture**: affidamento delle attività di raccolta, trasporto, recupero e smaltimento rifiuti;
- **gestione beni immobili**: errato smaltimento di rifiuti pericolosi e non pericolosi; scarichi di acque reflue industriali senza autorizzazione, mancata bonifica del suolo, sottosuolo, acque superficiali o sotterranee.

b) Norme di condotta

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai reati ambientali di cui all'art. 25-*undecies* del D.Lgs. 231/2001. In particolare, ai Destinatari è richiesto di:

1. definire i principali adempimenti da adottare in merito alla gestione delle diverse tipologie di rifiuti, pericolosi e non pericolosi;
2. affidare le attività di raccolta, trasporto, recupero e smaltimento rifiuti esclusivamente ad imprese autorizzate e nel rispetto delle procedure aziendali relative alla qualificazione dei fornitori;
3. verificare che i fornitori di servizi connessi alla gestione dei rifiuti, ove richiesto dal D.Lgs. 152/2006 e dalle ulteriori fonti normative e regolamentari, dichiarino e diano, in ogni caso, evidenza, in base alla natura del servizio prestato, del rispetto della disciplina in materia di gestione dei rifiuti e di tutela dell'ambiente;
4. accertare, prima dell'instaurazione del rapporto, la rispettabilità e l'affidabilità dei fornitori di servizi connessi alla gestione dei rifiuti, anche attraverso l'acquisizione e la verifica delle comunicazioni, certificazioni e autorizzazioni in materia ambientale da questi effettuate o acquisite a norma di legge, astenendosi dall'avviare rapporti con i fornitori che non offrano garanzie di onorabilità e serietà professionale;
5. inserire nei contratti stipulati con i fornitori di servizi connessi alla gestione dei rifiuti specifiche clausole attraverso le quali i fornitori si impegnino nei confronti della Società a mantenere valide ed efficaci per l'intera durata del rapporto contrattuale le autorizzazioni prescritte dalla normativa per lo svolgimento dell'attività di gestione dei rifiuti;
6. con specifico riguardo all'apertura di nuovi cantieri, prevedere ed adottare le misure cautelative a tutela dell'ambiente e verificare le prescrizioni formulate dall'autorità che ha concesso l'autorizzazione all'apertura del cantiere.
7. aggiornare periodicamente l'archivio delle autorizzazioni, iscrizioni e comunicazioni acquisite dai fornitori terzi;
8. astenersi dall'intrattenere rapporti con gestori di rifiuti che, sulla base di notizie acquisite possano non dare garanzia di serietà nella conduzione degli affari.

c) Divieti

È fatto espresso divieto ai Destinatari, di:

- abbandonare o depositare in modo incontrollato i rifiuti ed immetterli, allo stato solido o liquido, nelle acque superficiali e sotterranee, in violazione delle procedure aziendali;
- violare gli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la gestione dei rifiuti;
- effettuare o predisporre attività organizzate per il traffico illecito di rifiuti;
- falsificare o alterare il certificato di analisi dei rifiuti, anche utilizzato nell'ambito del SISTRI – Area Movimentazione;
- falsificare o alterare qualsiasi documento da sottoporre a Pubbliche Amministrazioni o Autorità di controllo ovvero omettere di comunicare tempestivamente informazioni o dati su fatti o circostanze che possano compromettere la salute pubblica.

d) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.
L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.
I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/Processi Sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

7. REATI DI CRIMINALITÀ ORGANIZZATA

a) Aree a rischio

In relazione ai reati connessi alla criminalità organizzata, le aree ritenute più specificamente a rischio sono le seguenti:

1. **La gestione del personale**: il fatto di favorire l'assunzione di persone appartenenti ad organizzazioni criminali potrebbe integrare la partecipazione in attività delittuose da parte della Società, con conseguente commissione del reato di associazione per delinquere (anche a titolo di concorso);
2. **L'assegnazione lavori, servizi e forniture**: la collaborazione, da parte della Società, con un fornitore di beni o servizi di dubbia moralità che eserciti la sua attività con modalità illecite potrebbe integrare un delitto di criminalità organizzata, tipicamente associazione per delinquere; ovvero associazione per delinquere finalizzata all'evasione fiscale nel caso in cui, ad esempio, il rapporto con un fornitore sia veicolo per la emissione/utilizzazione di fatture per operazioni inesistenti ovvero per la commissione di altre attività illecite;
3. **La gestione interventi di iniziativa della Regione Piemonte e per conto proprio**:

- associazione per delinquere, anche transnazionale, nel caso in cui, ad esempio in fase di *signing* dei contratti e *closing* dell'investimento o del disinvestimento, o non effettuando un adeguato monitoraggio periodico sull'investimento, la Società partecipi ad una associazione criminosa formata da tre o più persone (anche giuridiche e con caratteristiche transnazionali) finalizzata, ad esempio, al riciclaggio di denaro di provenienza illecita o frode fiscale;
- delitti di criminalità organizzata, tipicamente associazione a delinquere, nel caso in cui la Società collabori con un fornitore di beni o servizi di dubbia moralità che eserciti la sua attività con modalità illecite; oppure associazione a delinquere finalizzata all'evasione fiscale nel caso in cui, ad esempio, il rapporto con un fornitore sia veicolo per la emissione/utilizzazione di fatture per operazioni inesistenti ovvero per la commissione di altre attività illecite;

4. **La tesoreria**: associazione a delinquere finalizzata all'evasione fiscale con l'eventuale coinvolgimento di fornitori di beni/servizi, al fine di portare vantaggi di natura economica o d'immagine alla Società.

b) Norme di condotta e divieti

La Società si impegna ad utilizzare costantemente criteri di selezione del personale per garantire che la scelta venga effettuata in modo trasparente, sulla base dei seguenti criteri:

- professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
- parità di trattamento;
- affidabilità rispetto al rischio di infiltrazione criminale.

Nella scelta dei fornitori e delle controparti contrattuali e nella gestione del rapporto contrattuale, la Società si impegna ad attuare le procedure aziendali volte a garantire che il processo di selezione avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri.

Tutti i Destinatari del Modello hanno il divieto di sottostare a richieste di qualsiasi tipo contrarie alla legge e di darne comunque informativa all'Amministratore Unico e/o all'Organo di Vigilanza, oltre che all'autorità di pubblica sicurezza con le denunce del caso.

Tutti i Destinatari del Modello hanno l'obbligo di segnalare all'Amministratore Unico e/o all'Organo di Vigilanza, qualsiasi elemento da cui possa desumersi il pericolo di interferenze criminali in relazione all'attività d'impresa e la Società si impegna a tal riguardo a garantire la riservatezza a coloro che adempiano ai suddetti obblighi di segnalazione o denuncia con un pieno supporto, anche in termini di eventuale assistenza legale.

Nella predisposizione e successiva tenuta delle scritture contabili rilevanti ai fini tributari, la Società pone in essere una serie di misure idonee ad assicurare che i Destinatari del Modello nell'ambito delle rispettive competenze:

- non emettano fatture o rilascino altri documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- custodiscano in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento.

La Società, anche attraverso la predisposizione di specifiche procedure, si impegna a garantire l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione nelle dichiarazioni tributarie.

c) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.
L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.
I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/Processi Sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

8. REATI DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

a) Premessa

I reati di terrorismo o eversione dell'ordine democratico sono stati valutati, nell'ambito delle attività della Società, a basso rischio di commissione.

b) Norme di condotta

Con riferimento ai reati di terrorismo, i Destinatari del Modello debbono osservare i seguenti obblighi e divieti:

- qualunque transazione finanziaria deve presupporre la conoscenza del beneficiario;
- 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 (ad es. presenza nelle Liste; referenze personali; ecc.);
- nel caso in cui alla Società vengano proposte operazioni anomale, l'operazione viene sospesa e valutata preventivamente dall'Organo Gestorio, e, se del caso, con l'ausilio dell'Organismo di Vigilanza;
- nei contratti deve essere contenuta apposita dichiarazione, secondo lo schema previsto dalle procedure aziendali e/o dalle indicazioni dell'Organismo di Vigilanza, da cui risulti che le parti si danno pienamente atto del reciproco impegno ad improntare i comportamenti finalizzati all'attuazione dell'iniziativa comune a principi di trasparenza e correttezza e nella più stretta osservanza delle disposizioni di legge;
- i dati raccolti relativamente ai rapporti con clienti, fornitori e partner esterni devono essere completi e aggiornati, sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del loro profilo.

c) Divieti

- Porre in essere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate dall'art. 25 *quater* del D.Lgs. 231/2001;
- Utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei reati di cui sopra;
- Promuovere, costituire, organizzare o dirigere associazioni che si propongono il compimento di atti di violenza in particolar modo con fini di eversione dell'ordine democratico;
- Fornire, direttamente o indirettamente, fondi a favore di soggetti che intendano porre in essere reati di terrorismo;
- Assumere o assegnare commesse o effettuare qualsivoglia operazione commerciale e/o finanziaria, sia in via diretta, che per il tramite di interposta persona, con soggetti - persone fisiche o persone giuridiche - i cui nominativi siano contenuti nelle liste nominative di soggetti collegati al terrorismo internazionale (liste pubblicate sui siti web dell'ufficio Italiano dei Cambi e del Ministero degli Interni) o controllati da soggetti contenuti nelle Liste medesime quando tale rapporto di controllo sia noto;
- Effettuare operazioni, assumere o assegnare commesse che possano presentare carattere anomalo per tipologia o oggetto e instaurare o mantenere rapporti che presentino profili di anomalia dal punto di vista dell'affidabilità e reputazione dei soggetti e delle operazioni da concludere;
- Effettuare prestazioni in favore dei Collaboratori Esterni che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- Riconoscere compensi in favore dei Collaboratori Esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.

d) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzato seguito.

L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.
I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/processi sensibili affinché questo provveda ad adeguare conseguentemente il Modello.

9. REATI TRIBUTARI

a) Aree a rischio

In relazione ai reati tributari, i processi aziendali nei quali si presentano attività sensibili sono i seguenti:

- emissione di fatture attive;
- ricezione di fatture passive;
- redazione e presentazione delle dichiarazioni sui redditi o sul valore aggiunto.

b) Norme di condotta

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" con riferimento ai reati societari di cui all'art. 25-*quinquiesdecies* del D.Lgs. 231/2001. In particolare, ai Destinatari è richiesto di:

1. definire un elenco di procedure specifiche cui i destinatari del modello devono attenersi nella registrazione della documentazione contabile nonché nella corretta conservazione delle scritture obbligatorie per legge;
2. Fornire all'ODV ed ai Responsabili interni chiamati a cooperare con lo stesso, gli strumenti operativi per un adeguato ed efficace controllo e monitoraggio;
3. definire ruoli e responsabilità nella gestione delle attività contabili.

c) Divieti

È fatto espresso divieto ai Destinatari, di:

- tenere comportamenti tali che integrino, direttamente o indirettamente, le fattispecie di reato previste dall'articolo 25 quinquiesdecies del D. lgs. 231/2001;
- tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra indicate, possano potenzialmente diventarlo;
- emmettere fatture ovvero registrare fatture senza che siano rispettate le specifiche procedure interne;
- tenere la documentazione contabile in modo da impedirne la ricostruzione;
- porre in essere comportamenti che impediscano o comunque ostacolino lo svolgimento dell'attività di controllo e da parte del sindaco Unico e dei soci.

d) Flussi informativi all'Organismo di Vigilanza

Le Funzioni aziendali coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.
L'Organismo di Vigilanza potrà richiedere, alle Funzioni a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.

I Responsabili delle Funzioni coinvolti nell'ambito del processo garantiranno, coordinando le strutture di propria competenza, la documentabilità dell'intero processo comprovante il rispetto della normativa, tenendo a disposizione dell'Organismo di Vigilanza tutta la documentazione all'uopo necessaria.
L'OdV ha il compito inoltre di proporre all'Amministratore Unico eventuali modifiche e/o integrazioni delle suddette aree di attività/Processi Sensibili affinché questo provveda ad adeguare conseguentemente il Modello.