



RO.S.S. - Road Safety Services S.r.l.

Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001

Approvato dal Consiglio di Amministrazione del 29.07.2024

Documento:	Modello di organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001			
File:	MOG231 Parte Generale			
Versione:	1	Prima versione del documento	Verifica dell'OdV del:	05.03.24
			Approvazione CdA del:	14.03.24
Versione:	2	Aggiornamento del documento	Verifica dell'OdV del:	23.07.24
			Approvazione CdA del:	29.07.24

INDICE

<i>PARTE GENERALE</i>	3
1. IL DECRETO LEGISLATIVO N. 231/2001	4
2. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO	9
3. MAPPA DELLE ATTIVITA' AZIENDALI "SENSIBILI"	11
4. DEFINIZIONE DELLE PARTI SPECIALI DEL MODELLO	12
5. ORGANISMO DI VIGILANZA	15
6. FORMAZIONE ED INFORMATIVA A SOGGETTI TERZI	20
7. SISTEMA DISCIPLINARE E SANZIONATORIO	20
<i>PARTI SPECIALI</i>	28
PARTE SPECIALE A: GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE	29
PARTE SPECIALE B: GESTIONE DELLE ATTIVITÀ AMMINISTRATIVE	41
PARTE SPECIALE C: SELEZIONE E GESTIONE DEL PERSONALE	60
PARTE SPECIALE D: GESTIONE DEGLI ACQUISTI DI BENI, SERVIZI E INCARICHI PROFESSIONALI	71
PARTE SPECIALE E: GESTIONE DELLE COMMESSE	79
PARTE SPECIALE F: GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI, DI TERZI E DELLA P.A.	91
PARTE SPECIALE G: GESTIONE DEGLI ADEMPIMENTI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO	100
PARTE SPECIALE H: GESTIONE DEGLI ADEMPIMENTI IN MATERIA AMBIENTALE	113
PARTE SPECIALE I: GESTIONE DEGLI ADEMPIMENTI RELATIVI AL PROCESSO FREE-FLOW	119
<i>FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA</i>	124

1. SCOPO.....	125
2. FLUSSI INFORMATIVI PERIODICI.....	125

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001

1.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche

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

Il Decreto, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa a carico degli enti (da intendersi come società, associazioni, consorzi, ecc., di seguito denominati "Enti") per reati tassativamente elencati e commessi nel loro interesse o vantaggio: (i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi, ovvero (ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. La responsabilità dell'Ente si aggiunge a quella (penale e civile) della persona fisica, che ha commesso materialmente il reato.

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

1.2 Fattispecie di reato previste dal Decreto

Il Decreto riguarda alcune particolari fattispecie di illecito penale, esplicitamente richiamate dal Decreto medesimo.

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

- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24¹);
- Delitti informatici e trattamento illecito di dati (art. 24-*bis*);
- Delitti di criminalità organizzata (art. 24-*ter*);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25²);
- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis*);
- Delitti contro l'industria e il commercio (art. 25-*bis*1);
- Reati societari (art. 25-*ter*)³;
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater*);
- Pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*1);
- Delitti contro la personalità individuale (art. 25-*quinqies*);
- Abusi di mercato (art. 25-*sexies*);
- Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies*);
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies*)⁴;
- Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies*.1)⁵;
- Delitti in materia di violazione del diritto d'autore (art. 25-*novies*);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies*);

¹ Articolo modificato dal D. Lgs. 75/2020 che ha dato attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (c.d. Direttiva PIF) e dal D.L. 10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023, che ha introdotto le fattispecie di reato previste dagli artt. 353 c.p. "*Turbata libertà degli incanti*" e 353-bis c.p. "*Turbata libertà del procedimento di scelta del contraente*".

² Articolo modificato dal D. Lgs. 75/2020 che ha dato attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (c.d. Direttiva PIF)

³ Articolo modificato dal D.lgs. n. 19 del 2 marzo 2023, (il "Decreto") recante "*Attuazione della direttiva (UE) 2019/2121 del Parlamento europeo e del Consiglio, del 27 novembre 2019, che modifica la direttiva (UE) 2017/1132 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere*" che ha introdotto nell'art. 25-*ter* "*Reati societari*" il delitto di "*false o omesse dichiarazioni per il rilascio del certificato preliminare*".

⁴ Le condotte tipiche dei reati ivi richiamati sono state modificate dal D.Lgs. 8 novembre 2021, n. 195 recante attuazione della direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale.

⁵ Articolo inserito dal D. Lgs. n. 184 recante "*Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio*". Il presente articolo è stato modificato dal D.L. 10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023, che ha introdotto la fattispecie di reato prevista dall'art. 512-bis c.p. "*Trasferimento fraudolento di valori*", che è stato successivamente modificata dal D.L. 19/2024, che ha introdotto un secondo comma all'art. 512 bis c.p.

- Reati ambientali (art. 25-*undecies*);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies*);
- Razzismo e xenofobia (art. 25-*terdecies*);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies*);
- Reati tributari (art. 25-*quinqüesdecies*);
- Contrabbando (art. 25-*sexiesdecies*)⁶;
- Delitti contro il patrimonio culturale (art. 25-*septiesdecies*)⁷;
- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies*)⁸.

Si rinvia all'Allegato I *"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"* per una descrizione di dettaglio dei reati elencati nel Decreto e nelle successive modificazioni e integrazioni.

1.3 Sanzioni previste dal Decreto

Qualora se ne ravveda la responsabilità ai sensi del Decreto, in conseguenza della commissione o tentata commissione dei reati sopra menzionati, a carico della società sono previste le seguenti sanzioni:

- sanzione pecuniaria, calcolata tramite un sistema basato su quote, che vengono determinate dal giudice nel numero e nell'ammontare, entro limiti definiti per legge;
- sanzioni interdittive che, a loro volta, possono consistere in:
 - interdizione dall'esercizio dell'attività;
 - sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
 - divieto di contrattare con la pubblica amministrazione;
 - esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi;
 - divieto di pubblicizzare beni o servizi;
- confisca del prezzo o del profitto del reato;
- pubblicazione della sentenza in uno o più giornali.

⁶ Articolo inserito dal D. Lgs. 75/2020 che ha dato attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (c.d. Direttiva PIF).

⁷ Articolo inserito dalla L. 9 marzo 2022, n. 22 "Disposizioni in materia di reati contro il patrimonio culturale".

⁸ Articolo inserito dalla L. 9 marzo 2022, n. 22 "Disposizioni in materia di reati contro il patrimonio culturale".

1.4 L'adozione dei modelli di organizzazione, gestione e controllo quali esimenti della responsabilità amministrativa dell'Ente

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

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

Detti modelli di organizzazione, gestione e controllo (di seguito denominati anche “Modelli”), devono rispondere alle seguenti esigenze:

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

Ove il reato venga commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che:

- (i) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- (ii) il compito di vigilare sul funzionamento e l'osservanza dei Modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo;
- (iii) i soggetti hanno commesso il reato eludendo fraudolentemente i Modelli;
- (iv) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo in ordine ai Modelli.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato,

abbia adottato ed efficacemente attuato Modelli idonei a prevenire reati della specie di quello verificatosi, secondo una valutazione che deve necessariamente essere *a priori*.

1.5 Il Decreto Legislativo n. 24/2023 ha recepito la Direttiva UE 2019/1937 in materia di «Protezione degli individui che segnalano violazioni delle norme comunitarie».

In materia di segnalazioni whistleblowing, il recente Decreto Legislativo n. 24/2023 – che recepisce la Direttiva UE 2019/1937 in materia di «Protezione degli individui che segnalano violazioni delle norme comunitarie – contribuisce a far progredire la cultura della legalità della compliance nei contesti organizzativi recependo, all'interno della disciplina nazionale del whistleblowing, le indicazioni emanate dalle istituzioni europee e le best practices internazionali.

Tale disposto normativo ha previsto l'obbligo per la Società di prevedere dei canali che consentano la segnalazione di illeciti aventi ad oggetto violazioni di disposizioni normative nazionali e/o europee, che ledono gli interessi e/o l'integrità dell'organizzazione di appartenenza, garantendo la massima riservatezza in merito all'identità del segnalante.

Tutti i dipendenti della Società o terze parti connesse ad essa che vengono a conoscenza di condotte illecite, rilevanti ai sensi del D. Lgs. 24/2023, in ragione delle funzioni svolte, devono quindi tempestivamente segnalare tali comportamenti mediante diversi canali di comunicazione.

In considerazione di quanto sopra indicato, la Società implementa un sistema di gestione delle segnalazioni (*Whistleblowing*) che prevede l'utilizzo di canali di segnalazione in forma scritta e orale al fine di garantire la massima tutela e riservatezza sia delle persone segnalanti che dell'oggetto delle segnalazioni.

In particolare, le segnalazioni inerenti a RO.S.S. potranno essere inviate attraverso:

- in forma scritta o orale tramite la Piattaforma Digitale accessibile all'indirizzo <http://roadsafetyservices.integrityline.app>
- mediante posta ordinaria o raccomandata, riservata e personale, indirizzata al Ricevente, all'indirizzo di RO.S.S. Srl – via San Giuliano 2/a – 10059 Susa (TO);
- in forma orale, tramite incontro con il Ricevente.

La Società non tollera alcuna conseguenza pregiudizievole nei confronti del segnalante in ambito disciplinare, tutelandolo in caso di adozione di «misure discriminatorie, dirette o indirette, aventi effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia». La predetta tutela non trova, quindi, applicazione nei casi in cui la segnalazione riporti informazioni false rese con dolo o colpa grave.

Per il dettaglio delle modalità operative di gestione delle segnalazioni si rimanda alla Procedura Interfunzionale sulla Gestione delle Segnalazioni (Whistleblowing) – PGS 040.

2. ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

2.1 Adozione e approvazione del Modello

L'adozione, efficace attuazione e successive modifiche e integrazioni del Modello costituiscono atti di competenza del Consiglio di Amministrazione. È pertanto rimessa a tale organo amministrativo la responsabilità di approvare e recepire, mediante apposita delibera, anche i principi cardine enunciati nel presente documento, che costituiscono parte integrante.

La Società, sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri azionisti e del lavoro dei propri dipendenti, ha deciso di avviare un progetto di analisi ed adeguamento dei propri strumenti organizzativi, di gestione e di controllo alle esigenze espresse dal Decreto che si è concluso con l'adozione del Modello di Organizzazione Gestione e Controllo in data 16.03.2021.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello di gestione e controllo (di seguito anche il "Modello") allineato alle prescrizioni del Decreto possa costituire sia un valido strumento di sensibilizzazione di tutti coloro che operano per conto di RO.S.S., affinché tengano comportamenti corretti e lineari nell'espletamento delle proprie attività, sia un imprescindibile mezzo di prevenzione contro il rischio di commissione dei reati previsti dal Decreto stesso. In particolare, attraverso l'adozione del Modello, il Consiglio d'Amministrazione si propone di perseguire le seguenti principali finalità:

- determinare, in tutti coloro che operano per conto di RO.S.S. nell'ambito di attività aziendali sensibili, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in conseguenze disciplinari e/o contrattuali oltre che in sanzioni penali e amministrative comminabili nei loro stessi confronti;
- ribadire che tali forme di comportamento illecito sono fortemente condannate, in quanto le stesse sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali RO.S.S. intende attenersi nell'esercizio dell'attività aziendale;
- consentire a RO.S.S., grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello.

2.2 Destinatari del Modello

Il presente Modello è indirizzato a tutto il personale apicale e sottoposto della Società, in particolare, a quanti svolgano attività aziendali "sensibili". Le prescrizioni del presente Modello devono pertanto essere rispettate sia dal personale che svolge funzioni di rappresentanza, di amministrazione, di direzione e controllo, anche di fatto, (c.d. "apicali"), sia da tutti i lavoratori sottoposti a qualsiasi titolo alla direzione o alla vigilanza degli stessi, ossia tutti coloro che operano in nome o per conto della Società (c.d. "sottoposti").

La Società richiede, tramite la previsione di apposite clausole contrattuali, ai consulenti,

collaboratori, fornitori e partner il rispetto delle prescrizioni dettate dal Decreto e dei principi etici adottati, attraverso la documentata presa visione del Codice Etico della Società.

L'insieme dei Destinatari così definiti è tenuto a rispettare, con la massima diligenza, le disposizioni contenute nel Modello e nei suoi protocolli di attuazione.

2.3 Gli elementi qualificanti del Modello

Con riferimento alle tematiche individuate dal legislatore, gli elementi qualificanti del Modello di Organizzazione, Gestione e Controllo possono essere così brevemente riassunti:

- mappatura dettagliata delle attività aziendali “sensibili” intendendosi per tali le attività nell’ambito delle quali, per loro natura, possono essere potenzialmente commessi i reati di cui al Decreto e pertanto da sottoporre ad analisi e monitoraggio;
- definizione di meccanismo di controllo atti a garantire:
 - la separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
 - la chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell’ambito della struttura organizzativa;
 - l’esistenza di regole etico-comportamentali idonee a garantire l’esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell’integrità del patrimonio aziendale;
 - un adeguato livello di regolamentazione dei processi aziendali, attraverso la definizione di parti speciali / procedure che regolamentino le modalità e tempistiche di svolgimento delle attività;
 - la protezione del patrimonio e il corretto utilizzo di tutte le risorse, in particolare di quelle finanziarie;
- definizione di un insieme di regole di condotta alle quali i destinatari devono uniformarsi, finalizzate ad impedire il verificarsi di comportamenti illeciti o non allineati agli standard aziendali (c.d. “Codice Etico”);
- identificazione dell’Organismo di Vigilanza (di seguito anche “Organismo”) e attribuzione allo stesso di specifici compiti di vigilanza sull’efficace e corretto funzionamento del Modello;
- definizione dei flussi informativi nei confronti dell’Organismo;
- definizione delle attività di informazione, sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e dei presidi di controllo istituiti;
- definizione e applicazione di disposizioni disciplinari idonee a sanzionare il mancato

rispetto delle misure indicate nel Modello;

- definizione delle responsabilità relativamente al recepimento, all'integrazione ed all'implementazione del Modello con conseguente verifica del funzionamento dei medesimi nonché del loro periodico aggiornamento.

2.4 Aggiornamento del Modello

Il Consiglio di Amministrazione delibera in merito all'aggiornamento del Modello e al suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza, ad esempio di:

- cambiamenti significativi della struttura organizzativa o dell'operatività dell'Ente;
- significative violazioni del Modello e/o esiti di verifiche sull'efficacia del medesimo o di esperienze di pubblico dominio del settore;
- specifici eventi (es. ampliamento del novero dei reati, richieste del Consiglio di Amministrazione, etc.) che richiedano l'estensione dell'ambito di applicazione del Modello a nuove fattispecie di rischio.

Il Modello sarà sottoposto, da parte del Consiglio di Amministrazione e dell'Organismo di Vigilanza ad un procedimento di analisi periodica, al fine di garantire la continuità dinamica delle funzioni che gli sono proprie in relazione all'evoluzione delle esigenze emerse.

In ogni caso, eventuali accadimenti che rendano necessaria la modifica o l'aggiornamento del Modello devono essere segnalati in forma scritta dall'Organismo di Vigilanza al Consiglio di Amministrazione, affinché lo stesso possa effettuare le delibere di propria competenza.

Le modifiche dei principi di comportamento e controllo necessari per l'attuazione del Modello avvengono ad opera delle strutture dell'Ente. L'Organismo di Vigilanza è costantemente informato in merito alle attività di aggiornamento ed ha facoltà di esprimere il proprio parere sulle proposte di modifica.

3. MAPPA DELLE ATTIVITA' AZIENDALI "SENSIBILI"

Ai fini della definizione del Modello Organizzativo, sono state individuate, le attività e i processi nel cui ambito potrebbero potenzialmente configurarsi le condizioni e le occasioni per la commissione dei reati previsti dal Decreto (c.d. "attività sensibili").

Le risultanze dell'attività di analisi svolta sono illustrate nel documento di "*Risk Assessment*".

Con specifico riferimento ai reati commessi con violazione delle norme antinfortunistiche e tutela dell'igiene e della salute sul lavoro è stata effettuata un'analisi volta a valutare il sistema di gestione del rischio, già implementato dalla Società sulla base della normativa di riferimento, mediante lo svolgimento di interviste ai Responsabili del Servizio di Prevenzione e Protezione nonché attraverso l'analisi della documentazione inerente alle misure organizzativo/procedurali caratterizzanti il sistema di gestione della sicurezza. Anche con

riferimento ai reati in materia ambientale, è stata svolta un'analisi dedicata. Le risultanze di entrambe le attività di analisi sono descritte nel documento *“Rapporto di ‘Assessment di salute e sicurezza sul lavoro e ambientale’ finalizzato all'adozione del Modello Organizzativo ex D.Lgs. 231/2001”*.

4. DEFINIZIONE DELLE PARTI SPECIALI DEL MODELLO

4.1 Parti Speciali

Al fine di prevenire le fattispecie di rischio-reato rilevate in fase di mappatura delle attività aziendali “sensibili”, RO.S.S. ha individuato i processi “strumentali” alla realizzazione dei reati, ovvero quei processi nel cui ambito, potenzialmente, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione di reati.

Con riferimento ai processi “strumentali” identificati, la Società ha definito e formalizzato, a garanzia della trasparenza delle scelte effettuate e decisioni assunte, delle “Parti Speciali” contenente le seguenti sezioni:

Attività sensibili	Riferimento Parte Speciale	Principali rischi-reato
<ol style="list-style-type: none"> 1. Gestione degli adempimenti verso la Pubblica Amministrazione; 2. Gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza in occasione di visite ispettive 3. Accesso e gestione dei finanziamenti pubblici 4. Gestione del contenzioso 	<p>A - Gestione dei rapporti con la Pubblica Amministrazione</p>	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati Societari - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria -
<ol style="list-style-type: none"> 5. Tenuta della contabilità e predisposizione del bilancio d'esercizio 6. Gestione degli adempimenti fiscali 7. Gestione dei rapporti infragruppo 8. Gestione dei rapporti con il Sindaco Unico e la Società di Revisione 9. Gestione della finanza e della tesoreria 10. Gestione delle operazioni societarie straordinarie 11. Gestione delle locazioni passive 12. Gestione del trattamento delle informazioni riservate 13. Gestione di omaggi e liberalità 	<p>B - Gestione delle Attività Amministrative</p>	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati societari - Reati di illeciti amministrativi di abuso di mercato - Delitti di criminalità organizzata - Reati di ricettazione, riciclaggio, impiego di denaro, beni, utilità di provenienza illecita, nonché autoriciclaggio - Delitti in materia di strumenti di pagamento diversi dai contanti - Reati monetari - Reati di terrorismo - Reati Tributari

Attività sensibili	Riferimento Parte Speciale	Principali rischi-reato
14. Selezione e assunzione del personale 15. Gestione dei rapporti con le Organizzazioni Sindacali 16. Gestione di livelli retributivi, avanzamenti di carriera, riconoscimenti <i>ad personam</i> 17. Assegnazione e gestione dei beni aziendali 18. Elaborazione delle paghe e dei contributi 19. Gestione dei rimborsi spese e delle spese di rappresentanza 20. Predisposizione e trasmissione della documentazione necessaria per l'ottenimento di finanziamenti pubblici / contributi agevolati per la realizzazione di corsi di formazione 21.	C - Selezione e Gestione del Personale	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati societari - Reati di ricettazione, riciclaggio, impiego di beni, denaro e altra utilità di provenienza illecita, autoriciclaggio - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare - Reati di criminalità organizzata - Reati di terrorismo - Reati Tributari - Delitti contro la personalità individuale
22. Gestione degli acquisti di beni, servizi e incarichi professionali	D - Gestione degli Acquisti di beni, servizi e incarichi professionali	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati Societari - Reati di criminalità organizzata - Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio - Reati Tributari - Reati di terrorismo
23. Gestione delle richieste di offerta e partecipazione a gare 24. Gestione delle commesse 25. Gestione dei rapporti con il Committente nell'ambito della gestione delle commesse, anche in occasione di visite ispettive	E - Gestione delle commesse	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati Societari - Reati di terrorismo - Reati di criminalità organizzata - Reati contro la personalità individuale - Reati in materia di immigrazione clandestina - Delitti in materia di strumenti di pagamento diversi dai contanti; - Reati Tributari - Reati contro il patrimonio culturale - Reati in materia di igiene e sicurezza sui luoghi di lavoro - Reati in materia ambientale

Attività sensibili	Riferimento Parte Speciale	Principali rischi-reato
26. Gestione dei sistemi informativi aziendali, di terzi e della Pubblica Amministrazione 27. Gestione delle licenze d'uso per applicazioni software	<i>F - Gestione dei Sistemi informativi Aziendali</i>	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati informatici e trattamento illecito dei dati - Reati in materia di violazione del diritto d'autore - Reati contro la personalità individuale - Delitti in materia di strumenti di pagamento diversi dai contanti - Reati Tributari
28. Gestione degli adempimenti in materia di Salute e Sicurezza sui luoghi di lavoro	<i>G - Gestione degli adempimenti in materia di Salute e Sicurezza nei Luoghi di Lavoro</i>	<ul style="list-style-type: none"> - Reati di omicidio colposo e lesioni colpose gravi e gravissime
29. Gestione degli adempimenti in materia ambientale	<i>H - Gestione degli adempimenti in materia ambientale</i>	<ul style="list-style-type: none"> - Reati ambientali
30. Gestione del Free-Flow	<i>I – Gestione adempimenti relativi al processo Free-Flow</i>	<ul style="list-style-type: none"> - Reati contro la Pubblica Amministrazione - Reati societari - Reati informatici e trattamento illecito dei dati

4.2 Sistema di deleghe e procure

Il sistema di attribuzione dei poteri e delle responsabilità che sovrintende l'intera struttura organizzativa si articola sui seguenti elementi:

- organigramma aziendale;
- procure;
- ordini di servizio.

La Società dispone di un organigramma nel quale sono riportate funzioni, compiti, responsabilità ed autorità delle varie direzioni ed uffici facenti parte dell'organizzazione aziendale.

Il Presidente e l'Amministratore Delegato esercitano i poteri loro conferiti dal Consiglio di Amministrazione nel rispetto delle previsioni e dei limiti di legge e dello Statuto.

Procure speciali regolamentano e disciplinano le funzioni e gli ambiti operativi dei singoli Direttori responsabili delle varie aree aziendali.

4.3 Principi etici

La Società ha definito i principi etici cui intende uniformare la propria attività anche in relazione ai comportamenti che possono integrare le fattispecie di reato previste dal Decreto ed ha adottato il “Codice Etico e di Comportamento”⁹.

Tali principi sottolineano la necessità di:

- rispettare le leggi, le normative vigenti e i regolamenti interni;
- improntare lo svolgimento delle prestazioni professionali da parte dei dipendenti e dei collaboratori della Società a criteri di diligenza, competenza, professionalità, efficienza ed imparzialità;
- improntare a principi di correttezza e trasparenza i rapporti con la Pubblica Amministrazione.

I principi ispiratori del Modello si integrano con quelli del Codice Etico adottato dalla Società, per quanto il Modello, per le finalità che gli stessi intendono perseguire in specifica attuazione delle disposizioni del Decreto, abbiano portata e finalità differenti rispetto al Codice Etico.

Sotto tale profilo, infatti, è opportuno precisare che:

- il Codice Etico riveste una portata generale in quanto contiene una serie di principi di “deontologia aziendale”, che la Società riconosce come propri e sui quali intende richiamare l’osservanza di tutti i suoi dipendenti e di tutti coloro che, anche all’esterno della Società, cooperano al perseguimento dei fini aziendali;
- il Modello risponde e soddisfa, invece, conformemente a quanto previsto nel Decreto, l’esigenza di predisporre un sistema di regole interne diretto a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi nell’interesse o a vantaggio della Società, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

5. ORGANISMO DI VIGILANZA

5.1 Istituzione e nomina dell’Organismo di Vigilanza

L’affidamento, ad un organismo societario dotato di autonomi poteri di iniziativa e controllo, dei compiti di vigilare sul funzionamento e l’osservanza del Modello, nonché di curarne l’aggiornamento, unitamente al corretto ed efficace svolgimento degli stessi, rappresentano presupposti indispensabili per l’esonero dalla responsabilità prevista dal D.Lgs. 231/2001.

I requisiti principali dell’Organismo di Vigilanza (di seguito anche “OdV”), così come proposti dalle Linee Guida emanate da Confindustria e fatti propri anche dagli organi giudicanti nelle diverse pronunce giurisprudenziali pubblicate, possono essere così identificati:

⁹ Coerentemente con quanto previsto all’art. 10 del “Regolamento in materia di esercizio del potere di direzione e coordinamento da parte della Capogruppo”, approvato dal Consiglio di Amministrazione di SITAF SpA in data 21 novembre 2017, il Codice Etico di RO.S.S. recepisce quello della Capogruppo SITAF S.p.A.

- autonomia ed indipendenza;
- professionalità;
- continuità di azione.

In base alle previsioni del Decreto l'Organismo di Vigilanza può essere individuato in una struttura monocratica, il cui membro coincide con la figura del Presidente, ovvero in una struttura plurisoggettiva all'interno della quale uno dei membri assolve alle funzioni di Presidente.

I membri dell'Organismo di Vigilanza, nominati direttamente dal Consiglio di Amministrazione, devono possedere i requisiti di onorabilità previsti, dalla vigente normativa per i membri del Consiglio di Amministrazione e per il Sindaco Unico della Società e sono individuati tra soggetti interni od esterni alla Società che abbiano le conoscenze e capacità tecniche necessarie allo svolgimento dei compiti dell'Organismo.

L'Organismo di Vigilanza risponde del proprio operato direttamente al Consiglio di Amministrazione di R.O.S.S., in modo da garantire la sua piena autonomia e indipendenza di giudizio nello svolgimento dei compiti che gli sono affidati.

Il compenso dell'Organismo di Vigilanza è definito dal Consiglio di Amministrazione. In particolare, ai membri del citato Organismo compete il rimborso delle spese vive sostenute nell'espletamento dell'incarico, nonché il riconoscimento di un emolumento annuo lordo.

L'Organismo provvede, a propria volta, a disciplinare le regole per il proprio funzionamento, formalizzandole in apposito regolamento (il "Regolamento").

5.2 Durata in carica e sostituzione dei membri dell'Organismo

I componenti dell'Organismo restano in carica per tre anni e sono sempre rieleggibili.

Consiglio di Amministrazione può revocare in ogni momento i membri dell'Organismo, per ragioni tassativamente previste, connesse a gravi inadempimenti rispetto al mandato assunto, ivi comprese le violazioni degli obblighi di riservatezza.

Costituiscono giusta causa di revoca dei componenti dell'OdV:

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico;
- la violazione dei doveri di riservatezza;
- l'"omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d), D.Lgs. 231/2001;
- gravi e accertati motivi di incompatibilità che ne vanifichino l'indipendenza e l'autonomia.

La revoca del mandato dovrà, in ogni caso, essere deliberata dal Consiglio di Amministrazione della Società con atto che specifichi chiaramente i motivi della decisione intrapresa.

I componenti dell'Organismo di Vigilanza debbono comunicare all'Organismo medesimo ed

al Consiglio di Amministrazione, sotto la loro piena responsabilità, il venir meno dei requisiti di onorabilità di cui al precedente paragrafo 5.1, con obbligo di rassegnare le dimissioni.

L'Organismo di Vigilanza comunica tempestivamente al Consiglio di Amministrazione il venir meno dalla carica per qualsiasi motivo di un suo membro.

5.3 Funzioni e poteri dell'Organismo di Vigilanza

All'OdV sono conferiti i poteri di iniziativa e controllo necessari ad assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello. In particolare, all'Organismo di Vigilanza di RO.S.S. è affidato il compito di:

- a) verificare l'efficienza ed efficacia del Modello, rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il D.lgs. 231/01;
- b) verificare il rispetto delle regole comportamentali e presidi di controllo previsti dal Modello e rilevare eventuali inosservanze;
- c) segnalare al Consiglio di Amministrazione eventuali necessità od opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso, anche in relazione a mutate condizioni aziendali o normative;
- d) segnalare al Consiglio di Amministrazione, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società.

L'Organismo potrà inoltre avvalersi - sotto la propria diretta sorveglianza e responsabilità, d'intesa con il Consiglio di Amministrazione - dell'ausilio di soggetti interni od esterni alla Società, cui demandare lo svolgimento delle attività operative di verifica. A tale fine il Consiglio di Amministrazione assegna all'Organismo un *budget* di spesa affinché quest'ultimo possa operare in autonomia e con gli strumenti opportuni per un efficace espletamento dei compiti assegnateli.

L'Organismo di Vigilanza ha libero accesso a tutta la documentazione aziendale rilevante. Inoltre il suo operato non può essere sindacato da nessun altro organismo o struttura aziendale, ad eccezione del Consiglio di Amministrazione, che ha il compito di vigilare sull'adeguatezza degli interventi dell'Organismo.

5.4 Modalità e periodicità di riporto agli organi societari

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riferisce direttamente al Consiglio di Amministrazione dell'Ente.

In particolare l'Organismo è tenuto a trasmettere al Consiglio di Amministrazione:

- con cadenza semestrale una relazione informativa, relativa all'attività svolta - che deve essere trasmessa anche al Sindaco Unico;
- al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione per quanto di competenza.

Nella relazione semestrale devono essere affrontati i seguenti aspetti:

- l'attività di vigilanza svolta dall'Organismo nel periodo di riferimento;
- le eventuali criticità emerse sia in termini di comportamenti interni a RO.S.S. sia in termini di efficacia del Modello;
- le comunicazioni delle eventuali indicazioni per l'aggiornamento o il miglioramento del Modello;
- il recepimento degli eventuali interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione;
- eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito della violazione del Modello;
- il piano delle attività previsto per il semestre successivo.

Gli incontri con i componenti della struttura societaria debbono essere verbalizzati e copie dei verbali saranno custodite a cura dell'Organismo con facoltà, da parte del Consiglio di Amministrazione, di prenderne visione.

5.5 Flussi informativi e segnalazioni all'Organismo di Vigilanza

A norma dell'art. 6, comma 2, lettera d), del D.Lgs. 231/2001, tra le esigenze cui deve rispondere il Modello è specificata la previsione di *“obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli”*.

All'Organismo di Vigilanza deve essere tempestivamente segnalata, da parte dei Destinatari del Modello, ogni situazione o informazione che possa essere rilevante per il monitoraggio dell'efficacia del Modello o che possa determinare una violazione del Modello, nonché ogni evento che possa ingenerare responsabilità ai sensi del Decreto o che comunque rappresenti un'infrazione alle regole societarie. Del pari, all'OdV deve essere trasmesso ogni documento che denunci tali circostanze.

È stato pertanto istituito un obbligo di informativa verso l'OdV, che si concretizza in flussi informativi periodici e segnalazioni occasionali. In particolare, l'OdV riceve:

- Flussi informativi periodici:** in capo a ciascun Responsabile di Direzione / Funzione / Ufficio aziendale, in qualità di soggetto preposto alla completa e corretta adozione delle regole aziendali a presidio dei rischi individuati nei settori di sua competenza, è previsto l'obbligo di trasmettere all'Organismo di Vigilanza, su base periodica, i dati e le informazioni necessarie all'espletamento delle funzioni di monitoraggio realizzate da quest'ultimo, così come dettagliate nella sezione *“Flussi Informativi verso l'Organismo di Vigilanza”*. (**“Flussi informativi”**);
- Segnalazioni occasionali:** tutti i Destinatari del presente Modello hanno l'obbligo di segnalare tempestivamente all'OdV le seguenti informazioni (**“Segnalazioni”**):
 - la commissione, il tentativo di commissione o il ragionevole pericolo di commissione dei reati previsti dal Decreto;

- eventuali presunte violazioni delle regole e delle modalità comportamentali ed operative definite nel Codice Etico, nel Modello e/o nel corpo normativo e procedurale aziendale – che possano determinare illeciti o irregolarità – di cui siano direttamente o indirettamente venuti a conoscenza;
- qualsiasi atto, fatto, evento od omissione rilevato od osservato nell'esercizio delle responsabilità e dei compiti assegnati, con profilo di criticità rispetto alle norme del Decreto;
- osservazioni sull'adeguatezza del sistema di controllo;
- qualsiasi eccezione comportamentale o qualsiasi evento inusuale indicando le ragioni delle difformità e dando atto del diverso processo seguito;
- ogni altra informazione inerente all'attuazione del Modello nelle attività a rischio reato, nonché il rispetto delle previsioni del Decreto, che possa risultare utile ai fini dell'assolvimento dei compiti dell'OdV.

In ogni caso, con riferimento al predetto elenco di informazioni, è demandato all'Organismo di Vigilanza il compito di richiedere, se necessario od opportuno, eventuali modifiche ed integrazioni delle informazioni da fornirsi.

Le segnalazioni, in ottemperanza al Decreto Legislativo n. 24/2023 in materia di *Whistleblowing*, potranno essere inviate a RO.S.S. attraverso i seguenti canali :

- in forma scritta o orale tramite la Piattaforma Digitale accessibile all'indirizzo <http://roadsafetyservices.integrityline.app>
- mediante posta ordinaria o raccomandata, riservata e personale, indirizzata al Ricevente, all'indirizzo di RO.S.S. Srl – via San Giuliano 2/a – 10059 Susa (TO);
- in forma orale, tramite incontro con il Ricevente.

Per i dettagli relativi alla gestione delle segnalazioni whistleblowing si rimanda alla Procedura interfunzionale gestione delle segnalazioni (whistleblowing) PGS040 di RO.S.S.

La Società vieta espressamente qualsiasi atto di ritorsione o di discriminazione, diretta o indiretta, nei confronti dei soggetti segnalanti per motivi collegati, direttamente o indirettamente, alle segnalazioni.

Inoltre, costituiscono condotte sanzionabili coerentemente con le previsioni del sistema disciplinare, sia la violazione da parte di un Destinatario delle misure di tutela del segnalante definite dalla Società, sia l'effettuazione, con dolo o colpa grave, di segnalazioni che si rivelino infondate.

L'Organismo di Vigilanza conserva tutta la documentazione inerente alle le comunicazioni ricevute in un apposito archivio informatico e cartaceo: l'accesso a detto archivio è consentito esclusivamente ai componenti dell'OdV e per le sole ragioni connesse all'espletamento dei compiti innanzi rappresentati.

Infine, l'Organismo di Vigilanza potrà richiedere, su base periodica o al verificarsi di

determinati eventi, dati e informazioni sulle attività svolte (c.d. “informazioni specifiche”) a tutti i Destinatari del presente Modello.

6. FORMAZIONE ED INFORMATIVA A SOGGETTI TERZI

6.1 Formazione del personale

L'adeguata formazione e la costante informazione dei Destinatari in ordine ai principi e alle prescrizioni contenute nel Modello rappresentano fattori di grande importanza per la corretta ed efficace attuazione dello stesso.

A tale proposito la Società garantisce l'organizzazione di attività formative specifiche rivolte ai soggetti apicali e agli altri dipendenti coinvolti nelle attività sensibili, con frequenza, modalità e contenuti idonei a garantire la conoscenza del Decreto e la diffusione del Modello e del Codice di Condotta.

La partecipazione ai corsi di formazione è obbligatoria rispetto a tutti i destinatari della formazione stessa e deve essere documentata.

Con specifico riferimento agli adempimenti in materia di salute e sicurezza dell'ambiente di lavoro le funzioni preposte si occupano di predisporre i necessari corsi di aggiornamento e di addestramento previsti dalla legge, nonché corsi di formazione per specifici ruoli in materia di sicurezza dandone pronta comunicazione all'Organismo di Vigilanza.

6.2 Informativa a collaboratori e professionisti esterni

Ai soggetti esterni alla Società (fornitori, collaboratori, professionisti, consulenti ecc.) sono fornite - da parte dei responsabili delle funzioni aziendali aventi contatti istituzionali con gli stessi e sotto il coordinamento dell'Organismo di Vigilanza - apposite informative sulle politiche e sulle procedure adottate dalla Società in conformità al Modello ed al Codice Etico. Tale informativa si estende altresì alle conseguenze che comportamenti contrari alle previsioni del Modello o comunque contrari al Codice Etico ovvero alla normativa vigente possono avere con riguardo ai rapporti contrattuali. Laddove possibile sono inserite, nella documentazione contrattuale, specifiche clausole dirette a disciplinare tali aspetti.

7. SISTEMA DISCIPLINARE E SANZIONATORIO

7.1 Principi generali

La definizione di un adeguato “Sistema Disciplinare”, che sanzioni il mancato rispetto e la violazione delle norme contenute nel Modello e nel Codice Etico adottato dalla Società, ed in generale violazioni di etica professionale, costituisce un presupposto essenziale per l'efficacia del Modello stesso.

Tale sistema disciplinare deve rivolgersi tanto ai lavoratori dipendenti quanto ai collaboratori e terzi che operino per conto della Società, prevedendo sia idonee sanzioni di carattere disciplinare sia di carattere contrattuale/negoziale (es. risoluzione del contratto,

cancellazione dall'elenco fornitori, ecc.).

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

Con specifico riferimento alle violazioni del Modello in materia di salute e sicurezza sul lavoro, i comportamenti sanzionabili sono quelli relativi al mancato rispetto degli adempimenti previsti dal T.U.S. o delle procedure interne aziendali.

7.2 Sanzioni per i lavoratori dipendenti (non dirigenti)

Con riguardo ai lavoratori dipendenti, il sistema disciplinare relativo al personale dipendente non dirigente applicato in R.O.S.S. è specificamente regolato dal vigente Contratto Collettivo Nazionale di Lavoro adottato (di seguito CCNL), nonché dalle Norme Disciplinari adottate dalla società (le "Norme Disciplinari").

Al fine di ottemperare alle previsioni del Decreto con riguardo all'adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto, da parte dei dipendenti non dirigenti, delle misure previste nel Modello, la Società si avvarrà del sistema disciplinare già previsto dal vigente CCNL, provvedendo (tramite, ad esempio, un ordine di servizio od una comunicazione interna) ad adeguare e ad aggiornare il sistema esistente al disposto normativo del citato Decreto.

In particolare, la Società renderà edotti i propri dipendenti del fatto che il Modello rientra nelle attribuzioni del datore di lavoro di impartire disposizioni per l'esecuzione e per la disciplina del lavoro (art. 2104 c.c.) e che, conseguentemente, il mancato rispetto e/o la violazione degli stessi, delle regole di comportamento imposte dal Codice Etico e delle procedure aziendali, ad opera di lavoratori dipendenti della Società, costituiscono inadempimento alle obbligazioni derivanti dal rapporto di lavoro e, pertanto, illecito disciplinare (art. 2106 c.c.): in quanto tali, possono comportare la comminazione delle sanzioni previste dalla normativa vigente e dalla contrattazione collettiva.

La predetta opera di adeguamento alla realtà aziendale delle previsioni contenute nel citato CCNL in conseguenza all'adozione del Modello potrà avvenire, a titolo esemplificativo, prevedendo la possibilità di applicare le sanzioni previste nel CCNL e nelle citate Norme Disciplinari a fronte di qualunque violazione delle misure previste nel Modello.

In particolare, si prevede l'applicazione dei seguenti provvedimenti disciplinari a fronte di inadempimenti contrattuali:

- a) rimprovero verbale;
- b) rimprovero scritto;
- c) multa (non eccedente a 4 ore della normale retribuzione);

- d) sospensione dal servizio e dalla retribuzione fino ad un massimo di 10 giorni;
- e) licenziamento senza preavviso.

Restano ferme, e si intendono qui richiamate, tutte le disposizioni di cui all'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori") in relazione sia all'esposizione del codice disciplinare ed all'obbligo di preventiva contestazione dell'addebito al dipendente, anche al fine di consentire allo stesso di approntare una idonea difesa e di fornire eventuali giustificazioni.

Ad integrazione, nell'ambito del presente Modello di Organizzazione e Gestione e Controllo, dell'esemplificazione prevista dal CCNL di categoria si precisa che:

- le sanzioni disciplinari previste ai punti (a) e (b) sono comminate ai lavoratori dipendenti che, per negligenza, violano le regole, i principi e le procedure previste dal Modello e dal Codice Etico adottando, eventualmente anche mediante omissioni, comportamenti non conformi agli stessi o non adeguati, ma comunque tali da non minare l'efficacia dei citati documenti. Tali sanzioni disciplinari sono inoltre previste nel caso in cui i dipendenti non rispettino gli obblighi previsti in materia di *whistleblowing*.

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

E così in via esemplificativa:

- la sanzione dell'ammonizione verbale può essere attuata in caso di lieve inosservanza dei principi e dalle procedure previste dal Modello e dal Codice Etico dovuti a negligenza del dipendente. A titolo esemplificativo e non esaustivo, è punibile con l'ammonizione verbale il dipendente che, per negligenza, trascuri di conservare in maniera accurata la documentazione di supporto necessaria per ricostruire l'operatività della Società nelle aree a rischio 231;
- la sanzione dell'ammonizione scritta viene adottata in ipotesi di ripetute mancanze punite con il rimprovero verbale, o in caso di violazione colposa dei principi e delle procedure previste dal Modello e Codice Etico, attraverso un comportamento eventualmente anche mediante omissioni, non conforme o non adeguato: a titolo esemplificativo e non esaustivo in caso di ritardata segnalazione all'OdV delle informazioni dovute ai sensi del Modello. Tale sanzione viene applicata altresì nei casi in cui si verifichi una inosservanza colposa della normativa in materia di *whistleblowing*, ad esempio nel caso in cui un dipendente effettui una o più segnalazioni che si rivelano false e prive di fondamento nei confronti di un altro soggetto o qualora un dipendente tenti di violare le norme in materia di tutela del segnalante.

Le sanzioni disciplinari di cui ai punti (c) e (d) sono comminate ai lavoratori dipendenti in caso di reiterate violazioni di cui ai precedenti punti o in caso di comportamenti colposi e/o

negligenti posti in essere dal personale dipendente che opera in aree a rischio 231, che possono minare anche potenzialmente l'efficacia del Modello e del Codice Etico.

E così, in via esemplificativa:

- la multa può essere applicata in misura non eccedente a 4 ore della normale retribuzione, nel caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello e dal Codice Etico per un comportamento non conforme o non adeguato in misura tale da essere considerata di una certa gravità. A titolo esemplificativo e non esaustivo, tra tali comportamenti rientra la violazione degli obblighi di informazione nei confronti dell'OdV di irregolarità commesse nello svolgimento delle proprie attività, ovvero la mancata reiterata partecipazione, senza giustificato motivo alle sessioni formative erogate dalla Società relative al D.Lgs. 231/2001, al Modello di organizzazione, gestione e controllo e al Codice Etico o in ordine a tematiche relative;
- la sospensione dal servizio e dalla retribuzione non può essere disposta per più di 10 giorni e va applicata in caso di gravi violazioni procedurali tali da esporre la Società a responsabilità nei confronti di terzi. A titolo esemplificativo e non esaustivo: l'inosservanza delle prescrizioni del Codice Etico; l'omissione o il rilascio di false dichiarazioni relative al rispetto del Modello; l'inosservanza delle disposizioni dei poteri di firma e del sistema delle deleghe; l'omissione della vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità al fine di verificare le loro azioni nelle aree sensibili; la violazione degli obblighi di informazione nei confronti dell'OdV di ogni situazione a rischio di verifica dei reati presupposti avvertita nello svolgimento delle proprie attività; ogni e qualsiasi altra inosservanza contrattuale o di specifica disposizione comunicata al dipendente. Inoltre, in materia di *whistleblowing*, tale sanzione è prevista, ad esempio, nei casi in cui un dipendente effettui, all'interno dell'ambito lavorativo e con dolo, una segnalazione di illecito nei confronti di un altro soggetto che successivamente si riveli falsa ed infondata, o ancora nei casi in cui un dipendente violi le misure volte alla tutela del segnalante illeciti.

La sanzione disciplinare di cui al punto e) è inflitta al dipendente che ponga in essere, nell'espletamento delle sue attività, un comportamento non conforme alle prescrizioni del Modello e del Codice Etico e diretto in modo univoco al compimento di un reato sanzionato dal Decreto e tale da poter determinare l'applicazione a carico di R.O.S.S. delle sanzioni amministrative derivanti da reato previste dal Decreto.

- E così in via esemplificativa il licenziamento senza preavviso per giusta causa è una sanzione inflitta in conseguenza di una mancanza così grave (per la dolosità del fatto, o per i riflessi penali o pecuniari o per la sua recidività) da non consentire la prosecuzione, anche provvisoria del rapporto di lavoro. Tra le violazioni passibili della predetta sanzione, a titolo esemplificativo e non esaustivo: comportamento fraudolento inequivocabilmente diretto alla commissione di uno dei reati previsti dal Decreto tale da far venir meno il rapporto fiduciario con il datore di lavoro; redazione di documentazione incompleta o non veritiera dolosamente diretta ad impedire la

trasparenza e verificabilità dell'attività svolta; violazione dolosa di procedure aventi rilevanza esterna; omessa redazione della documentazione prevista dal Modello; violazione o elusione dolosa del sistema di controllo previsto dal Modello in qualsiasi modo effettuata, incluse la sottrazione, distruzione o alterazione della documentazione inerente alla procedura; realizzazione di comportamenti di ostacolo o elusione ai controlli dell'OdV, impedimento di accesso alle informazioni e alla documentazione da parte dei soggetti preposti ai controlli o alle decisioni. Inoltre, in materia di *whistleblowing*, tale sanzione è prevista, ad esempio, nei casi in cui un dipendente effettui in maniera reiterata, all' interno dell'ambito lavorativo e con dolo, una segnalazione di illecito nei confronti di un altro soggetto che successivamente si riveli falsa ed infondata, o ancora nei casi in cui un dipendente violi ripetutamente gli obblighi di riservatezza di cui al decreto legislativo n. 24 del 2023 art.12.

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

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

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

7.3 Sanzioni per i lavoratori dipendenti (dirigenti)

Con riguardo ai dirigenti, in assenza di un sistema disciplinare applicabile agli stessi ed in considerazione del particolare rapporto fiduciario con il datore di lavoro, gli stessi sono tenuti al rispetto di quanto previsto nel presente Modello e/o nel Codice Etico e il rispetto delle normative in materia di tutela del segnalante nell'ambito di un rapporto lavorativo e l'obbligo a che gli stessi facciano rispettare quanto previsto negli stessi documenti è elemento essenziale del rapporto di lavoro dirigenziale, costituendo stimolo ed esempio per tutti coloro che a loro riportano gerarchicamente. In caso di violazione dei principi generali del Modello, delle regole di comportamento imposte dal Codice etico e dei presidi di controllo contenuti nelle Parti Speciali del Modello e nelle procedure aziendali – anche su segnalazione dell'Organismo di Vigilanza - l'Amministratore Delegato o, in caso di conflitto di interesse, il Consiglio di Amministrazione, provvederà ad assumere nei confronti dei responsabili i provvedimenti ritenuti idonei in funzione delle violazioni commesse, tenuto conto che le stesse costituiscono inadempimento alle obbligazioni derivanti dal rapporto di lavoro.

Le sanzioni saranno comminate in ragione della gravità e/o recidività della condotta del dirigente e comunque sulla base di quanto previsto dallo Statuto dei Lavoratori e dal

Contratto Collettivo Nazionale di Lavoro per i Dirigenti. Il medesimo regime sanzionatorio si applica nei casi in cui il dirigente, sia coinvolto in episodi che comportano violazioni della normativa in materia di *whistleblowing*.

In via esemplificativa, potranno essere applicate nei confronti dei Dirigenti le seguenti sanzioni:

- rimprovero scritto e intimazione a conformarsi alle disposizioni del Modello, in caso di violazione non grave di una o più regole comportamentali o procedurali previste nel Modello e nel Codice Etico. Inoltre, in materia di *whistleblowing*, tale sanzione è prevista, ad esempio, nei casi in cui un dirigente effettui, all' interno dell'ambito lavorativo e con colpa, un ostacolo o un tentato ostacolo alla segnalazione di illecito, o ancora nei casi in cui un dirigente non abbia provveduto all'adozione di procedure per la gestione dei sistemi di segnalazione, ovvero ad effettuare le attività di verifica ed analisi delle segnalazioni ricevute;
- sospensione a titolo cautelare dalla prestazione lavorativa - fermo il diritto degli stessi dirigenti alla retribuzione, nonché, sempre in via provvisoria ed eventuale per un periodo non superiore a tre mesi, l'adibizione ad incarichi diversi, nel rispetto dell'art. 2103 codice civile – in caso di grave violazione di una o più regole comportamentali o procedurali previste nel Modello e nel Codice Etico. Inoltre, in materia di *whistleblowing*, tale sanzione è prevista, ad esempio, nei casi in cui un dirigente effettui, all' interno dell'ambito lavorativo e con dolo, un ostacolo o un tentato ostacolo alla segnalazione di illecito, o ancora nei casi in cui un dirigente non abbia provveduto all'adozione di procedure per la gestione dei sistemi di segnalazione, ovvero ad effettuare le attività di verifica ed analisi delle segnalazioni ricevute;
- licenziamento per giusta causa, in caso di reiterate e gravi violazioni di una o più prescrizioni del Modello e del Codice Etico tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro. Tale sanzione è applicata ad esempio, nel caso in cui un dirigente violi in modo reiterato le misure previste per la tutela del segnalante illeciti nell'ambito di un rapporto lavorativo o effettui reiterate dolose segnalazioni nei confronti di altro soggetto all'interno dell'ambito lavorativo, che si rivelino false ed infondate.

Resta salvo il diritto della Società a richiedere il risarcimento del maggior danno subito a causa del comportamento del dirigente.

Al dirigente potranno inoltre essere revocate le procure o le deleghe eventualmente conferitegli.

7.4 Sanzioni nei confronti degli Amministratori e dei Sindaci

In caso di violazione della normativa vigente, delle disposizioni del Modello, ivi incluse quelle della documentazione che di esso forma parte, o del Codice Etico e di Comportamento e il mancato rispetto delle normative in materia di tutela del segnalante illeciti nell'ambito di un rapporto lavorativo (whistleblowing) da parte di componenti del Consiglio di Amministrazione della Società, ovvero il Sindaco Unico, l'Organismo di Vigilanza informa tempestivamente l'intero Consiglio di Amministrazione ed il Sindaco Unico, i quali procederanno ai sensi di legge ad assumere le iniziative più opportune e adeguate in relazione alla gravità della violazione rilevata e conformemente ai poteri previsti dalla vigente normativa e dallo Statuto sociale, coinvolgendo, ove necessario, l'Assemblea dei Soci..

7.5 Sanzioni nei confronti di collaboratori, consulenti ed altri soggetti terzi

Ogni comportamento posto in essere dai collaboratori, dai consulenti o da altri terzi collegati alla Società da un rapporto contrattuale non di lavoro dipendente, in violazione delle previsioni del Decreto e/o del Codice etico per le parti di loro competenza, potrà determinare l'applicazione di penali o la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società, anche indipendentemente dalla risoluzione del rapporto contrattuale.

A tal fine è previsto, soprattutto nel caso di attività affidate a terzi in “*outsourcing*”, l'inserimento nei contratti di specifiche clausole che i) diano atto della conoscenza del Decreto, ii) richiedano l'assunzione di un impegno ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto medesimo (a prescindere dalla effettiva consumazione del reato o dalla punibilità dello stesso), iii) disciplinino le conseguenze in caso di violazione delle previsioni contenute nella citata clausola; ovvero una dichiarazione unilaterale da parte del terzo o del collaboratore circa la conoscenza del Decreto e l'impegno a improntare la propria attività al rispetto delle previsioni dello stesso.

7.6 Garanzie inerenti al sistema di segnalazione whistleblowing

Si segnala che, gli enti e le persone che effettuano le segnalazioni, possono comunicare all'ANAC le ritorsioni che ritengono di avere subito. In caso di ritorsioni commesse nel contesto lavorativo del segnalante l'ANAC informa l'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza.

Inoltre, al fine di acquisire elementi istruttori indispensabili all'accertamento delle ritorsioni, l'ANAC può avvalersi, per quanto di rispettiva competenza, della collaborazione dell'Ispettorato nazionale del lavoro, ferma restando l'esclusiva competenza dell'ANAC in ordine alla valutazione degli elementi acquisiti e all'eventuale applicazione delle sanzioni amministrative di cui all'articolo 21. Al fine di regolare tale collaborazione, l'ANAC conclude

specifici accordi, ai sensi dell'articolo 15 della legge 7 agosto 1990, n. 241, con l'Ispettorato nazionale del lavoro.

Gli atti assunti in violazione dell'articolo 17 (divieto di ritorsione) sono nulli. I soggetti che siano stati licenziati a causa della segnalazione, della divulgazione pubblica o della denuncia all'autorità giudiziaria o contabile hanno diritto a essere reintegrate nel posto di lavoro, ai sensi dell'articolo 18 della legge 20 maggio 1970, n. 300 o dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23, in ragione della specifica disciplina applicabile al lavoratore.

L'Autorità giudiziaria adita adotta tutte le misure, anche provvisorie, necessarie ad assicurare la tutela alla situazione giuridica soggettiva azionata, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l'ordine di cessazione della condotta posta in essere in violazione dell'articolo 17 e da dichiarazione di nullità degli atti adottati in violazione del medesimo articolo. riportare l'art 19 del decreto 24/2023La Società non tollera un abuso dell'istituto del whistleblowing, ossia un utilizzo di detto canale riservato per effettuare segnalazioni con un evidente carattere diffamatorio e opportunistico.

PARTI SPECIALI

PARTE SPECIALE A: GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Gestione degli adempimenti verso la Pubblica Amministrazione;
- Gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza in occasione di visite ispettive;
- Gestione del contenzioso.

Alla data di emissione del presente documento, in ragione delle attività affidate in *service* alla Capogruppo SITAF S.p.A. (*si vedano in particolare le successive sezioni B e C*), i rapporti con i Funzionari della Pubblica Amministrazione possono essere intrattenuti direttamente dalle Direzioni / Aree interessate presso la Capogruppo.

3. DEFINIZIONI

Ai fini del presente documento, rientrano nel concetto di Pubblica Amministrazione le Istituzioni Pubbliche, i Pubblici Ufficiali e gli Incaricati di Pubblico Servizio.

Le **Istituzioni Pubbliche** sono, a titolo esemplificativo e non esaustivo: le amministrazioni dello Stato, le regioni, le province, i comuni, consorzi e associazioni, le camere di commercio, industria, artigianato e agricoltura, le aziende e gli enti del servizio sanitario nazionale etc.; funzione pubblica viene rivestita anche dai membri della Commissione delle comunità europee e del Parlamento Europeo.

Per **Pubblico Ufficiale** si intende un soggetto, pubblico dipendente o privato, che concorre a formare o forma la volontà dell'Ente Pubblico ovvero lo rappresenta all'esterno; un soggetto munito di poteri autorizzativi e di certificazione.

Secondo la dottrina prevalente per **Incaricato di Pubblico Servizio** si intende un soggetto che pur svolgendo un'attività pertinente allo Stato o ad un altro Ente pubblico non è dotato dei poteri tipici del pubblico ufficiale e, d'altra parte, non svolge funzioni meramente materiali.

4. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati contro la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01):
 - Reati corruttivi;
 - Concussione;
 - Induzione indebita a dare o promettere utilità;
 - Istigazione alla corruzione; Traffico di influenze illecite;
 - Malversazione di erogazioni pubbliche;
 - Indebita percezione di erogazioni, truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee o per il conseguimento di erogazioni pubbliche;
- Reati Societari (art. 25-ter del D.Lgs. 231/01):
 - Corruzione tra privati;
 - Istigazione alla corruzione tra privati;
 - Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza.
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies D.Lgs. 231/2001).

Si rimanda all'Allegato 1 del Modello (*"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"*) per una descrizione di dettaglio di ciascuna fattispecie richiamata.

5. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- assicurare che i rapporti intrattenuti con i pubblici funzionari avvengano nell'assoluto rispetto delle leggi e normative vigenti;
- intrattenere rapporti corretti, trasparenti, imparziali e collaborativi con i funzionari della Pubblica Amministrazione, coerentemente con i principi contenuti nel Codice Etico;
- assicurare che gli adempimenti nei confronti della Pubblica Amministrazione siano effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete e veritiere evitando, e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto di interesse, nonché modalità espositive che possano trarre in inganno la controparte pubblica. In caso di pratiche di difficile o dubbia soluzione, è necessario rivolgersi a consulenti specializzati;
- fornire, ai propri collaboratori (interni ed esterni) adeguate direttive sulle modalità di condotta da adottare nei contatti formali e informali con soggetti della Pubblica Amministrazione;
- espletare diligentemente e tempestivamente tutti gli adempimenti richiesti dalla normativa / regolamentazione applicabile nell'ambito della propria attività;
- trasmettere tutte le comunicazioni previste dalla legge e dai regolamenti alle Autorità di Vigilanza, o qualsiasi altra comunicazione richiesta per altri motivi, con la massima tempestività e nel modo più completo e accurato possibile;

- assicurare che tutta la documentazione inviata a o condivisa con la Pubblica Amministrazione (compresa la documentazione inerente agli adempimenti fiscali), predisposta sia internamente che con il supporto di collaboratori / consulenti esterni, sia completa, veritiera e corretta;
- sottoporre a soggetti muniti di idonei poteri, coerentemente con il sistema di procure e deleghe in vigore, la documentazione al fine di verificarla e approvarla prima dell'inoltro alla Pubblica Amministrazione;
- garantire, in caso di visite ispettive, che a rappresentare la Società siano soggetti autorizzati in base al sistema di procure e deleghe in essere e che sia tenuta traccia delle ispezioni ricevute e delle relative risultanze; chiunque sia coinvolto nella predisposizione/invio di informazioni e/o documenti, ovvero nella predisposizione di tutto o parte di relazioni, report, segnalazioni, ecc., deve contribuire garantendo massima trasparenza, veridicità, completezza, pertinenza, riservatezza e integrità delle informazioni. Le informazioni generate dovranno essere altresì aggiornate (sempre nel rispetto del principio di stretta necessità e non eccedenza delle informazioni, di cui alla normativa in materia di privacy vigente). Le informazioni dovranno essere esposte in modo chiaro e non ingannevole, non dovranno essere omesse informazioni necessarie al corretto intendimento del documento o dei fatti, affinché non si induca in errore il lettore. Nell'elaborazione dei documenti è vietata qualsiasi forma di raggirio o inganno;
- sottoporre ai soggetti muniti di idonei poteri, in base al sistema di procure e deleghe in essere, la documentazione al fine di verificarla ed approvarla prima dell'inoltro alla Pubblica Amministrazione;
- garantire la corretta archiviazione di tutta la documentazione prodotta e consegnata al fine di garantire la completa tracciabilità delle varie fasi del processo;
- prestare completa e immediata collaborazione ai funzionari della Pubblica Amministrazione durante le visite ispettive, fornendo la documentazione e le informazioni richieste in modo esaustivo e puntuale;
- segnalare, senza ritardo, al proprio responsabile gerarchico e all'Organismo di Vigilanza eventuali tentativi di richieste indebite da parte di funzionari della Pubblica Amministrazione rivolti, ad esempio, a ottenere favori, elargizioni illecite di denaro o altre utilità, anche nei confronti di terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la Pubblica Amministrazione.

Con particolare riferimento ai rapporti con le Autorità Giudiziarie:

- avvertire tempestivamente il proprio responsabile gerarchico in merito ad ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o ad essa attinente;
- prestare completa, trasparente e immediata collaborazione all'Autorità Giudiziaria e agli Organi di Polizia Giudiziaria, fornendo puntualmente ed esaustivamente la documentazione e le informazioni richieste;

- rendere sempre all'Autorità Giudiziaria dichiarazioni veritiere, complete, corrette e rappresentative dei fatti;
- esprimere liberamente le proprie rappresentazioni dei fatti o esercitare la facoltà di non rispondere, accordata dalla legge, se indagati o imputati in procedimenti penali;
- avvertire tempestivamente il proprio responsabile gerarchico di ogni minaccia, pressione, offerta o promessa di denaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da utilizzare in procedimenti penali.

È inoltre espressamente **vietato**:

- corrispondere o offrire, direttamente o indirettamente, anche sotto forme diverse di aiuti o contribuzioni (ad esempio, sponsorizzazioni e liberalità), pagamenti o benefici materiali a pubblici ufficiali o incaricati di pubblico servizio o a persone a questi vicini, o a intermediari o mediatori per influenzare il loro comportamento e assicurare vantaggi di qualunque tipo alla Società;
- indurre pubblici ufficiali o incaricati di pubblico servizio a procurare alla Società un ingiusto vantaggio patrimoniale ovvero ad arrecare un danno a terzi in violazione di norme di legge o di regolamento;
- accettare omaggi o altre utilità provenienti da pubblici funzionari o incaricati di pubblico servizio;
- cedere a raccomandazioni o pressioni provenienti da pubblici funzionari o incaricati di pubblico servizio;
- tenere condotte ingannevoli nei confronti della Pubblica Amministrazione tali da indurla in errori di valutazione;
- omettere informazioni dovute o presentare documenti e dichiarazioni non veritieri, al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione;
- esporre dati, notizie, informazioni false nelle comunicazioni alle Autorità Pubbliche di Vigilanza o occultare fatti che avrebbero dovuto essere comunicati;
- omettere le informazioni dovute nelle comunicazioni alle predette Autorità e, in genere, tenere comportamenti ostruzionistici quali, a titolo puramente indicativo, opporre rifiuti pretestuosi, ritardare l'invio delle comunicazioni o la messa a disposizione della documentazione richiesta;
- ostacolare in qualunque modo le Autorità Pubbliche di Vigilanza nell'esercizio delle funzioni loro demandate dalla legge;
- porre in essere qualsiasi comportamento, anche attraverso interposta persona, finalizzato a influenzare l'indipendenza di giudizio del Pubblico Ufficiale, finalizzato a distoglierlo dal servizio esclusivo alla Pubblica Amministrazione, a violare le regole di disciplina ed onore della stessa o i principi di buon andamento e imparzialità della Pubblica Amministrazione;

- nelle ore di lavoro, distogliere il Pubblico Ufficiale dallo svolgimento delle proprie incombenze, promettendo o coinvolgendolo in attività di svago, viaggi e/o sollevandolo dai propri compiti eseguendone le attività;
- chiedere al Pubblico Ufficiale informazioni di cui dispone per ragioni d'ufficio, comportamenti che ostacolino l'esercizio di diritti di terzi, comportamenti che intralcino l'esercizio della Pubblica Amministrazione;
- laddove gli adempimenti vengano effettuati utilizzando il sistema informatico / telematico della Pubblica Amministrazione, accedere senza autorizzazione, alterare lo stesso e i dati inseriti, ovvero utilizzare in modo improprio o illecito i dati trattati, procurando un danno alla Pubblica Amministrazione stessa;

Con particolare riferimento alla richiesta e/o gestione di finanziamenti od agevolazioni devono essere rispettati i seguenti principi comportamentali:

- In occasione della predisposizione di documenti e informazioni devono rispettarsi le norme fiscali e le regole disposte dal Codice etico e, in particolare, deve garantirsi la massima trasparenza, veridicità, completezza, pertinenza, riservatezza e integrità delle informazioni;
- Nella pratica di richiesta devono essere indicate solo ed esclusivamente informazioni vere, complete aggiornate e documentabili. Per gli aspetti fiscali e tributari, nonché per gli aspetti di regolamentazione del bando, se del caso (per esempio laddove vi siano dubbi interpretativi rispetto alle norme), devono essere assunti pareri da parte di esperti che confermino la conformità alle norme anche fiscali della pratica;
- Le informazioni devono essere espone in modo chiaro e non ingannevole, non devono essere omesse informazioni necessarie al corretto intendimento del documento o dei fatti, affinché non si induca in errore il lettore;
- Nell'elaborazione dei documenti è vietata qualsiasi forma di raggirio o inganno.
- I finanziamenti possono essere utilizzati esclusivamente per finalità di gestione o esecuzione dei progetti finanziati;
- Per il finanziamento o agevolazione, concesso o erogato in conto capitale dallo Stato, da altri enti pubblici o dall'Unione Europea, la Società – se richiesto dal bando - deve avvalersi di uno o più conti correnti bancari o postali accesi presso banche o presso la società Poste Italiane S.p.A. A tal fine, l'organo/persona delegata, sulla base del sistema di deleghe e procure vigente, autorizza l'apertura di un conto corrente bancario appositamente dedicato, anche se non in via esclusiva, al finanziamento stesso ovvero indicherà come conto corrente dedicato anche un conto già esistente.
- Tutti i movimenti finanziari relativi al finanziamento devono essere effettuati esclusivamente tramite bonifico bancario (o postale) ovvero con altri strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni.
- Ai progetti finanziati devono essere imputati solo ed esclusivamente costi effettivi, veritieri supportati da idonea documentazione contabile-fiscale relativa ad attività imputabili al progetto finanziato.

Con particolare riferimento ai rapporti con le Autorità Giudiziarie è **vietato**:

- porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa, nel corso di un procedimento penale, civile o amministrativo;
- condizionare, in qualsiasi forma e con qualsiasi modalità, la volontà dei soggetti chiamati a rispondere all'Autorità Giudiziaria al fine di non rendere dichiarazioni o dichiarare fatti non rispondenti al vero;
- promettere o offrire denaro, omaggi o altra utilità, direttamente o per interposta persona, a soggetti coinvolti in procedimenti penali, civili o amministrativi o a persone a questi vicini;
- accettare denaro o altra utilità, anche attraverso consulenti o terzi, se coinvolti in procedimenti penali, civili o amministrativi.

Eventuali rapporti lavorativi con dipendenti pubblici, quali consulenze, dovranno essere anticipati da una comunicazione alla Pubblica Amministrazione. Si ricorda che sul dipendente pubblico grava l'obbligo di astenersi dal partecipare all'adozione di decisioni o ad attività che possano coinvolgere interessi propri ovvero:

- di suoi parenti entro il quarto grado o conviventi (che abbiano rapporti con la Società);
- di individui od organizzazioni con cui egli stesso o il coniuge abbia causa pendente o grave inimicizia o rapporti di credito o debito (quale la Società);
- di individui od organizzazioni di cui egli sia tutore, curatore, procuratore o agente;
- ogni altro caso in cui esistano gravi ragioni di convenienza.

Si ricorda che in base al codice comportamentale dei dipendenti delle pubbliche amministrazioni, 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".

6. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

6.1 Gestione degli adempimenti verso la Pubblica Amministrazione

Ciascun soggetto aziendale che, nell'espletamento delle proprie funzioni, intrattenga rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza, deve coordinarsi con l'Ufficio

Competente nella specifica area di interesse ed eventualmente con la Direzione / Area rilevante presso la Capogruppo SITAF S.p.A.

Tutte le comunicazioni pervenute da parte della Pubblica Amministrazione e delle Autorità di Vigilanza devono essere condivise con l'Amministratore Delegato (o soggetto da questo delegato) che, sulla base delle tematiche affrontate, ha il compito di indirizzarle all'Ufficio Competente e di valutare la necessità di rilasciare deleghe o procure speciali al fine della gestione dei rapporti con l'esterno.

L'Ufficio Competente, valutate le richieste pervenute, ovvero nell'espletamento degli adempimenti di legge di competenza, ha il compito di richiedere i dati e le informazioni ufficiali agli Uffici responsabili e di trasmettere, nel rispetto dei principi di tempestività, correttezza, chiarezza e accuratezza, la documentazione alla Pubblica Amministrazione e alle Autorità di Vigilanza. I documenti devono essere elaborati in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo.

Prima dell'invio, tutte le comunicazioni devono essere verificate e sottoscritte dall'Amministratore Delegato e/o da un procuratore delegato.

È fatto obbligo all'Ufficio Competente archiviare e conservare tutta la documentazione prodotta nell'ambito della propria attività, trasmessa alla Pubblica Amministrazione e alle Autorità di Vigilanza.

Qualora la Società si avvalga, per la gestione degli adempimenti verso la Pubblica Amministrazione e le Autorità di Vigilanza, di consulenti esterni, nel processo di selezione e contrattualizzazione del professionista si applicano i presidi di controllo disciplinati con riferimento alla "Gestione degli acquisti di beni, servizi e incarichi professionali" (*sezione D del presente documento*).

L'assunzione di impegni verso la Pubblica Amministrazione e le Istituzioni Pubbliche è riservata esclusivamente all'organo/persona delegata, nel rispetto della più rigorosa osservanza delle disposizioni di legge e regolamentari applicabili. In particolare.

6.2 Gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza in occasione di visite ispettive

Le visite ispettive da parte di funzionari della Pubblica Amministrazione sono gestite dall'Amministratore Delegato o da soggetto da questo formalmente delegato, con il supporto dei Responsabili degli Uffici Competenti e delle Direzioni / Aree preposte della Capogruppo SITAF S.p.A., a seconda dell'oggetto dell'ispezione.

Nel corso della visita ispettiva, i Funzionari Pubblici sono sempre accompagnati da almeno due soggetti aziendali. Qualora questo non fosse possibile e all'ispezione fosse presente un solo referente aziendale, questo è tenuto ad indicarne formalmente la motivazione nel verbale di visita ispettiva.

In occasione di ispezioni i soggetti interessati possono avvalersi, se opportuno, di professionisti esterni, sulla base della rilevanza e delle implicazioni giuridiche dell'ispezione, anche allo scopo di verificare la legittimità della stessa. Qualora la Società intenda avvalersi di consulenti esterni, nel processo di selezione e contrattualizzazione del professionista si applicano i presidi di controllo disciplinati nella "Gestione degli acquisti di beni, servizi e incarichi professionali" (*sezione D del presente documento*).

La Società è tenuta a conservare evidenza documentale delle richieste ricevute, dei verbali predisposti dai funzionari pubblici in occasione delle visite ispettive nonché delle informazioni, dei dati e dei documenti consegnati, resi disponibili e/o comunicati. L'Amministratore Delegato o soggetto da lui formalmente delegato è responsabile di siglare i verbali predisposti dai Funzionari stessi.

Qualora l'esito dell'ispezione preveda l'invio di ulteriore documentazione, ovvero siano previste ulteriori visite da parte degli ispettori, l'Amministratore Delegato o soggetto da lui formalmente delegato è garante dell'invio degli ulteriori documenti e partecipa, se necessario, alle visite di controllo. La Società dovrà infine archiviare i verbali presso gli uffici di competenza.

Nel caso in cui a valle dell'ispezione non sia prevista, da parte dei Funzionari Pubblici, la formalizzazione di un verbale, i soggetti che hanno presenziato alla visita sono tenuti a predisporre un *memorandum* ad uso interno della Società, con indicazione almeno delle seguenti informazioni: data e oggetto dell'ispezione, Ente e soggetti aziendali coinvolti, esito della visita.

6.3 Gestione del contenzioso

L'avvio del procedimento di contenzioso è preventivamente autorizzato dall'Amministratore Delegato. La gestione dei contenziosi avviene con il supporto di legali esterni, contrattualizzati secondo le modalità previste nella sezione D "Gestione degli acquisti di beni, servizi e incarichi professionali", cui si rimanda per maggiori dettagli.

Le lettere di incarico a tali professionisti sono sottoscritte dall'Amministratore Delegato o da soggetto da questo delegato e contengono una clausola risolutoria ex D.Lgs. 231/01, con la quale la controparte dichiara di conoscere il contenuto del D.Lgs. 231/2001 ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto medesimo. Il professionista si impegna inoltre a rispettare i principi di comportamento richiamati dal Codice Etico di RO.S.S..

Tutti i soggetti aziendali/consulenti devono evitare di prendere contatti in modo autonomo con soggetti chiamati a rendere, avanti l'Autorità Giudiziaria, dichiarazioni utilizzabili in un procedimento penale per fatti che siano in qualsiasi modo connessi all'attività della Società. Tutti i soggetti aziendali / consulenti che intrattengono rapporti con l'Autorità Giudiziaria per conto di RO.S.S. sono autorizzati dall'Amministratore Delegato o altro soggetto dotato di adeguati poteri. In particolare, ai legali esterni a cui sono attribuiti poteri di rappresentanza

devono essere conferite, a firma dell'Amministratore Delegato o altro soggetto delegato, apposite procure speciali.

Tutta la documentazione da inviare all'Autorità Giudiziaria è firmata per approvazione dall'Amministratore Delegato o da altro soggetto delegato.

Nella gestione del contenzioso è comunque fatto divieto di:

- concludere accordi transattivi in assenza dei necessari presupposti come contropartita per indurre la controparte a promuovere o favorire gli interessi della Società impropriamente o in ogni caso in violazione delle normative applicabili;
- accettare denaro, altra utilità o qualsiasi forma di condizionamento, al fine di rilasciare false dichiarazioni, o a non rilasciare dichiarazioni, nell'ambito di un processo penale;
- ricorrere alla forza fisica, a minacce o all'intimidazione oppure promettere, offrire o concedere un'indebita utilità per indurre colui il quale può avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'Autorità Giudiziaria, con l'intento di ottenere una pronuncia favorevole alla Società o determinare il conseguimento di altro genere di vantaggio.

6.4 Gestione della collaborazione volontaria con la prefettura ed il gruppo interforze

Qualora la Società intraprendesse una collaborazione volontaria e in modo trasparente con la Prefettura di Torino e il Gruppo Interforze al fine di prevenire/ contrastare i rischi da infiltrazione mafiosa, la stessa individuerà – tempo per tempo – i soggetti delegati ad interloquire con le Autorità.

Questi ultimi acquisiranno le informazioni e la documentazione da condividere di volta in volta con la Prefettura ed il Gruppo Interforze (atti di disposizione, acquisto o pagamento effettuati e ricevuti; incarichi professionali conferiti, ovvero di amministrazione o di gestione fiduciaria ricevuti, per un valore condiviso con la Prefettura, nonché tutti gli atti rispondenti ai parametri indicati dal Prefetto; utilizzo di un conto corrente all'uopo dedicato per determinati atti indicati dal Prefetto; finanziamenti, in qualsiasi forma, eventualmente erogati da parte dei soci o di terzi; contratti di associazione in partecipazione eventualmente stipulati) ovvero le informazioni e la documentazione da sottoporre all'attenzione della Prefettura e/o del Gruppo Interforze al fine di ottenere informazioni di merito per i casi specifici in cui la Società abbia interesse a richiedere valutazioni che non possono trovare soddisfazione attraverso i controlli esercitabili da un'impresa privata, considerati i limiti normativi a cui risponde il sistema dei controlli interni.

Nell'adempimento delle attività di collaborazione volontaria, i soggetti deputati ad interloquire con le Autorità dovranno:

- Rispettare i principi comportamentali nei confronti della Pubblica Amministrazione;

- garantire che i rapporti con la Prefettura e con il Gruppo Interforze siano improntati alla massima collaborazione al fine di permettere a questi ultimi di espletare accertamenti e controlli di cui è incaricato;
- garantire, nella predisposizione e/o nell'invio di informazioni e/o documenti (relazioni, report, segnalazioni, ecc.), la massima trasparenza, veridicità, completezza, pertinenza, riservatezza, chiarezza e integrità delle informazioni, che devono essere altresì aggiornate;
- assicurare che gli adempimenti richiesti siano effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete e veritiere evitando, e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto di interesse, nonché modalità espositive che possano trarre in inganno la controparte;
- garantire la corretta archiviazione di tutta la documentazione prodotta e consegnata al fine di assicurare la completa tracciabilità delle varie fasi del processo.

Ai Destinatari sarà inoltre fatto esplicito divieto di:

- omettere le informazioni necessaria al corretto intendimento dei documenti condivisi con la Prefettura e con il Gruppo Interforze o dei fatti in essi riportati;
- tenere qualsiasi comportamento finalizzato ad assicurare un qualsiasi illecito vantaggio alla Società;
- effettuare promesse o indebite elargizioni di denaro, omaggi o altre utilità con la Prefettura e con il Gruppo Interforze o a persone a questi vicine al fine di promuovere o favorire i propri interessi o gli interessi della Società o anche per compensare o ripagare per un atto del suo ufficio, ovvero per conseguire l'esecuzione di un atto contrario ai doveri del suo ufficio;
- presentare dichiarazioni non veritiere esibendo documenti in tutto o in parte non corrispondenti alla realtà;
- tenere condotte ingannevoli nei confronti delle Autorità tali da indurre quest'ultima in errori di valutazione nel corso dello svolgimento della propria attività;
- porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa, nel corso di processi civili, penali o amministrativi;

- porre in essere qualsiasi comportamento, anche attraverso interposta persona, finalizzato a influenzare l'indipendenza di giudizio dell'Autorità;
- occultare documenti ed informazioni richiesti dalla Prefettura e/o dal Gruppo Interforze, fornire documenti ed informazioni incompleti e fuorvianti, nonché ostacolare in qualsiasi modo lo svolgimento dell'attività di controllo da parte di questi ultimi;
- distruggere, manipolare o sottrarre documentazione che riguardi operazioni che abbiano o debbano avere riflessi contabili o fiscali o qualunque altro processo oggetto di controllo.

7. TRACCIABILITÀ E ARCHIVIAZIONE

Tutta la documentazione prodotta a supporto del processo di gestione dei rapporti con la Pubblica Amministrazione deve essere archiviata, in formato elettronico o cartaceo, a cura dei Responsabili degli Uffici interessati di RO.S.S. e delle Direzioni / Aree aziendali rilevanti di SITAF S.p.A., ciascuno per le parti di propria competenza.

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE B: GESTIONE DELLE ATTIVITÀ AMMINISTRATIVE

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Tenuta della contabilità e predisposizione del bilancio d'esercizio.
- Gestione degli adempimenti fiscali.
- Gestione dei rapporti infragruppo.
- Gestione dei rapporti con il Sindaco Unico e con la Società di Revisione.
- Gestione della finanza e della tesoreria.
- Gestione delle operazioni societarie straordinarie.
- Gestione delle locazioni passive;
- Gestione del trattamento delle informazioni rilevanti e privilegiate;
- Gestione di omaggi¹⁰ e liberalità.

Alla data di redazione del presente documento, le attività sensibili di: "tenuta della contabilità e predisposizione del bilancio di esercizio", "gestione degli adempimenti fiscali", "gestione dei rapporti con il Sindaco Unico e la Società di Revisione" sono svolte anche con il supporto della Società SITAF S.p.A. in forza di uno specifico contratto di service¹¹, che prevede:

- una descrizione sintetica delle attività esternalizzate;
- i criteri di determinazione dei compensi per i servizi resi.

3. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati di criminalità organizzata (art. 24-ter del D.Lgs. 231/01):
 - Associazione per delinquere;
 - Associazione di tipo mafioso anche straniera;
 - Scambio elettorale politico mafioso.

¹⁰ Gli omaggi vengono erogati in occasione delle festività natalizie o nel corso dell'esercizio, qualora si verifichino esigenze ed eventi particolari per elargizioni, a soggetti aventi finalità culturali, scientifiche o altre finalità meritorie. Alla data del presente documento, la Società non elargisce liberalità.

¹¹ Sottoscritto in data 17/12/2011 e in fase di revisione alla data di emissione del presente documento.

- Reati contro la Pubblica Amministrazione (art. 25 del D.Lgs. 231/01):
 - Reati corruttivi;
 - Concussione;
 - Induzione indebita a dare o promettere utilità;
 - Istigazione alla corruzione;
 - Traffico di influenze illecite.

- Reati Societari (art. 25-ter del D.Lgs. 231/01):
 - False comunicazioni sociali;
 - Impedito controllo;
 - Indebita restituzione dei conferimenti;
 - Illegale ripartizione di utili e riserve;
 - Illecite operazioni sulle azioni o quote sociali o della società controllante;
 - Operazioni in pregiudizio dei creditori;
 - Formazione fittizia del capitale;
 - Corruzione tra privati;
 - Istigazione alla corruzione tra privati;
 - Illecita influenza sull'Assemblea;
 - Aggiotaggio;
 - Market Abuse;
 - Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza.

- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies del D.Lgs. 231/01):
 - Ricettazione;
 - Riciclaggio;
 - Impiego di beni, denaro, utilità di provenienza illecita;
 - Autoriciclaggio.

- Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1 del D.Lgs. 231/01):
 - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti;
 - Trasferimento fraudolento di valori.

- Reati Monetari (art. 25 bis del D.Lgs 231/01):
 - Spendita e introduzione nello Stato, senza concerto di monete falsificate;
 - Spendita di monete falsificate ricevute in buona fede;
 - Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati;

- Uso di valori di bollo contraffatto e alterato.
- Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater del D.Lgs. 231/01):
 - Associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico;
 - Assistenza agli associati;
 - Delitti posti in essere in violazione di quanto previsto dall'art. 2 Convenzione Internazionale di New York, 9 dicembre 1999 per la repressione del finanziamento del terrorismo.
- Reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/01):
 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
 - Dichiarazione fraudolenta mediante altri artifici;
 - Emissione di fatture o documenti per operazioni inesistenti;
 - Occultamento o distruzione di documenti contabili;
 - Sottrazione fraudolenta al pagamento di imposte.

Si rimanda all'Allegato 1 del Modello (*"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"*) per una descrizione di dettaglio di ciascuna fattispecie richiamata.

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- osservare, nella gestione delle attività contabili, le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla Legge e dai principi contabili adottati;
- rispettare scrupolosamente, nell'attività di contabilizzazione dei fatti relativi alla gestione della Società, la normativa vigente, integrata, qualora esistenti, dai principi contabili aziendali, in modo tale che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- garantire la completezza, accuratezza e tempestività nella contabilizzazione delle scritture contabili di chiusura e delle poste valutative, ivi incluso il calcolo e la contabilizzazione delle imposte correnti e differite;
- assicurare che tutte le eventuali attività affidate in outsourcing siano regolate tramite formali contratti di servizio sottoscritti da soggetti dotati di adeguati poteri;
- assicurare che eventuali difficoltà di interpretazione sulle modalità di contabilizzazione e valutazione delle poste di bilancio siano preventivamente condivise con il Sindaco Unico al fine di individuare la modalità di trattamento più corretta ed idonea;

- assicurare la completezza e accuratezza del Reporting Package inviato ai fini del consolidamento;
- mantenere, nei confronti dell'attività di controllo attribuita agli organi sociali, di controllo ed alla Società di Revisione, un comportamento corretto, trasparente e collaborativo tale da permettere agli stessi l'espletamento della loro attività istituzionale;
- fornire all'Organo di Controllo e ai revisori libero e tempestivo accesso ai dati e alle informazioni richieste;
- fornire all'Organo di Controllo e ai revisori informazioni accurate, complete, fedeli e veritiere;
- assicurare che ogni operazione societaria sia condotta dalla Società nel pieno rispetto delle norme di legge o dei regolamenti applicabili;
- tenere un comportamento corretto, trasparente e collaborativo in tutte le attività finalizzate alla predisposizione di prospetti ed altre comunicazioni sociali finalizzati ad una operazione societaria, al fine di fornire ai soci ed ai terzi un'informativa veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società e dell'operazione stessa;
- 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;
- rispettare le normative vigenti in materia di fiscalità al fine di garantire la corretta determinazione e liquidazione delle imposte;
- garantire la tracciabilità del processo relativo alla trasmissione delle dichiarazioni fiscali alle Autorità competenti, da effettuarsi nel rispetto delle norme di legge e regolamenti, in virtù degli obiettivi di trasparenza e corretta informazione;
- verificare che tutte le transazioni contabili che partecipano alla determinazione dell'imponibile fiscale siano rilevate in modo veritiero, corretto e completo e nel rispetto dei principi di inerenza e competenza, nonché che siano supportate da idonee evidenze documentali che ne consentano una ricostruzione accurata;
- mantenere rapporti trasparenti e collaborativi con l'amministrazione finanziaria e tutte le autorità con cui si interfaccia la società in occasione di adempimenti e verifiche fiscali;
- garantire il monitoraggio delle scadenze fiscali, sulla base delle scadenze di legge previste e provvedere nel rispetto delle stesse all'effettuazione delle dichiarazioni fiscali e dei relativi pagamenti;
- operare nel rispetto della normativa vigente in materia di strumenti di incasso e pagamento, tracciabilità dei flussi finanziari e antiriciclaggio;
- effettuare i pagamenti solo a seguito di adeguato controllo e autorizzazione, e adeguata verifica dei documenti giustificativi (es. contratto, fattura, nota spesa, nota addebito) che devono corrispondere in termini di soggetto beneficiario, tempistiche e modalità di pagamento con quanto definito nel documento giustificativo stesso;

- assicurare la ricostruzione delle operazioni finanziarie attraverso l'identificazione della clientela e la conservazione dei dati in appositi archivi;
- garantire che i pagamenti siano gestiti attraverso un comportamento collaborativo, corretto e trasparente, nel rispetto delle norme di legge e delle procedure aziendali interne; assicurare, in caso di pagamenti a favore di soggetti terzi tramite bonifico bancario, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché della registrazione a sistema della relativa distinta;
- assicurare che sia sempre prevista la rilevazione e l'analisi di pagamenti/incassi ritenuti anomali per controparte, tipologia importo, oggetto, frequenza o entità sospette;
- assicurare che sia costantemente verificata la regolarità dei pagamenti effettuati, tramite strumenti di pagamento immateriali, con riferimento anche alla coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- utilizzare in via preferenziale il canale bancario nell'effettuazione delle operazioni di incasso e pagamento. L'effettuazione di incassi e di pagamenti in contanti deve essere limitata ai soli casi espressamente consentiti, nei limiti delle necessità aziendali e comunque per importi di modico valore e nel rispetto dei limiti previsti dalla normativa vigente in materia di strumenti di pagamento, facendo ricorso a conti correnti inattivi o poco movimentati solo in casi eccezionali adeguatamente motivati;
- disporre pagamenti congrui con la documentazione sottostante (es. fattura autorizzata), assicurandosi di effettuare il pagamento su un conto corrente effettivamente riconducibile al fornitore e nel Paese in cui il fornitore ha sede o ha prestato i propri servizi;
- utilizzare conti correnti c.d. "temporanei" unicamente per lo svolgimento di operazioni strumentali / funzionali alle attività proprie di business (quali, a titolo di esempio, operazioni di copertura);
- assicurare che la Società non apra conti correnti all'estero in Paesi considerati paradisi fiscali;
- verificare periodicamente la presenza di conti inattivi o poco utilizzati ed eventuali operazioni anomale su tali conti;
- effettuare un'analisi periodica dei soggetti aziendali formalmente delegati a compiere operazioni su conti correnti della Società;
- verificare periodicamente la bontà delle fidejussioni e delle garanzie assicurative in essere (che potrebbero rappresentare lo strumento per impiegare denaro proveniente da attività illecite al fine di ostacolarne la provenienza delittuosa) anche al fine di verificarne la necessità ai fini dell'esecuzione dell'attività di business;
- assicurare che ogni operazione infragruppo avvenga secondo criteri di correttezza, liceità e trasparenza, secondo condizioni in linea con quelle di mercato, sulla base di valutazioni di reciproca convenienza economica e avendo riguardo al comune obiettivo di creare valore per l'intero Gruppo;

- operare nel rispetto della normativa vigente in materia di gestione delle informazioni privilegiate;
- assicurare la riservatezza in merito alle informazioni ed ai documenti acquisiti nell'ambito della loro funzione;
- assicurare che la comunicazione all'esterno delle informazioni che rivestono carattere di riservatezza e confidenzialità avvenga esclusivamente da parte di personale autorizzato, in conformità alle vigenti disposizioni e con l'osservanza dei principi della parità e della contestualità dell'informativa.

È inoltre espressamente **vietato**:

- rappresentare in contabilità - 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;
- registrare in contabilità operazioni a valori non corretti rispetto alla documentazione di riferimento, oppure a fronte di transazioni soggettivamente o oggettivamente inesistenti in tutto o in parte, o senza un'adeguata documentazione di supporto che ne consenta una corretta rilevazione contabile e successivamente una ricostruzione accurata;
- omettere di comunicare dati ed informazioni previsti dalla normativa vigente o dalle procedure e prassi interne sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere di segnalare/denunciare eventuali registrazioni illegittime, non corrette, false o che corrispondano a operazioni sospette o in conflitto di interessi;
- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio mediante utilizzo di fatture per operazioni inesistenti emesse da terzi), ovvero finalizzate alla creazione di "fondi neri" o di "contabilità parallele";
- alterare o distruggere documenti ed informazioni finanziarie e contabili disponibili in formato cartaceo e/o elettronico;
- fruire di regimi fiscali speciali ovvero di esenzioni o detrazioni nella consapevolezza dell'assenza dei presupposti normativi (soggettivi e oggettivi), attraverso l'alterazione dei documenti contabili o la dissimulazione delle sottostanti condizioni fattuali;
- compensare crediti d'imposta inesistenti o in misura superiore a quella spettante dall'effettivo calcolo;
- omettere di comunicare dati e informazioni imposti dalla legge riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale previsti dalla legge;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- ripartire riserve nei casi in cui ciò non sia consentito dalla legge;

- acquistare o sottoscrivere azioni/quote della Società e/o delle sue controllanti fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- aumentare in modo fittizio il capitale sociale, attribuendo azioni/quote per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- effettuare operazioni straordinarie in violazione delle disposizioni di legge a tutela dei creditori;
- diffondere, attraverso qualsiasi canale di comunicazione, informazioni, voci o notizie correlate alla gestione delle operazioni societarie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla Società o al Gruppo in generale;
- predisporre e inviare dichiarazioni fiscali alle Autorità competenti, contenenti dati falsi, artefatti, incompleti o non rispondenti al vero;
- indicare, al fine di evadere le imposte sui redditi o sul valore aggiunto, nelle dichiarazioni relative a dette imposte, elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o inesistenti o crediti e ritenute fittizie;
- omettere dichiarazioni / comunicazioni di natura fiscale, dovute per legge, al fine di evadere le imposte;
- effettuare operazioni in paesi in "black list" o a fiscalità privilegiata;
- porre in essere comportamenti che ostacolano lo svolgimento delle attività di controllo da parte del Sindaco Unico e della Società di Revisione, mediante l'occultamento di documenti ed informazioni richiesti, ovvero fornendo documenti ed informazioni incompleti, non chiari o fuorvianti;
- promettere o offrire somme di denaro o altra utilità, sotto qualsiasi forma (compresi gli omaggi), ai sindaci ed ai rappresentanti/dipendenti della Società di Revisione con la finalità di favorire gli interessi della Società;
- effettuare operazioni infragruppo in maniera "anomala" al fine di impiegare, sostituire o trasferire disponibilità finanziarie provenienti da delitti non colposi, in modo da ostacolare concretamente l'identificazione della loro provenienza illecita;
- porre in essere operazioni infragruppo fittizie o non adeguatamente giustificate o prive della necessaria formalizzazione in specifici contratti e ordini autorizzati e sottoscritti da soggetti dotati di idonei poteri;
- effettuare operazioni infragruppo con pagamenti non adeguatamente documentati e autorizzati o in contanti o utilizzare conti o libretti di risparmio in forma anonima o con intestazione fittizia o aperti presso filiali in Paesi esteri ove ciò non sia correlato alla sottostante operazione;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi di denaro di rilevante entità;

- corrispondere od offrire/promettere pagamenti o elargizioni di denaro a soggetti pubblici o privati o a persone a questi vicini, per assicurare vantaggi di qualunque tipo alla Società;
- corrispondere od offrire, direttamente o indirettamente, pagamenti o benefici materiali a rappresentanti e dipendenti di istituzioni bancarie e finanziarie o a persone a questi vicini, per influenzare il loro comportamento ed assicurare vantaggi di qualunque tipo alla Società;
- dare seguito a richieste indebite di denaro o altri benefici provenienti da qualunque persona. In tali casi, il dipendente deve informare tempestivamente il proprio superiore e sospendere ogni rapporto con il richiedente;
- trasferire a qualsiasi titolo denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore alla soglia indicata dalla normativa vigente;
- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e/o in Paesi esteri inseriti nelle principali black list;
- emettere assegni bancari o postali che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare bonifici, anche internazionali, senza indicazione esplicita della controparte;
- disporre pagamenti o incassare denaro verso/da Paesi inseriti nelle principali black list internazionali che non trovino adeguata giustificazione (ad esempio in caso di controparti che abbiano sede in tali Paesi);
- re-immettere nel circuito monetario banconote o monete falsificate, o anche semplicemente sospette di falsificazione. Tali banconote devono essere trattenute e consegnate ad un istituto di credito;
- frazionare artificiosamente un'operazione / transazione al fine di eludere le normative applicabili;
- impiegare, sostituire o trasferire disponibilità finanziarie provenienti da delitto, in modo da ostacolare l'identificazione della loro provenienza delittuosa;
- effettuare transazioni finanziarie fuori mercato, ovvero a condizioni che differiscono in modo sostanziale da quelle prevalenti sul mercato al momento in cui la transazione è posta in essere;
- richiedere, ove non fosse strettamente necessario ai fini dell'esecuzione dell'attività di business, finanziamenti assistiti da garanzie reali o personali da parte di persone fisiche o giuridiche residenti in paesi non collaborativi;
- porre in essere operazioni immobiliari finalizzate a impiegare, sostituire o trasferire denaro, beni o altra utilità provenienti da delitto non colposo ostacolandone l'identificazione della provenienza illecita;
- diffondere, attraverso qualsiasi canale di comunicazione, informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o

anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla compagine azionaria quotata.

5. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

5.1. Tenuta della contabilità e predisposizione del bilancio d'esercizio

Gestione dei profili di accesso al sistema contabile e del piano dei conti

Il sistema di contabilità generale è accessibile tramite credenziali composte di User ID e password personali e garantisce la tracciabilità delle azioni svolte al proprio interno, consentendo l'identificazione dell'utente che ha effettuato le registrazioni.

La definizione dei profili di accesso e l'assegnazione agli utenti di User ID e password, nonché la manutenzione periodica degli stessi, è affidata operativamente al Responsabile AFC di SITAF S.p.A., sulla base delle autorizzazioni alla creazione / cancellazione / modifica del profilo utente di volta in volta rilasciate dal Responsabile dell'Ufficio Amministrazione, Finanza e Controllo.

La gestione del piano dei conti della società è interamente demandata all'Area Amministrazione, Finanza e Controllo di Gestione della Capogruppo SITAF S.p.A.

Predisposizione del bilancio di esercizio

Il calendario interno per il completamento delle attività di chiusura contabile è predisposto dal Dirigente Ufficio Amministrazione, Finanza e Controllo e condiviso con i Responsabili di Uffici rilevanti, nel rispetto delle scadenze contabili imposte dalla Capogruppo SITAF S.p.A. Entro questi termini, il Responsabile Ufficio Amministrazione, Finanza e Controllo di RO.S.S. provvede a raccogliere tutta la documentazione rilevante per la chiusura contabile e trasmetterla all'Area Amministrazione, Finanza e Controllo di Gestione di SITAF S.p.A.

La gestione delle registrazioni contabili di chiusura (e.g. rettifiche, stanziamenti) è interamente demandata all'Area Amministrazione, Finanza e Controllo di Gestione di SITAF S.p.A., che successivamente si occupa della redazione del bilancio d'esercizio entro i termini previsti per legge.

Il progetto di bilancio viene sottoscritto per approvazione dall'Amministratore Delegato prima della trasmissione al Consiglio di Amministrazione.

5.2. Gestione degli adempimenti fiscali

La gestione degli adempimenti fiscali di RO.S.S. è demandata ad uno studio esterno, che a sua volta si avvale anche del supporto del Responsabile Area Amministrazione, Finanza e Controllo di Gestione di SITAF S.p.A.

Il contratto sottoscritto con lo studio esterno include una clausola risolutoria ex D.Lgs. 231/01, con la quale la controparte dichiara di conoscere il contenuto del D.Lgs. 231/2001 e si impegna ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto medesimo, nonché a rispettare i principi di comportamento richiamati dal Codice Etico di RO.S.S..

Per quanto riguarda la gestione della fiscalità, la Capogruppo SITAF S.p.A. non procede ad attività di consolidamento nei confronti delle proprie controllate, pertanto RO.S.S. provvede direttamente al versamento delle imposte. Tutta la documentazione presentata all'amministrazione finanziaria è sottoscritta dall'Amministratore Delegato o da soggetto da questo delegato, nel rispetto del sistema di deleghe e procure in essere.

5.3. Gestione dei rapporti infragruppo

Tutti i rapporti infragruppo sono disciplinati da appositi contratti, che definiscono puntualmente l'oggetto della prestazione e i corrispettivi dovuti per le prestazioni rese.

I contratti infragruppo sono sottoscritti dall'Amministratore Delegato e contengono una clausola risolutoria ex D.Lgs. 231/01, con la quale la controparte dichiara di conoscere il contenuto del D.Lgs. 231/2001 e si impegna ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto medesimo, nonché a rispettare i principi di comportamento richiamati dal Codice Etico di RO.S.S..

Nella gestione dei contratti infragruppo, gli Uffici di volta in volta competenti garantiscono la tracciabilità dell'effettivo svolgimento dei servizi infragruppo prestati o goduti, attraverso la formalizzazione e archiviazione di apposita documentazione a supporto delle attività di monitoraggio (a titolo esemplificativo e non esaustivo: scambi di mail, file di riepilogo dei servizi, dei costi associati e di eventuali modalità di ripartizione degli stessi, etc.).

Al ricevimento delle fatture da parte della controparte, gli Uffici di volta in volta competenti svolgono attività di verifica circa l'effettività e la congruità delle prestazioni in relazione alle quali le fatture sono state rilasciate, con il coinvolgimento, ove necessario, delle strutture aziendali che hanno usufruito della prestazione al fine di acquisire attestazione dell'effettivo svolgimento della stessa e della sua rispondenza all'oggetto del contratto.

5.4. Gestione dei rapporti con il Sindaco Unico e la Società di Revisione

La gestione dei rapporti con il Sindaco Unico è demandata al Responsabile Area Amministrazione, Finanza e Controllo di RO.S.S. e al Responsabile Area Societario e Compliance di SITAF S.p.A., ognuno per la parte di propria competenza, con il supporto del Responsabile Ufficio Amministrazione, Finanza e Controllo di SITAF.

I rapporti con la Società di Revisione nel corso delle verifiche periodiche sono intrattenuti dal Responsabile Area Amministrazione, Finanza e Controllo di RO.S.S. S.p.A., che si avvale del supporto del Responsabile Ufficio Amministrazione, Finanza e Controllo di SITAF.

Tutte le Funzioni aziendali interessate hanno la responsabilità di agire con la massima correttezza e trasparenza, rispondendo alle richieste informative di carattere ordinario e straordinario avanzate.

Le risultanze delle attività di verifica svolte dal Sindaco Unico vengono sintetizzate in specifici verbali, trascritti nel Libro del Sindaco Unico e sottoscritti per approvazione dallo stesso.

Per quanto concerne le attività di verifica svolte dalla Società di Revisione, il Responsabile Ufficio Amministrazione, Finanza e Controllo di RO.S.S. archivia le relazioni rilasciate.

5.5. Gestione della finanza e della tesoreria

Gestione dei conti correnti

I rapporti con le banche/istituti finanziari e postali sono gestiti con il supporto dalla Direzione Finanza Centrale, responsabile della selezione della controparte bancaria e della definizione delle condizioni applicate.

L'autorizzazione all'apertura o alla chiusura di un conto corrente bancario o postale è di competenza esclusiva dell'Amministratore Delegato, mentre la gestione della attività operative di apertura, gestione o chiusura è di competenza del Responsabile Ufficio Amministrazione, Finanza e Controllo di RO.S.S..

Le riconciliazioni bancarie o postali sono effettuate con cadenza mensile a cura del Responsabile dell'Ufficio Amministrazione, Finanza e Controllo di Sitaf.

Gestione degli incassi

La contabilizzazione degli incassi avviene a cura dell'Area Amministrazione, Finanza e Controllo di Gestione di SITAF S.p.A., sulla base degli estratti conto ricevuti, con cadenza mensile, da parte del Responsabile Ufficio Amministrazione, Finanza e Controllo di RO.S.S..

Gestione dei pagamenti

Tutti i pagamenti, supportati da adeguata documentazione autorizzativa, sono effettuati tramite bonifico bancario attraverso i portali di web-banking delle banche, cui hanno accesso esclusivamente l'Amministratore Delegato e il Responsabile Ufficio Amministrazione, Finanza e Controllo di RO.S.S., ciascuno in possesso di credenziali di accesso nominative e separate.

Prima di procedere con il pagamento delle fatture, il Responsabile Ufficio Amministrazione, Finanza e Controllo verifica che queste siano state autorizzate da parte del Responsabile dell'Ufficio richiedente, tramite firma apposta sui documenti stessi.

Prima di poter effettuare il pagamento delle fatture, il Responsabile Ufficio Amministrazione, Finanza e Controllo richiede formale autorizzazione all'Amministratore Delegato, nei limiti di quanto previsto dal sistema di deleghe e procure vigente.

Gestione degli incassi e dei pagamenti tramite strumenti di pagamento diversi dal contante

Le operazioni di incasso e pagamento che avvengono tramite strumenti di pagamento offerti da intermediari autorizzati¹², carte di pagamento “a spendibilità limitata” (c.d. “strumenti privativi”)¹³, servizi di pagamento in Internet (c.d. “e-payments”) ovvero pagamenti riscossi tramite l'utilizzo di dispositivi portatili telefono cellulare o altro dispositivo mobile (es. tablet) (c.d. “m-payments”) devono avvenire nel rispetto dei protocolli di sicurezza previsti dalla normativa di settore.

È fatto espresso divieto di estrapolare dati inerenti agli stessi strumenti in tutte le fasi del processo di incasso (sia ordine di pagamento emesso che gestione all'interno del relativo circuito che consente lo scambio dell'informazione di pagamento tra prestatori di servizi e accreditamento al beneficiario, quest'ultimo, in particolare, nel caso in cui sia nella disponibilità della Società).

È inoltre fatto divieto di utilizzare credenziali, dati o supporti di titolarità di terzi per operazioni di pagamento non autorizzate dai legittimi titolari e/o comunque ad insaputa degli stessi.

Si ricorda che la raccolta, il trattamento e la conservazione dei dati inerenti a tali strumenti di pagamento deve avvenire nel rispetto dei principi di liceità, correttezza, trasparenza, esattezza, integrità e riservatezza, limitazione delle finalità, e minimizzazione dei dati di cui all'art. 5 del Regolamento (UE) 2016/679 (GDPR).

È fatto espresso divieto:

- di utilizzare indebitamente e non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi;
- falsificare o alterare carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi;

¹² Ovvero, carta di credito o carta di debito rilasciata da banche, istituti di pagamento, istituti di moneta elettronica, Poste.

¹³ Ci si riferisce a carte di pagamento utilizzabili esclusivamente: a) presso l'emittente per i beni e servizi da lui forniti (es. pedaggi autostradali e gift card); oppure b) presso una rete definita di esercizi commerciali, ovvero per l'acquisto di una gamma ristretta di beni e servizi (es. carte carburante). Per questa loro caratteristica tali carte possono essere emesse da soggetti non vigilati, i quali - nei casi in cui il valore complessivo delle operazioni di pagamento eseguite con tali strumenti superi la soglia di 1 milione di euro - compaiono nell'apposita appendice dell'albo di vigilanza degli Istituti di pagamento, assieme ai fornitori di reti o servizi di comunicazione elettronica (che consentono agli utenti di effettuare talune operazioni di pagamento addebitandole alla relativa fattura o a un conto pre-alimentato).

- possedere, cedere o acquisire le predette carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;
- alterare in qualsiasi modo il funzionamento dei sistemi, informatici o telematici, di pagamento ovvero ancora intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti;
- installare sistemi (HW e/o SW idonei a intercettare dati inerenti a sistemi di pagamento diversi dal contante;
- abusare di dati o informazioni di sistemi di pagamento diversi dal contante in generale e, in particolare, al fine di effettuare per pagamenti non autorizzati dal legittimo titolare o a sua insaputa.

Gestione dei pagamenti tramite carte ricaricabili

La Società possiede delle carte ricaricabili, intestate ai Responsabili degli Uffici, poggianti su conto corrente aziendale ed utilizzabili per acquisti di modico valore. Tali carte possono essere ricaricate esclusivamente da parte del Responsabile Amministrativo di RO.S.S. previa autorizzazione dell'AD, che archivia copia della ricevuta di avvenuta ricarica.

Salvo situazioni di emergenza, che devono essere autorizzate e supportate da adeguata documentazione giustificativa, le carte ricaricabili non sono utilizzate per l'acquisto di carburante dei mezzi di servizio. A tale scopo, infatti, la Società si avvale di convenzioni dedicate con le società petrolifere al fine di gestire al meglio l'acquisto tramite carte carburante associate alle targhe dei singoli veicoli e garantire la tracciabilità di ogni operazione di rifornimento per ogni mezzo.

I dipendenti sono tenuti a consegnare al Responsabile Ufficio Amministrazione, Finanza e Controllo di RO.S.S. tutti i giustificativi delle spese effettuate tramite carte ricaricabili, affinché possa svolgere dei controlli puntuali sulla coerenza degli acquisti effettuati e la corrispondenza tra gli estratti conto delle carte e i giustificativi presentati.

Monitoraggio flussi finanziari

Per quanto concerne le modalità operative e di gestione per ottemperare agli obblighi di tracciabilità dei flussi finanziari previsti nell'ambito dei contratti pubblici dagli artt. 3 e 6 della Legge n. 136/2010 e della Delibera ANAC n. 556 del 31/05/2017, sono definite le attività da attuare e le relative responsabilità per ottemperare in maniera adeguata ai due pilastri fondamentali della normativa sulla tracciabilità:

1. Comunicazione all'Ente Appaltante dei conti correnti dedicati;
2. Obbligo di indicazione dei codici di tracciabilità Codice Identificativo Gara (CIG) e Codice Unico di Progetto (CUP) nei documenti fiscali e contrattuali e nella singola transazione finanziaria tracciabile.

In particolare, nel contratto di appalto (o documento equipollente) devono essere correttamente riportati i codici CIG/CUP, coerenti con quelli riportati nella documentazione di gara, nonché le clausole contrattuali previste dal “Protocollo Operativo per il Monitoraggio Finanziario”.

In ciascun ordine di acquisto (o conferma d'ordine) sono riportati i codici CIG e CUP della commessa.

Prima di procedere ai pagamenti a mezzo bonifico e/o ricevuta bancaria, viene verificato il corretto inserimento - nella fattura del fornitore e nella causale della transazione finanziaria - dei codici CIG/CUP.

Per le transazioni rese da subappaltatori e/o sub-affidatari, viene verificato che il conto corrente indicato in fattura sia stato preliminarmente e correttamente comunicato e dedicato (in caso contrario ottiene chiarimenti e/o aggiornamenti da parte del fornitore).

È fatto obbligo altresì rispettare quanto previsto dai Protocolli di Legalità applicabili in merito alla gestione dei flussi finanziari relativi all'appalto.

Gestione della cassa contante

La Società possiede una cassa contante contenuta gestita dall'ufficio AFC di RO.S.S., utilizzabile per l'effettuazione di spese di modico valore (e.g. minuterie, piccole spese con carattere di urgenza). La giacenza della cassa contante è allineata alle effettive esigenze operative della Società.

Tutti i reintegri di cassa sono supportati da adeguata documentazione giustificativa (scontrino emesso al momento del prelievo di contanti), che deve essere verificata e conservata a cura del Responsabile Ufficio Amministrazione, Finanza e Controllo. La cassa contante può essere reintegrata solo da specifici soggetti aziendali, autorizzati ad effettuare un prelievo dal conto corrente della Società e diversi da chi effettua le riconciliazioni di cassa e le verifiche di conformità dei giustificativi di spesa.

Nell'effettuare spese per cassa, la Società garantisce il pieno rispetto della normativa vigente in materia di antiriciclaggio, ponendo particolare attenzione all'ammontare massimo ammesso per le transazioni in contanti.

Mensilmente, il Responsabile Ufficio Amministrazione, Finanza e Controllo effettua una conta fisica dei valori di cassa ai fini della riconciliazione con il relativo saldo contabile e trasmette copia del prospetto di riconciliazione firmato all'Area Amministrazione, Finanza e Controllo di Gestione di SITAF S.p.A. per le registrazioni contabili di competenza.

Gestione dei crediti

La rinuncia a crediti è riservata all'organo dirigente o all'Amministratore Delegato.

5.6. Gestione di omaggi e liberalità

Nella gestione di omaggi e liberalità devono essere rispettati i seguenti principi comportamentali:

- rispettare il Codice etico e i principi comportamentali nei confronti della Pubblica Amministrazione e anticorruzione;
- effettuare liberalità e sponsorizzazioni solo se esse risultino a sostegno di organizzazioni/eventi rispettabili nonché nell'osservanza di leggi e regolamenti locali e non vi siano conflitti di interessi o persone esposte politicamente nell'ambito dell'ente beneficiario; tale verifica viene svolta attraverso analisi dei dati inerenti i beneficiari economici, soci e/o amministratori degli enti beneficiari attraverso documentazione da questi ultimi rese o informazioni provenienti da banche dati pubbliche (GOOGLE, CCIAA, ecc.);
- tenere comportamenti di ospitalità e promozione che rientrano nella prassi di normale conduzione degli affari, dunque non eccedenti rispetto alle normali pratiche commerciali o di cortesia;
- garantire la congruità, adeguatezza e documentabilità dell'attivazione di ogni sponsorizzazione o erogazione liberale;
- garantire la trasparenza e tracciabilità dell'operazione, registrando le operazioni secondo gli adempimenti amministrativo-contabili di rito;
- conservare la documentazione prodotta e quella ricevuta.

Con riferimento a rapporti di sponsorizzazione, donazione e altre liberalità si devono rispettare le norme fiscali e tributarie. Le operazioni dovranno avere adeguata rappresentazione contabile, con registrazioni veritiere, supportate e tempestive.

In caso di dubbio dovranno essere acquisiti pareri da parte di esperti e le operazioni dovranno essere condivise con la Società di revisione.

È inoltre espressamente **vietato**:

- promettere o offrire omaggi, sponsorizzazioni, donazioni o altre liberalità, anche sotto pressione psicologica o coercizione, anche se indirettamente, per tramite di interposta persona, a soggetti appartenenti alla Pubblica Amministrazione o controparti private o a soggetti da questi segnalati con la finalità, anche implicita, di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;
- elargire omaggi che possano essere interpretati come eccedenti le normali pratiche commerciali o di cortesia;
- promettere o effettuare omaggi per finalità diverse da quelle istituzionali;
- erogare omaggi, sponsorizzazioni o liberalità qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione di uno dei reati disciplinati dal D.Lgs. 231/2001.

5.7. Gestione delle operazioni societarie straordinarie

Tutte le operazioni societarie straordinarie sono di competenza del Consiglio di Amministrazione della Società.

Preventivamente ad ogni operazione straordinaria, l'Amministratore Delegato con il supporto del Responsabile Ufficio Amministrazione, Finanza e Controllo e delle Unità Organizzative/Funzioni aziendali di volta in volta competenti, predispone, ove necessario, tutta la documentazione necessaria per istruire e valutare la fattibilità dell'operazione, eventualmente con l'ausilio di consulenti esterni competenti in materia fiscale, amministrativa, legale e societaria..

Ove necessario, l'Amministratore Delegato richiede eventuali pareri a consulenti terzi.

L'operazione, una volta definita in tutti i suoi aspetti e corredata della necessaria documentazione, è sottoposta all'esame ed approvazione del Consiglio di Amministrazione e/o dell'Assemblea dei Soci nel rispetto delle vigenti disposizioni normative, statutarie e regolamentari.

5.8. Gestione delle locazioni passive

Gli immobili da prendere e/o concedere in locazione sono individuati a cura dell'Ufficio Tecnico e sottoposti all'approvazione dell'Amministratore Delegato.

Le valutazioni tecniche ed economiche svolte ai fini della selezione dell'immobile prevedono sempre il coinvolgimento dei soggetti preposti alla gestione della sicurezza sul lavoro, al fine di garantire che siano tenuti in considerazione i requisiti necessari per il rispetto della normativa in materia. Gli esiti delle valutazioni sono formalizzati in una relazione interna.

Il rapporto tra le parti è regolato tramite contratto formale sottoscritto dall'Amministratore Delegato o da soggetto da questo delegato. Nel caso in cui il contratto di locazione abbia durata superiore a 9 anni, questo deve essere sottoposto all'approvazione del Consiglio di Amministrazione.

Qualora la Società intenda avvalersi di professionisti esterni, ad esempio per l'effettuazione di perizie sugli immobili oggetto di valutazione, il rapporto tra le parti è regolato tramite contratto sottoscritto per approvazione dall'Amministratore Delegato o da soggetto da questo delegato, inclusivo di clausola risolutoria ex D.Lgs. 231/01 con cui la controparte dichiara di conoscere il contenuto del D.Lgs. 231/2001 e si impegna ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto medesimo, nonché a rispettare i principi di comportamento richiamati dal Codice Etico di RO.S.S..

5.9. Gestione delle informazioni rilevanti e privilegiate

La comunicazione o l'invio a terzi di informazioni o documenti riservati deve essere effettuata nel rispetto delle clausole di riservatezza inserite nei contratti che regolano i rapporti con i terzi, ovvero previa sottoscrizione, da parte del richiedente a cui è consegnata copia del documento societario riservato richiesto, di una dichiarazione con cui lo stesso si obbliga alla riservatezza rispetto alla circolazione del documento ricevuto in copia e al trattamento delle informazioni ivi contenute.

Dichiarazioni ufficiali e rapporti con la stampa finalizzati alla divulgazione di documenti o alla diffusione di informazioni su fatti rilevanti riguardanti la Società devono avvenire esclusivamente per il tramite del Presidente e/o dell'Amministratore Delegato.

Il personale di RO.S.S., a qualsiasi titolo coinvolto nelle attività di cui al presente processo, è tenuto a osservare i principi di comportamento ed i presidi di controllo esposti nel presente documento, le prescrizioni di legge esistenti in materia, nonché le norme comportamentali richiamate nel Codice Etico

Le informazioni e notizie che potenzialmente possono presentare il carattere di privilegiate per la Capogruppo ASTM S.p.A. - dovranno essere comunicate tempestivamente dall'Amministratore Delegato di RO.S.S., all'Amministratore Delegato di ASTM per consentire la corretta valutazione dell'informazione nonché di adempiere agli obblighi di comunicazione previsti dalla normativa vigente.

I Destinatari del suddetto Processo sono personalmente responsabili della custodia della documentazione inerente all'Informazione Privilegiata cui hanno accesso e ne curano la conservazione garantendone la riservatezza.

5.10. Gestione dei conflitti di interesse in capo agli Amministratori

Il presente paragrafo disciplina i comportamenti che devono essere tenuti in caso di operazioni nelle quali uno o più amministratori di RO.S.S. siano portatori di un qualsiasi interesse, anche potenziale, per conto proprio o di terzi, non solo in conflitto, ma anche concorrente con l'interesse sociale della Società ma in contrapposizione a quest'ultimo.

In particolare, ricorre un interesse dell'Amministratore ogni qual volta questi possa trarre dall'operazione societaria, per sé o per altri, una qualunque utilità, anche di natura non strettamente patrimoniale, indipendentemente dagli effetti di tale operazione per la Società. Con l'espressione "interesse per conto di terzi" si intende, fra l'altro, un interesse nascente da rapporti giuridicamente rilevanti, ivi incluse eventuali cariche ricoperte in altri Enti ovvero le relazioni di convivenza e i rapporti sociali di fatto, potenzialmente in grado di influenzare l'Amministratore e di indurlo a privilegiare interessi extrasociali.

In presenza di un interesse, come sopra definito, deve essere tenuto il seguente comportamento:

- Qualora l'operazione sia soggetta all'approvazione del C.d.A. della Società, l'Amministratore portatore di un interesse deve informare tempestivamente ed esaurientemente il C.d.A. e il Sindaco Unico prima dell'inizio della discussione consiliare, specificando la natura, i termini, l'origine e la portata dell'interesse sottostante (anche se potenziale o per conto di terzi), e deve allontanarsi dalla riunione consiliare al momento della discussione e della conseguente delibera.
- Qualora l'operazione rientri nei poteri dell'Amministratore con deleghe, portatore di un interesse, quest'ultimo si astiene dal compiere l'operazione, sottoponendola ad approvazione del C.d.A..
- In entrambi i suddetti casi, la delibera del C.d.A. dovrà contenere adeguata motivazione delle ragioni e della convenienza dell'operazione per la Società.

Nel caso in cui:

- I. gli Amministratori interessati siano stati inadempienti al loro obbligo di dare notizia del loro interesse all'operazione, o abbiano dato una notizia incompleta e priva delle caratteristiche indicate; oppure
- II. l'informativa sia stata data in modo adeguato, ma il Consiglio sia inadempiente rispetto all'obbligo di adeguata motivazione sulle ragioni e sulla convenienza dell'operazione; oppure
- III. gli Amministratori siano stati inadempienti ad uno o entrambi i propri obblighi di valutare con diligenza e senza conflitti di interessi l'opportunità e la convenienza per la società di compiere l'operazione,

l'Amministratore risponde dei danni derivati alla Società dalla sua azione od omissione.

L'Amministratore risponde altresì dei danni che siano derivati alla Società dalla utilizzazione a vantaggio proprio o di terzi di dati, notizie o opportunità di affari appresi nell'esercizio del suo incarico.

6. TRACCIABILITÀ E ARCHIVIAZIONE

Tutta la documentazione prodotta a supporto del processo di gestione delle attività amministrative è archiviata presso l'Ufficio Amministrazione, Finanza e Controllo di RO.S.S. e presso l'Area Amministrazione, Finanza e Controllo di Gestione di SITAF, per le parti di competenza.

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE C: SELEZIONE E GESTIONE DEL PERSONALE

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Selezione e assunzione del personale.
- Gestione di livelli retributivi, avanzamenti di carriera, riconoscimenti *ad personam*.
- Assegnazione e gestione dei beni aziendali.
- Gestione dei rimborsi spese e delle spese di rappresentanza.
- Elaborazione paghe e contributi.
- Predisposizione e trasmissione della documentazione necessaria per l'ottenimento di finanziamenti pubblici / contributi agevolati per la realizzazione di corsi di formazione.
- Gestione dei rapporti con le Organizzazioni Sindacali.

Il processo di selezione del personale del Gruppo SITAF è disciplinato dalla Procedura "Reclutamento del personale Infragruppo SITAF SPA e Società Controllate", approvata dal Consiglio di Amministrazione della Capogruppo SITAF in data 06 giugno 2018 e divulgata con apposita comunicazione a tutte le Società controllate da parte del Direttore Risorse Umane di SITAF.

3. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati contro la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01):
 - Reati corruttivi;
 - Concussione;
 - Induzione indebita a dare o promettere utilità;
 - Istigazione alla corruzione;
 - Indebita percezione di erogazioni, truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee o per il conseguimento di erogazioni pubbliche;
 - Malversazione di erogazioni pubbliche;
 - Traffico di influenze illecite;
 - Peculato.

- Reati Societari (art. 25-ter del D.Lgs. 231/01):
 - Corruzione tra privati;
 - Istigazione alla corruzione tra privati;
 - False comunicazioni sociali;
 - Impedito controllo.
- Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare (art. 25-duodecies del D.Lgs. 231/01):
 - Impiego di lavoratori il cui soggiorno è irregolare;
 - Disposizioni contro l'immigrazione clandestina.
- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies del D.Lgs. 231/01):
 - Riciclaggio;
 - Impiego di beni, denaro, utilità di provenienza illecita;
 - Autoriciclaggio.
- Reati di criminalità organizzata (art. 24 ter del D.Lgs. 231/01):
 - Associazione per delinquere;
 - Associazione di tipo mafioso anche straniera.
- Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater del D.Lgs. 231/01):
 - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico;
 - Delitti posti in essere in violazione di quanto previsto dall'art. 2 Convenzione Internazionale di New York, 9 dicembre 1999 per la repressione del finanziamento del terrorismo.
 - Assistenza agli associati.
- Reati contro la personalità individuale (art. 25-quinquies del D.Lgs 231/01)
 - Riduzione o mantenimento in schiavitù o servitù;
 - Intermediazione illecita e sfruttamento del lavoro.
- Reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/01):
 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
 - Dichiarazione fraudolenta mediante altri artifici;
 - Occultamento o distruzione di documenti contabili;
 - Sottrazione fraudolenta al pagamento di imposte.

Si rimanda all'Allegato 1 del Modello (*"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"*) per una descrizione di dettaglio di ciascuna fattispecie richiamata.

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- rispettare le normative sul lavoro vigenti (ad esempio in termini di contributi previdenziali e assistenziali, permessi di soggiorno, ecc.);
- assicurare condizioni di lavoro rispettose della dignità personale, delle pari opportunità, nonché un ambiente di lavoro adeguato;
- operare nel rispetto del criterio di meritocrazia e nel rispetto delle reali esigenze della Società;
- verificare preventivamente le informazioni disponibili sui candidati al fine di instaurare rapporti unicamente con soggetti che godano di buona reputazione, che siano impegnati solo in attività lecite e la cui cultura etica sia comparabile a quella della Società;
- effettuare le attività di selezione e assunzione esclusivamente sulla base delle valutazioni di idoneità tecnica, etica e attitudinale; l'attività deve essere ispirata a criteri di trasparenza nella valutazione dei requisiti di competenza e professionalità, di capacità e potenzialità individuale;
- verificare che la definizione delle condizioni economiche sia coerente con la posizione ricoperta in azienda e le responsabilità/compiti assegnati;
- provvedere affinché gli adempimenti obbligatori previsti in caso di assunzione del personale, nonché in relazione alla gestione amministrativa dello stesso, siano predisposti con la massima diligenza e professionalità, in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere e i rapporti con i Funzionari Pubblici siano improntati alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del ruolo istituzionale;
- garantire la tracciabilità delle procedure di selezione e assunzione e la corretta archiviazione della documentazione attestante il loro corretto svolgimento;
- assicurare che ogni modifica dell'anagrafica dipendente sia tracciabile e autorizzata;
- assicurare il pieno rispetto delle norme di legge e regolamentari e dei principi contabili di riferimento nella determinazione e contabilizzazione del costo del personale.
- assicurare riconoscimenti di aumenti retributivi, riconoscimenti ad personam e avanzamenti di carriera basati esclusivamente su criteri meritocratici;
- assicurarsi, in caso di assunzione di personale extra-comunitario, che la documentazione attestante il regolare permesso di soggiorno sia adeguatamente archiviata nella cartella del dipendente e, in caso di permesso scaduto, sia stato tempestivamente sollecitato il dipendente al rinnovo;
- verificare che l'assegnazione dei benefit e dei beni aziendali sia coerente con la posizione ricoperta dal dipendente in azienda e le responsabilità/compiti assegnati;
- verificare che i beni aziendali siano utilizzati esclusivamente per le finalità aziendali;

- assicurarsi che l'assegnazione dei benefit avvenga nel rispetto della normativa previdenziale e fiscale in materia;
- curare la gestione e la conservazione dei benefit e beni aziendali assegnati con la massima diligenza;
- gestire l'autorizzazione e il controllo delle trasferte secondo criteri di economicità e di massima trasparenza, nel rispetto della regolamentazione interna e di Gruppo nonché delle leggi e normative fiscali vigenti;
- richiedere/riconoscere il rimborso delle sole spese sostenute per motivi di lavoro, opportunamente documentate;
- garantire l'erogazione di rimborsi spese solo a fronte dell'esibizione da parte del richiedente di appropriati giustificativi di spesa;
- consentire la tracciabilità dell'iter autorizzativo delle trasferte e delle attività di controllo svolte;
- sostenere spese di rappresentanza esclusivamente per finalità lecite, in modo trasparente, secondo criteri di economicità e di contenimento dei costi;
- operare nel rispetto della normativa vigente in materia di strumenti di pagamento, tracciabilità dei flussi finanziari e antiriciclaggio;
- improntare le relazioni con le organizzazioni sindacali ai principi di correttezza e di collaborazione nell'interesse della Società e dei dipendenti.

È inoltre espressamente **vietato**:

- operare secondo logiche di favoritismo;
- promettere o concedere promesse di assunzione quale contropartita di attività difforni dalle leggi e dalle norme e regole interne;
- promettere assunzioni in favore di rappresentanti della Pubblica Amministrazione oppure di rappresentanti sindacali ovvero di altre controparti terze con cui la società intrattenga relazioni di business (o di soggetti ad essi "vicini" o "graditi"), al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società;
- selezionare dipendenti vicini o suggeriti da funzionari pubblici o da qualsiasi soggetto terzo privato o corrispondere loro un compenso superiore a quello dovuto o di mercato, al fine di assicurare vantaggi di qualunque tipo alla Società;
- inserire, nell'anagrafica del personale, dipendenti fittizi allo scopo di creare disponibilità extracontabili o per ottenere agevolazioni di qualsivoglia natura;
- assumere personale, anche per contratti temporanei, senza il rispetto delle normative vigenti in materia (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, etc.);
- assumere o impiegare lavoratori minorenni o lavoratori stranieri privi di permessi di soggiorno, ovvero il cui permesso sia scaduto (e per il quale non si sia richiesto il rinnovo), revocato o annullato;

- assegnare benefit e beni aziendali a soggetti diversi da quelli indicati dalle procedure interne e di Gruppo, salvo che tali assegnazioni trovi giustificazione in relazione al livello di inquadramento contrattuale e/o al contenuto della mansione svolta;
- promettere o concedere benefit quale contropartita di attività difformi alle leggi, al Codice Etico e alle norme e regole interne o di Gruppo;
- riconoscere rimborsi spese che non trovino adeguata giustificazione in relazione al tipo di incarico svolto o in assenza di idonea documentazione giustificativa;
- creare fondi a fronte di rimborsi spese inesistenti in tutto o in parte;
- sostenere e riconoscere spese di rappresentanza che possano essere interpretate come eccedenti le normali pratiche commerciali o di cortesia;
- esporre nella documentazione inviata o condivisa con la Pubblica Amministrazione fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società.

5. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

5.1. Selezione e assunzione del personale

L'Area Gestione del Personale e Organizzazione, sulla base delle richieste di organico da parte dell'Area Tecnica in funzione dei lavori pianificati, e riportate all'interno di un apposita relazione suddivisa per commessa richiede l'approvazione da parte del Direttore del Personale e dell'Amministratore Delegato, e successivamente invia la richiesta approvata alle Agenzie per il Lavoro, le quali programmano le selezioni del personale con le conseguenti sessioni formative per fornire a RO.S.S. il personale formato necessario.

Per quanto riguarda il personale impiegatizio, ciascun Responsabile di Area manifesta la necessità di integrare il proprio organico attraverso l'invio all'Area Gestione del Personale e Organizzazione di una richiesta formale, che successivamente viene sottoposta all'approvazione del Direttore del Personale e dell'Amministratore Delegato.

Nel caso di personale dirigente, è l'Amministratore Delegato che in collaborazione con il Direttore del Personale individua la necessità di assumere nuovi dirigenti e che sottopone la proposta al Consiglio di Amministrazione, per approvazione, nel rispetto delle vigenti procure e della Procedura "Reclutamento del personale Infragruppo SITAF SPA e Società Controllate".

Una volta accertato l'effettivo fabbisogno di risorse, per le sole figure impiegatizie e dirigenziali, a seguito di approvazione da parte del Direttore del Personale e dell'Amministratore Delegato, si avvia il processo di reclutamento valutando innanzitutto l'eventuale disponibilità di adeguate candidature interne al Gruppo, pubblicando appositi

bandi, o, in caso di esito negativo, sul mercato esterno, secondo quanto disciplinato nella sopracitata Procedura “Reclutamento del personale Infragruppo SITAF SPA e Società Controllate”, cui si rimanda per maggiori dettagli.

I colloqui di valutazione dei candidati selezionati sono condotti secondo quanto disciplinato dalla Procedura Reclutamento del Personale. In tale sede, il Responsabile di Area richiedente, compila la “ Scheda di valutazione del candidato” mettendo in evidenza l’esito del colloquio.

Se il processo di selezione ha riguardato la valutazione di più candidati per una posizione, il Responsabile di Area richiedente, di concerto con il Direttore del Personale e l’Amministratore Delegato, effettua l’analisi comparativa dei candidati e formalizza la scelta effettuata sulla scheda di valutazione del candidato prescelto, motivandola. La scheda di valutazione viene siglata dal Responsabile di Area, dal Direttore del Personale e sottoscritta dall’Amministratore Delegato.

A fronte di un colloquio con esito positivo, l’Amministratore Delegato comunica alla Direzione Risorse Umane di SITAF S.p.A. l’intenzione di assumere la risorsa, secondo le modalità previste dal Regolamento. Nel caso di un colloquio di personale dirigente con esito positivo, la relativa assunzione viene sottoposta all’approvazione del Consiglio di Amministrazione della Società.

I contratti di assunzione sono sottoscritti da parte dell’Amministratore Delegato. La raccolta di tutta la documentazione rilevante e l’espletamento delle pratiche di assunzione presso gli Enti competenti sono in capo alla Direzione Risorse Umane di SITAF S.p.A..

Tutti i contratti di assunzione sono firmati dall’Amministratore Delegato della Società e includono un’apposita clausola ex D.Lgs. 231/01, con la quale il neoassunto dichiara di conoscere il contenuto del Codice Etico e del Modello 231 della Società, disponibili anche nella intranet aziendale, e si impegna ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto 231/01 medesimo.

Qualunque forma di collaborazione contrattuale inerente al personale deve essere preceduta da una due-diligence preliminare. Sono oggetto di verifica:

- l’identità e i requisiti reputazionali, di onorabilità e di integrità del personale sia in fase iniziale di assunzione che periodicamente nel corso del rapporto di lavoro (prima dell’attribuzione di procure o di cambi mansione che comportino l’attribuzione di deleghe funzionali e poteri di spesa o rappresentanza in nome e per conto della Società), da svolgersi tramite analisi realizzate con Google News o Banche Dati, quali ad esempio *Word-Check*, *Moody’s Analytics*, *Fenergo Kyc* o simili da ripetersi in base ad un approccio basato sul rischio e in base alla strategicità e importanza);
- l’esistenza di eventuali procedimenti, sanzioni o condanne per reati presupposto del D. Lgs. 231/2001, in materia di salute e sicurezza sui luoghi di lavoro o tutela dell’ambiente, condotte di natura corruttiva o per reati associativi a carico del personale (ricerca Google);

- l'eventuale sussistenza di rapporti di parentela o pregressi rapporti di lavoro - sia in forma subordinata che in via autonoma - con la Pubblica Amministrazione e, in caso di risposta affermativa a tale ultima circostanza, deve essere raccolta una dichiarazione di non aver esercitato, nel triennio precedente alla candidatura in corso, poteri autoritativi o negoziali e di non aver elaborato atti endoprocedimentali obbligatori in grado di incidere in maniera determinante sul contenuto del provvedimento finale, per conto della stessa, di cui sia stata destinataria la Società;

In sede di assunzione dovrà essere altresì richiesto al candidato di fornire un'autocertificazione relativa all'eventuale pendenza di procedimenti penali con l'indicazione specifica del tipo di reato contestato e dell'Autorità Giudiziaria procedente.

5.2. Gestione di livelli retributivi, avanzamenti di carriera, riconoscimenti *ad personam*

Con cadenza annuale, i Responsabili di Area provvedono alla valutazione delle performance dei propri collaboratori e condividono le risultanze con l'Area Gestione del Personale e Organizzazione.

Sulla base delle valutazioni ricevute, l'Area Gestione del Personale e Organizzazione, predispone delle proposte di avanzamenti di carriera / riconoscimenti *ad personam* e le sottopone all'approvazione del Direttore del Personale e dell'Amministratore Delegato della Società.

5.3. Assegnazione e gestione dei beni aziendali

Gestione automezzi aziendali

La Società dispone di un parco mezzi utilizzati per finalità di servizio. Tali mezzi sono tutti inventariati al momento dell'acquisto nell'apposito registro, in coerenza con quanto disciplinato dal "Regolamento aziendale per la gestione dei mezzi di lavoro in dotazione" (PGS 033 - Rev. 3 del 01/03/2019).

La gestione operativa del parco mezzi è demandata all' Area Servizi Generali – Gestione Parco Mezzi, responsabile di verificare periodicamente lo stato d'uso e curare la manutenzione ordinaria dei mezzi. In caso di necessità a procedere con interventi di manutenzione o riparazione straordinaria, questi devono essere preventivamente autorizzati da parte della Direzione. L'individuazione dell'officina o carrozzeria a cui affidare il lavoro avviene nel rispetto delle normali procedure di selezione dei fornitori.

Al momento dell'utilizzo dei mezzi di servizio da parte dei dipendenti, è necessario che questi compilino correttamente il libretto di marcia del mezzo, inserendo i km di inizio, i km di fine, lo scopo di utilizzo del mezzo, il nominativo e la firma. I rifornimenti di carburante per i mezzi di servizio devono essere effettuati presso l'Autoporto di Susa, salvo specifiche disposizioni diverse. Al momento del rifornimento, il dipendente deve comunicare all'operatore della stazione di servizio il codice del mezzo e il kilometraggio segnalato dal veicolo.

Per quanto concerne le modalità di acquisto del carburante per i veicoli parte della flotta aziendale, si rimanda a quanto illustrato nella Parte Speciale B, al paragrafo “Gestione dei pagamenti tramite carte ricaricabili”.

L’ Area Servizi Generali – Gestione Parco Mezzi provvede ad effettuare dei controlli periodici sui dati di rifornimento dei mezzi di servizio, verificando la congruità dei consumi rispetto alle effettive esigenze di servizio e segnalando qualsiasi anomalia alla Direzione per le indagini di competenza.

Gestione delle autovetture in benefit

La Società assegna un’autovettura aziendale in benefit ai Responsabili di Area e ad ogni dipendente che ne abbia necessità in ragione della propria mansione lavorativa. L’assegnazione dell’autovettura in benefit è stabilita dall’Amministratore Delegato ed avviene secondo quanto stabilito internamente con riferimento alla gestione dei benefit aziendali, alle modalità di assegnazione, gestione e riconsegna degli stessi, le categorie di benefit ammessi sulla base della mansione ricoperta, le modalità di rifornimento etc.

L’approvvigionamento dell’auto è curato direttamente da RO.S.S., secondo le normali procedure di acquisto in vigore.

Gestione delle Carte Aziendali

La Società possiede carte ricaricabili personali poggianti su conto corrente aziendale, la cui ricarica deve essere preventivamente autorizzata dall’AD con adeguato giustificativo di spesa. È a cura dell’Area Gestione dell’Amministrazione, Finanza e Controllo la verifica della corretta consuntivazione delle stesse tramite l’invio mensile dei relativi giustificativi. Tali carte possono essere ricaricate esclusivamente da parte del Responsabile dell’Area Gestione dell’Amministrazione, Finanza e Controllo.

Le carte di credito e di debito o pagamento (incluse carte carburante e telepass) devono essere attribuite esclusivamente a personale della Società e utilizzate solo per fini di lavoro. L’attribuzione delle carte deve essere previamente autorizzata dal responsabile gerarchico dell’utilizzatore (che valuta la coerenza e l’inerenza delle spese sostenute rispetto alla competenza della Società), nonché dall’Amministratore Delegato che approva l’autorizzazione finale.

L’Amministrazione, in collaborazione con le funzioni operative, garantisce un sistema di tracciabilità che permette di verificare in ogni momento l’esatto utilizzatore della carta.

5.4. Gestione dei rimborsi spese e delle spese di rappresentanza

Tutte le trasferte devono essere pianificate e formalmente approvate da parte del Responsabile del richiedente prima dell’effettuazione della trasferta stessa, fatti salvi i casi di emergenza. RO.S.S. provvede direttamente a sostenere le spese di viaggio e di alloggio

per il soggetto interessato e, per la gestione delle spese di vitto (pranzi e cene), provvede ad erogare degli anticipi ai lavoratori pari ad € 15,00 per ogni pasto, che vengono poi gestiti all'interno della prima busta paga utile del lavoratore.

Nel caso in cui per il dipendente in trasferta fosse comunque necessario sostenere delle spese, al fine di ottenere il rimborso è necessario presentare opportuna documentazione giustificativa (es. scontrini, fatture etc.), allegata ad apposito modulo di nota spese, all'Area Gestione del Personale e Organizzazione, che provvederà all'accredito nella prima busta paga utile.

Nel caso in cui i dipendenti sostengano delle spese anche per conto di ospiti, i nominativi di questi ultimi devono essere riportati sulla documentazione giustificativa che dovrà essere consegnata all'Area Gestione del Personale e Organizzazione, che provvederà all'accredito nella prima busta paga utile.

5.5. Elaborazione paghe e contributi

Mensilmente, l'Area Gestione del Personale e Organizzazione verifica i dati delle presenze al mese precedente generati dagli applicativi "Badge2Work" ed "EVO HRP" e, una volta risolte eventuali anomalie, provvede a trasmetterli all'Ufficio Amministrazione, Finanza e Controllo Personale e Paghe Società Controllate di SITAF S.p.A. per l'elaborazione dei cedolini paga.

Una volta elaborato il flusso di pagamento degli stipendi, l'Ufficio Amministrazione, Finanza e Controllo Personale e Paghe della Società Controllate SITAF S.p.A. richiede autorizzazione all'Amministratore Delegato di RO.S.S. e successivamente procede alla predisposizione della distinta di pagamento sul sistema di web-banking.

5.6. Predisposizione e trasmissione della documentazione necessaria per l'ottenimento di finanziamenti pubblici / contributi agevolati per la realizzazione di corsi di formazione

Annualmente, l'Area Gestione del Personale e Organizzazione predispone il piano formativo per il personale della Società. Il piano include sia le attività formative obbligatorie per legge, sia specifici programmi formativi rivolti a distinte categorie di dipendenti, sulla base delle mansioni svolte e delle previsioni incluse nel contratto di lavoro in essere.

La documentazione necessaria per l'ottenimento di finanziamenti pubblici / contributi agevolati per la realizzazione di corsi di formazione, così come la documentazione di rendiconto, viene predisposta a cura dell'Area Gestione del Personale e Organizzazione con il supporto dell'Ufficio Amministrazione, Finanza e Controllo. Prima della trasmissione all'Ente finanziatore, la documentazione relativa alla rendicontazione dei costi viene sottoscritta da parte dell'Amministratore Delegato o da soggetto da questo delegato, a titolo di verifica circa la completezza dei dati richiesti. Analogamente, la comunicazione di invio del rendiconto viene sottoscritta da parte dell'Amministratore Delegato.

In caso di visite ispettive da parte dell'Ente finanziatore, i rapporti con quest'ultimo (inclusa la sottoscrizione di eventuali verbali di ispezione) vengono gestiti dall'Amministratore Delegato o da soggetto da questo delegato.

5.7. Gestione dei rapporti con le Organizzazioni Sindacali

Nel corso di ogni forma di contrattazione sindacale, RO.S.S. è rappresentata dal Direttore del Personale, assistito dal Responsabile del Personale. Il Direttore del Personale è dotato di apposita procura da parte dell'Amministratore Delegato affinché possa intervenire in trattative di carattere sindacale o comunque inerenti ai rapporti di lavoro con singole persone o con le organizzazioni o con le rappresentanze sindacali in genere.

Al termine degli incontri istituzionali, vengono formalizzati i verbali di accordo o di ipotesi di accordo o di riunione, sottoscritti dal Direttore del Personale.

6. TRACCIABILITÀ E ARCHIVIAZIONE

Tutta la documentazione prodotta a supporto del processo di selezione e gestione del personale è archiviata presso l'Area Gestione del Personale e Organizzazione di RO.S.S. e presso la Direzione Risorse Umane di SITAF S.p.A., per le parti di competenza.

La documentazione deve essere conservata in conformità a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di tutela dei dati personali, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE D: GESTIONE DEGLI ACQUISTI DI BENI, SERVIZI E INCARICHI PROFESSIONALI

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Gestione degli acquisti di beni e servizi, consulenze e incarichi professionali.

Alla data di redazione del presente documento, le attività sensibili di: "Creazione e modifica dell'anagrafica fornitori a sistema" e "contabilizzazione delle fatture passive" sono svolte da SITAF S.p.A. in forza di uno specifico contratto di service¹⁴, che prevede:

- una descrizione sintetica delle attività esternalizzate;
- i criteri di determinazione dei compensi per i servizi resi.

3. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati contro la Pubblica Amministrazione (art. 25 del D.lgs. 231/01):
 - Reati corruttivi;
 - Concussione;
 - Induzione indebita a dare o promettere utilità;
 - Istigazione alla corruzione;
 - Traffico di influenze illecite.
- Reati Societari (art. 25-ter del D.Lgs. 231/01):
 - Corruzione tra privati;
 - Istigazione alla corruzione tra privati.
- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies del D.Lgs. 231/01):
 - Ricettazione;
 - Riciclaggio;
 - Impiego di beni, denaro, utilità di provenienza illecita;
 - Autoriciclaggio.

¹⁴ Sottoscritto in data 17/12/2011 e in fase di revisione alla data di emissione del presente documento.

- Reati di criminalità organizzata (art. 24-ter del D.Lgs. 231/01):
 - Associazione per delinquere;
 - Associazione di tipo mafioso anche straniera.
- Reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/01):
 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
 - Dichiarazione fraudolenta mediante altri artifici;
 - Emissione di fatture o documenti per operazioni inesistenti.
- Reati di terrorismo o di eversione dell'ordine democratico (art. 25-quater del D.Lgs. 231/01):
 - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico;
 - Delitti posti in essere in violazione di quanto previsto dall'art. 2 Convenzione Internazionale di New York, 9 dicembre 1999 per la repressione del finanziamento del terrorismo.

Si rimanda all'Allegato 1 del Modello (*"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"*) per una descrizione di dettaglio di ciascuna fattispecie richiamata.

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- verificare preventivamente le informazioni disponibili sui fornitori / consulenti al fine di instaurare rapporti unicamente con soggetti di cui sia certa l'identità, che godano di buona reputazione, che siano impegnati solo in attività lecite, che siano finanziariamente solidi e la cui cultura etica aziendale sia comparabile a quella della Società;
- conservare tutta la documentazione che attesti la conformità della cessione o della prestazione eseguiti dal fornitore rispetto all'effettiva attività svolta dallo stesso come risultante da statuto, visure e anche pagine web e simili;
- verificare l'effettiva capacità del fornitore di svolgere l'operazione di cessione o di prestazione di servizi;
- verificare, prima dell'attivazione della fornitura, che ogni fornitore / consulente sia stato preventivamente qualificato secondo le regole definite dalla Società;
- assicurare che la selezione dei fornitori / consulenti avvenga a cura dei soggetti competenti e sia effettuata sulla base di requisiti di qualità, professionalità, affidabilità ed economicità;
- assicurare che il processo di selezione avvenga, ove possibile, tra almeno due fornitori / consulenti distinti;

- assicurare la tracciabilità del processo di individuazione del fornitore / consulente e rispettare i principi di trasparenza e non discriminazione nella relativa selezione;
- effettuare controlli specifici in presenza di offerte di fornitura di beni a prezzi significativamente inferiori a quelli di mercato, volti ad appurare, ove possibile, l'effettiva provenienza della merce o l'effettivo livello del servizio;
- assicurare la predisposizione della richiesta di acquisto da sottoporre ai workflow autorizzativi previsti dal sistema di deleghe e procure, anche interne, in vigore;
- assicurare che ogni acquisto sia supportato da un ordine di acquisto o da un contratto formale (e.g. in caso di affidamento di incarichi di consulenza);
- assicurare la trasparenza degli accordi ed evitare la sottoscrizione di patti o accordi segreti contrari alla legge;
- garantire che eventuali incarichi affidati a soggetti terzi per operare in rappresentanza e/o nell'interesse della Società siano sempre assegnati in forma scritta, richiedendo eventualmente, anche tramite specifiche clausole contrattuali, ai fornitori, professionisti, consulenti il rispetto dei principi comportamentali previsti dal Codice Etico;
- verificare l'effettivo adempimento della prestazione oggetto del rapporto contrattuale e degli eventuali stati di avanzamento prima del pagamento delle fatture;
- liquidare i compensi in modo trasparente, sempre documentabile e ricostruibile ex post.

È inoltre espressamente **vietato**:

- effettuare acquisti di beni, servizi, consulenze e prestazioni professionali che non trovino riscontro in una specifica e motivabile esigenza della Società;
- assegnare incarichi di fornitura a persone o società in assenza dei necessari requisiti di qualità, convenienza dell'operazione di acquisto e professionalità;
- assegnare incarichi di fornitura a persone o società "vicine" o "gradite" a soggetti pubblici o a qualsiasi controparte privata con cui la Società si relaziona in assenza dei necessari requisiti di qualità e convenienza dell'operazione;
- instaurare rapporti o porre in essere operazioni con soggetti terzi qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione dei reati di associazione per delinquere, ricettazione, riciclaggio o impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio o altro reato presupposto di cui al D.Lgs 231/01;
- corrispondere, promettere o offrire, direttamente o indirettamente, pagamenti impropri o altre utilità non dovute a rappresentanti di fornitori / potenziali fornitori / consulenti, o a persone a questi vicini, con la finalità di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;
- approvare fatture passive a fronte di prestazioni soggettivamente o oggettivamente inesistenti in tutto o in parte e/o non necessarie e/o a prezzi non allineati a quelli di mercato, allo scopo di impiegare, trasferire, sostituire o occultare disponibilità finanziarie

di provenienza illecita, oppure di ottenere un beneficio di natura fiscale, o per qualsiasi altra finalità;

- effettuare pagamenti in favore di fornitori, consulenti, professionisti e simili che operino per conto della Società, in assenza di adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e delle prestazioni effettuate;
- riconoscere compensi e rimborsi spese a fornitori / consulenti che non trovino giustificazione in relazione al tipo di incarico da svolgere ed ai prezzi di mercato;
- frazionare artificiosamente un'operazione / transazione di acquisto al fine di eludere le normative applicabili;
- intrattenere rapporti commerciali con coloro per cui si ha il sospetto che compiano frodi tributarie, in particolare legate all'IVA;
- accettare fatture a fronte di operazioni soggettivamente o oggettivamente inesistenti in tutto o in parte;
- creare fondi patrimoniali extra-contabili a fronte di operazioni contrattualizzate a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;

5. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

5.1. Qualifica fornitori e inserimento fornitore in anagrafica

Ai fini dell'accreditamento dei propri fornitori, RO.S.S. ha adottato un Regolamento pubblicato sul sito internet della Società, cui si rimanda per maggiori dettagli (Elenco elettronico degli operatori economici "Albo Fornitori" - Rev.0, Marzo 2018), che disciplina le modalità operative per la gestione dell'accreditamento da parte del fornitore.

Tutti gli operatori economici in possesso dei requisiti richiesti possono presentare domanda di iscrizione all'Albo Fornitori di RO.S.S. tramite procedura online, allegando tutta la documentazione richiesta. Prima di confermare l'iscrizione all'Albo, tutta la documentazione prodotta dal fornitore viene verificata a cura del personale dell'Area Commerciale e Acquisti/Contratti. Una volta iscritti all'albo, i fornitori possono essere invitati a presentare offerta nell'ambito degli affidamenti di lavori, servizi e forniture, nel rispetto delle modalità e degli importi previsti dalla normativa vigente.

È possibile ricorrere a fornitori non iscritti all'Albo, tramite ricerche di mercato, nel caso in cui quelli già presenti non siano rispondenti alle caratteristiche tecniche ricercate, oppure per casi di somma urgenza. In ogni caso, anche a seguito della prestazione effettuata, il fornitore dovrà essere sottoposto al normale processo di qualifica tramite l'analisi della documentazione richiesta in fase di normale iscrizione all'Albo.

Una volta approvato l'inserimento del fornitore nell'Albo, l'Area Commerciale e Acquisti/Contratti comunica i dati anagrafici del nuovo fornitore all'Area Amministrazione, Finanza e Controllo di Gestione di SITAF S.p.A. per la creazione dell'anagrafica a sistema.

5.2. Manifestazione dell'esigenza di acquisto e selezione del fornitore

Ciascun Ufficio Richiedente manifesta le proprie necessità di approvvigionamento inviando una richiesta via e-mail all'Area Commerciale e Acquisti/Contratti, con indicazione del materiale o del servizio da acquistare, delle caratteristiche tecniche necessarie e delle quantità richieste ed avendo cura di esplicitare l'eventuale unicità del fornitore o la richiesta di procedere con affidamento di carattere fiduciario ad una specifica controparte. In tutte le comunicazioni di richiesta di approvvigionamento, è necessario che il Responsabile dell'Ufficio richiedente sia sempre tenuto in copia conoscenza.

Ricevuta la richiesta via mail, l'Area Commerciale e Acquisti/Contratti provvede, con il supporto del Responsabile Ufficio Amministrazione, Finanza e Controllo, ad effettuare un controllo preventivo di capienza di budget. Nel caso in cui la capienza di budget non sia sufficiente a perfezionare l'acquisto, l'eventuale autorizzazione a procedere con un acquisto extra-budget deve essere fornita dall'Amministratore Delegato.

Una volta completati i controlli di capienza di budget, l'Area Commerciale e Acquisti/Contratti avvia il processo di selezione del fornitore come previsto dal regolamento acquisti. Per forniture contraddistinte da carattere fiduciario, quali determinati profili professionali (e.g. notaio, avvocato, etc.), la Società può procedere con l'affidamento diretto al fornitore designato.

Una volta raccolte tutte le offerte, l'Area Commerciale e Acquisti/Contratti avvia una valutazione comparativa di queste ultime al fine di individuare quella più vantaggiosa. Una volta selezionata l'offerta, l'Area Commerciale e Acquisti/Contratti formalizza sempre per iscritto la motivazione sottostante la scelta, sul DRS110 (SGI). Successivamente, ad evidenza dell'analisi svolta, l'Area Commerciale e Acquisti/Contratti archivia una copia di tutte le offerte ricevute.

Laddove non fosse possibile raccogliere un numero di offerte da parte di almeno 3 fornitori (e.g. a causa della specificità del materiale richiesto) l'Area Commerciale e Acquisti/Contratti formalizza le motivazioni di scelta sul DRS110 (SGI).

5.3. Predisposizione della Richiesta di Acquisto

A seguito della selezione dell'offerta, l'Area Commerciale e Acquisti/Contratti provvede all'inserimento della Richiesta di Acquisto a sistema. La RdA è sottoposta a validazione da parte del Responsabile Acquisti.

5.4. Predisposizione dell'Ordine di Acquisto / Contratto

L'Area Commerciale e Acquisti/Contratti predispone l'ordine di acquisto a sistema / la bozza di contratto di acquisto.

Tutti gli ordini / contratti di acquisto includono una clausola risolutoria ex D.Lgs. 231/01 con la quale la controparte dichiara di conoscere il contenuto del D.Lgs. 231/2001 e si impegna ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto medesimo, nonché a rispettare i principi di comportamento richiamati dal Codice Etico di RO.S.S..

Tutti gli ordini e i contratti di Acquisto sono sottoposti all'approvazione dell'Amministratore Delegato o altro soggetto dotato di idonei poteri tramite firma sulla copia cartacea e inviati al fornitore dall'Area Commerciale e Acquisti/Contratti.

5.5. Entrata Merce / Acquisizione della prestazione

Con riferimento all'acquisto di beni, la merce arriva presso la sede societaria e l'Area Commerciale e Acquisti/Contratti provvede a verificare che quanto ricevuto sia conforme a quanto indicato nell'Ordine di Acquisto prima di procedere con la registrazione a sistema della Bolla di Entrata Merce (BEM).

Analogamente, con riferimento all'acquisto di servizi e incarichi professionali, l'Area Commerciale e Acquisti/Contratti verifica, con il supporto dell'Ufficio Richiedente, che il servizio reso sia conforme a quanto pattuito contrattualmente e successivamente procede con la registrazione a sistema dell'Acquisizione della prestazione.).

Il sistema SAP non consente la registrazione della BEM o delle acquisizioni delle prestazioni in caso di mancata corrispondenza con l'Ordine di Acquisto o in assenza di un OdA/ObA registrato.

5.6. Registrazione fatture passive

La ricezione delle fatture passive, avviene tramite il Sistema di Interscambio (SdI), ed è possibile consultare e scaricare le stesse, attraverso i sistemi Archiflow e SAP utilizzati dalla società RO.S.S. nonché dalla società Sitaf. L'Area Commerciale e Acquisti/Contratti, provvede ad effettuare la verifica di coerenza con il relativo Oda/Oba precedentemente caricato a sistema. Successivamente le fatture vengono contabilizzate a sistema dalla Direzione Amministrazione, Finanza e Controllo di Sitaf, sulla base dei dati caricati e ove non presenti, sulla base delle indicazioni delle aree coinvolte.

5.7. Acquisti tramite carte ricaricabili

Si rinvia ai presidi di controllo disciplinati nella sezione B "Gestione delle Attività Amministrative", paragrafo "Gestione della finanza e della tesoreria - Gestione dei pagamenti tramite carte ricaricabili".

5.8. Acquisti tramite cassa contante

Si rinvia ai presidi di controllo disciplinati nella sezione B “Gestione delle Attività Amministrative”, paragrafo “Gestione della finanza e della tesoreria - Gestione della cassa contante”.

5.9. Acquisti tramite buoni d’acquisto

Per acquisti ripetitivi (e.g. minuterie) la Società si avvale della sottoscrizione di accordi quadro.

In questi casi, qualora si presenti la necessità di una fornitura, l'Ufficio richiedente sottopone al proprio Responsabile, per approvazione, un buono d’acquisto per attivare la fornitura. Il buono d’acquisto deve essere di importo unitario inferiore e/o uguale a 250,00 Euro.

I buoni siglati devono essere consegnati all’Area Commerciale e Acquisti/Contratti, che ha il compito, con cadenza mensile, di predisporre il relativo Ordine di Acquisto a sistema.

6. TRACCIABILITÀ E ARCHIVIAZIONE

Tutta la documentazione prodotta a supporto del processo di gestione degli acquisti è archiviata in formato elettronico dal sistema SAP e in formato cartaceo presso Area Commerciale e Acquisti/Contratti. Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE E: GESTIONE DELLE COMMESSE

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Gestione Richieste di Offerta e partecipazione a gare
- Gestione delle commesse.
- Gestione dei rapporti con il Committente nell'ambito della gestione delle commesse, anche in occasione di visite ispettive.
- Gestione fornitori, subappaltatori e prestatori d'opera

3. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati contro la Pubblica Amministrazione (art. 24 del D.Lgs. 231/01):
 - Truffa in danno dello Stato o di un ente pubblico;
 - Frode nelle pubbliche forniture;
 - Turbata liceità degli incanti;
 - Turbata libertà del procedimento di scelta del contraente.
- Reati contro la Pubblica Amministrazione (art. 25 del D.Lgs. 231/01):
 - Reati corruttivi;
 - Concussione;
 - Induzione indebita a dare o promettere utilità;
 - Istigazione alla corruzione;
 - Traffico di influenze illecite.
- Reati Societari (art. 25-ter del D.Lgs. 231/01):
 - Corruzione tra privati;
 - Istigazione alla corruzione tra privati;
 - False comunicazioni sociali;
 - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

- Reati di criminalità organizzata (art. 24 ter del D.Lgs 231/01):
 - Associazione per delinquere;
 - Associazione di tipo mafioso anche straniera.
- Reati di terrorismo (art. 25 quater del D.Lgs 231/01):
 - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico;
 - Delitti posti in essere in violazione di quanto previsto dall'art. 2 Convenzione internazionale di New York per la repressione del finanziamento del terrorismo del 9 dicembre 1999.
- Reati contro la personalità individuale (art. 25 quinquies del D.Lgs 231/01):
 - Intermediazione illecita di sfruttamento del lavoro;
 - Riduzione o mantenimento in servitù o schiavitù.
- Reati in materia di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare (art. 25-duodecies del D.Lgs. 231/01):
 - Impiego di lavoratori il cui soggiorno è irregolare;
 - Disposizioni contro l'immigrazione clandestina.
- Reati in materia di strumenti di pagamento diversi dal contante (art. 25 octies 1 del D.Lgs 231/01):
 - Trasferimento fraudolento di valori (riferito all'art. 512 bis comma 2).
- Reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/01):
 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
 - Dichiarazione fraudolenta mediante altri artifici;
 - Emissione di fatture o documenti per operazioni inesistenti.
- Reati in materia di salute e sicurezza sui luoghi di lavoro (art. 25 septies del D.Lgs 231/01):
 - Omicidio colposo;
 - Lesioni gravi e gravissime.
- Reati in materia ambientale:
 - attività di gestione di rifiuti non autorizzata;
 - Cessazione e riduzione dell'impiego delle sostanze lesive dell'ozono;
 - abbandono di rifiuti;

- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari;
- Sistema informatico di controllo della tracciabilità dei rifiuti;
- Combustione illecita di rifiuti;
- Inquinamento ambientale;
- Disastro ambientale;
- Delitti colposi contro l'ambiente;
- Circostanze aggravanti;
- Attività organizzate per il traffico illecito di rifiuti.

Si rimanda all'Allegato 1 del Modello (*"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"*) per una descrizione di dettaglio di ciascuna fattispecie richiamata.

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- assicurare che i profili di accesso al sistema di gestione delle commesse siano coerenti con i ruoli e le responsabilità definiti all'interno dell'organizzazione;
- garantire la predisposizione e il monitoraggio, per ogni commessa, di un budget dei costi e ricavi da inizio a fine commessa;
- osservare le regole di corretta, completa e trasparente contabilizzazione dei costi e ricavi di commessa, secondo i criteri indicati dalla legge e dai principi contabili di riferimento;
- garantire che i costi / ricavi di commessa contabilizzati siano supportati da adeguata documentazione giustificativa;
- garantire la tempestività, l'accuratezza ed il rispetto del principio di competenza nell'effettuazione delle registrazioni contabili;
- assicurare il rispetto della normativa in materia di subappalti;
- assicurare l'adempimento delle misure di legalità previste dai protocolli di legalità cui la Società aderisce, ottemperando agli impegni ivi previsti;
- garantire lo svolgimento dei rapporti negoziali e commerciali in modo chiaro e corretto;
- garantire il diligente adempimento degli obblighi contrattuali;
- garantire il principio di segregazione nella definizione e predisposizione delle offerte economiche;
- i contratti con i clienti, compresi quelli stipulati con le società del Gruppo, sono formalizzati e riportano in maniera chiara le indicazioni concernenti il servizio che viene loro erogato a fronte della corresponsione di un prezzo; detti contratti sono sottoscritti dai soggetti muniti degli appositi poteri e presentano al loro interno una chiara definizione di quelle che sono le responsabilità delle parti e delle specifiche clausole contrattuali che si impegnano a rispettare;
- costituire eventuali ATI o RTI previa due diligence sulla controparte;

- assicurarsi della sussistenza dei requisiti etici e reputazionali delle terze parti commerciali;
- effettuare gli adempimenti nei confronti del Cliente, con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere;
- assicurare che tutti i lavori portati in essere durante l'esecuzione della commessa rispettino le caratteristiche dichiarate ed i requisiti previsti dalla normativa;
- assicurare che siano consegnati agli acquirenti gli stessi lavori dichiarati per qualità, quantità o costo;
- monitoraggio dell'effettiva esecuzione dei progetti e delle attività nel rispetto degli standard di qualità, quantità ed affidabilità pattuiti contrattualmente;
- assicurarsi che tutto il personale che opera presso i luoghi di lavoro (interno ed esterno) sia in linea con gli adempimenti retributivi, contributivi ed assistenziali, nonché in possesso di regolare permesso di soggiorno, laddove si tratti di cittadini extracomunitari;
- garantire il rispetto degli standard previsti dai CCNL di riferimento;
- assicurare il rispetto di tutta la normativa in materia di salute, sicurezza, ambiente e responsabilità sociale.

È inoltre espressamente **vietato**:

- rappresentare in contabilità - 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, relativamente ai costi / ricavi di commessa;
- registrare in contabilità operazioni a valori non corretti rispetto alla documentazione di riferimento, oppure a fronte di transazioni inesistenti in tutto o in parte, o senza un'adeguata documentazione di supporto che ne consenta una corretta rilevazione contabile e successivamente una ricostruzione accurata;
- omettere di segnalare / denunciare eventuali registrazioni illegittime, non corrette, false o che corrispondano a operazioni sospette o in conflitto di interessi;
- alterare o distruggere documenti ed informazioni finanziarie e contabili disponibili in formato cartaceo e/o elettronico;
- nell'ambito dei rapporti con i funzionari della stazione appaltante, tenere una condotta finalizzata a ottenere una irregolare aggiudicazione della gara, mediante l'allontanamento di altri concorrenti e in ogni caso con ogni comportamento diretto a influenzare la libera concorrenza della gara;
- turbare il procedimento amministrativo diretto a stabilire il contenuto del bando ovvero di altro atto equipollente, alternativamente con violenza, minaccia, doni, promesse, collusioni o altri mezzi fraudolenti, al fine di condizionarne la scelta del contraente da parte della Pubblica Amministrazione, a proprio vantaggio.

5. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

5.1. Richieste pervenute dal Gruppo SITAF o altro soggetto

Gestione delle Richieste di Offerta e analisi di fattibilità

Le Richieste di Offerta sono convogliate all'ufficio commerciale che le riceve direttamente dai clienti.

Ricevuta una richiesta di offerta, l'area commerciale coinvolge tutti gli uffici (Area Commerciale e Acquisti/Contratti, Area Risorse Umane, Segreteria e Formazione, area produzione, Ufficio Amministrazione, Finanza e Controllo), ciascuno per la propria parte di competenza, al fine di valutare la fattibilità tecnica ed economica della richiesta.

Le risultanze di tale analisi sono sottoposte all'attenzione dell'Amministratore Delegato o di soggetto da questo delegato per preventiva approvazione a procedere con la predisposizione dell'offerta.

Una volta ottenuta l'autorizzazione a procedere, l'Area Commerciale e Acquisti/Contratti cura la redazione dell'offerta utilizzando il template dedicato del SGI e avvalendosi del supporto degli altri Uffici aziendali per le parti di competenza.

Prima della trasmissione alla controparte da parte dell'Area Commerciale e Acquisti/Contratti, l'offerta formulata viene sottoposta all'approvazione tramite firma dell'Amministratore Delegato o di soggetto da esso procurato/delegato.

Eventuali integrazioni successive alla documentazione di offerta devono essere sottoposte al medesimo iter approvativo.

5.2. Partecipazione a bandi di gara

Monitoraggio dei bandi di gara

L'Area Commerciale e Acquisti/Contratti si occupa del monitoraggio della pubblicazione di bandi di gara di interesse per il business della Società, anche attraverso l'utilizzo di un portale dedicato ("Infordat"), che giornalmente elabora un report riepilogativo dei bandi pubblicati.

Analisi di fattibilità e predisposizione della documentazione di gara

Una volta individuato un bando di potenziale interesse per la Società, l'Area Commerciale e Acquisti/Contratti elabora un'analisi preliminare di fattibilità tecnica ed economica della commessa, avvalendosi del supporto degli altri Uffici aziendali per le parti di competenza (Area Risorse Umane, Segreteria e Formazione, Ufficio Tecnico, Ufficio Amministrazione, Finanza e Controllo).

Tale analisi viene approvata in primis dal comitato gare e successivamente è sottoposta all'attenzione dell'Amministratore Delegato, che fornisce l'autorizzazione o meno a procedere con la gara nei limiti dei poteri conferitigli dal C.d.A.

Superati tali conferimenti, sarà lo stesso C.d.A che avrà l'onere di deliberare o meno il perseguimento dell'iniziativa commerciale.

Una volta ottenuta l'autorizzazione a procedere, l'Area Commerciale e Acquisti/Contratti cura la redazione della documentazione amministrativa, tecnica ed economica per la partecipazione al bando di gara, avvalendosi del supporto degli altri Uffici aziendali per le parti di competenza.

Prima della trasmissione, tutta la documentazione di gara viene sottoscritta dall'Amministratore Delegato.

Mancata aggiudicazione del bando di gara

In caso di mancata aggiudicazione del bando di gara, la Direzione Aziendale valuta se procedere con una richiesta di accesso agli atti e, in caso affermativo, individua formalmente il professionista incaricato di seguire l'iter giurisprudenziale.

A seguito dell'accesso agli atti di gara, gli Uffici competenti, ciascuno per la propria parte, collaborano a redigere un'analisi volta a valutare la possibilità di presentare un ricorso, che deve essere autorizzata dall'Amministratore Delegato.

La pratica viene gestita operativamente dal professionista incaricato, che si avvale del supporto dell'Area Commerciale e Acquisti/Contratti ove ritenuto necessario.

Nel caso in cui il ricorso non sia accolto, la pratica viene archiviata. In caso contrario, si procede come di seguito illustrato.

5.3. Verifica partner commerciali (ATI/RTI)

L'Area Acquisti/Contratti, con il supporto dell'Ufficio Legale verifica:

- l'ambito di attività e le caratteristiche del cliente, del titolare effettivo o dell'esecutore;
- il paese o l'area geografica nei quali essi hanno la propria sede o residenza;
- se il soggetto è persona giuridica: lo scopo sociale e i mezzi di cui si avvale per raggiungerlo;
- se ci sono elementi sospetti (quali: largo utilizzo di denaro contante, nuovi metodi di pagamento o offerta di servizi innovativi, etc.).

ed ancora:

- l'identità e i requisiti reputazionali, di onorabilità e di integrità del cliente o dei soci e degli amministratori della società terza sia in fase iniziale che, periodicamente, durante la prosecuzione del rapporto (analisi tramite Google News o Banche Dati, quali ad esempio word-check, moody's analytics, fenargo kyc o simili da ripetersi in base ad un approccio basato sul rischio e in base alla strategicità e importanza);
- l'esistenza di eventuali procedimenti, sanzioni o condanne, per violazioni della normativa ex D. Lgs. 231/2001, per reati presupposto del D. Lgs. 231/2001, in materia di salute e sicurezza sui luoghi di lavoro o tutela dell'ambiente, condotte di natura

corruttiva o per reati associativi a carico della controparte ovvero dei soci, degli amministratori o del management della stessa (ricerca Google).

- l'esistenza di un Modello di Organizzazione, Gestione e Controllo ex D. lgs. 231/2001, sistemi di gestione, policy anticorruzione nella società terza (quantomeno per appalti, mandati e somministrazioni).

I controlli possono essere svolti mediante:

- Visura camerale;
- Documenti di bilancio;
- Acquisizione e analisi documentali;
- Acquisizione del casellario giudiziario e carichi pendenti;
- Ricerche di notizie su Google e Google news (limitando la ricerca alle prime tre pagine indicate dal motore di ricerca utilizzato);
- Ricerche specifiche su banche dati pubbliche (es. liste antiterrorismo Banca d'Italia o internazionali pubbliche),
- Ricerche su banche dati informative private,
- Acquisizione di pareri di colleghi che abbiano già conosciuto il cliente o il partner nello svolgimento delle proprie mansioni per altri soggetti.

Possono essere omessi controlli in caso in cui il partner sia partner storico di cui da tempo si siano già acquisite idonee evidenze ovvero ancora sia già stato sottoposto a verifiche per protocolli di legalità o da stazioni appaltanti pubbliche (essendo quindi già sottoposto ad adeguata verifica fornitori).

5.4. Adempimenti previsti dai protocolli di legalità

RO.S.S. aderisce ai Protocolli di Legalità previsti nell'ambito delle varie commesse, al fine di assicurare la realizzazione del preminente interesse pubblico alla legalità e alla trasparenza in relazione alla realizzazione dell'opera.

L'adesione a tali Protocolli, che consentono alle imprese che vi aderiscono di attestare la propria affidabilità e di verificare quella dei propri partner commerciali, comporta una serie di adempimenti e impegni relativamente ai contratti conclusi dalla Società successivamente all'adesione ai Protocolli.

Le funzioni operative della Società cooperano al fine di adottare tutte le misure di legalità previste dal Protocollo, permettendo lo svolgimento dell'attività di impresa al riparo da gravi rischi di natura legale e reputazionale.

Per conoscere gli aspetti operativi riguardanti i processi di adeguata verifica dei fornitori, che costituiscono applicazione dell'adesione ai Protocolli di Legalità, si rimanda agli stessi, le cui prescrizioni sono vincolanti per tutti i soggetti che, nell'ambito del CUP oggetto del Protocollo, intrattengono un rapporto giuridico diretto con il soggetto aggiudicatore per l'esecuzione di

contratti relativi a parte dell'opera, e comportano clausole specifiche di impegno a denunciare eventuali tentativi di estorsione o illeciti di diversa natura.

La prima e più importante conseguenza derivante dall'adesione al Protocollo di Legalità è costituita dall'impegno che l'impresa assume di operare in un regime di assoluta trasparenza, attuando tutte le disposizioni in esso previste.

La Società garantisce i più elevati livelli di prevenzione antimafia nell'esecuzione delle opere, in conformità a quanto previsto dai Protocolli di Legalità e dal Codice Antimafia.

5.5. Gestione delle commesse

Aggiudicazione del bando di gara ed esecuzione della commessa

In caso di aggiudicazione del bando di gara o ricevuta l'accettazione dell'offerta, la Direzione Aziendale indice una riunione formale con tutti gli Uffici coinvolti ai fini dell'avvio della commessa (e.g. in termini di pianificazione degli acquisti ed eventualmente degli investimenti, di organico da impegnare / assumere, etc.), sulla base di quanto definito nella documentazione di offerta.

Nel corso di tale riunione, ovunque possibile, viene identificato formalmente il Responsabile di Commessa. Il verbale di tale riunione è conservato secondo quanto definito dal SGI della Società.

L'area commerciale ufficio acquisti/contratti provvede a verificare la correttezza formale e sostanziale della bozza di contratto con la controparte, sottoponendolo quindi alla firma dell'Amministratore Delegato ai fini della trasmissione alla Stazione Appaltante.

Successivamente, l'area commerciale provvede ad inserire il contratto in SAP.

Ciascuno per le parti di propria competenza, l'area commerciale ufficio acquisti/contratti, e il Servizio Sicurezza provvedono a raccogliere tutta la documentazione necessaria secondo i requisiti di legge (e.g. dichiarazioni antimafia, DURC, PSC, DVR etc.).

Rendicontazione della commessa

Il Responsabile di Commessa è incaricato della pianificazione e gestione operativa della commessa (e.g. gestione della turnazione del personale, monitoraggio delle risorse preventivate per l'esecuzione della commessa), nonché dell'effettuazione dei controlli previsti secondo il SGI aziendale.

In caso di contratto "a misura", l'addetto alla consuntivazione provvede alla verifica delle attività svolte sulla base delle condizioni pattuite contrattualmente.

L'addetto alla consuntivazione provvede inoltre a redigere la documentazione di Stato Avanzamento Lavori (SAL), che deve essere approvata dal Responsabile di commessa, verificato dal controllo di gestione ed approvato dal direttore tecnico operativo.

I SAL approvati sono trasmessi al Responsabile Ufficio Amministrazione, Finanza e Controllo ai fini della fatturazione.

Nel corso delle rilevazioni di collaudo e sullo stato di avanzamento dei lavori tutti i destinatari coinvolti dovranno garantire la massima collaborazione all'espletamento delle rilevazioni. In particolare, sono messi a disposizione con tempestività, trasparenza, completezza e pertinenza i dati e le informazioni necessari per la redazione del SAL, nel rispetto del principio di verità.

Per ogni ulteriore questione si rinvia alle norme del Codice dei Contratti Pubblici laddove applicabile.

Possono essere sottoscritti solo documenti veritieri, che rispecchino il reale stato dell'opera e di avanzamento lavori.

Gestione varianti in itinere

Qualora in fase di verifica di avanzamento vengano rilevate condizioni che possano pregiudicare il rispetto delle condizioni contrattuali o che richiedano la negoziazione di una variante, il Responsabile di commessa convoca una riunione operativa con tutti i Responsabili degli Uffici coinvolti al fine di verificare l'entità degli impatti sulla gestione della Commessa.

Nel caso in cui le criticità fossero tali da richiedere la formulazione di una nuova offerta al cliente, questa deve essere preventivamente approvata e sottoscritta da parte dell'Amministratore Delegato.

Gestione operativa della commessa ()

Per quanto concerne i rischi di reato connessi alle attività della società (quali, ad esempio, quelli in materia di igiene e sicurezza sui luoghi di lavoro, ambiente, reati contro la personalità individuale, reati in materia di immigrazione clandestina, reati di criminalità organizzata, reati di terrorismo) si rimanda ai principi di comportamento di cui al paragrafo 4, nonché a quanto previsto dalle Parti Speciali G ed H per quanto riguarda, rispettivamente, gli adempimenti in materia di salute e sicurezza sui luoghi di lavoro e quelli in materia ambientale. Si rinvia inoltre alla Parte Speciale C, per quanto riguarda la selezione del personale.

Chiusura delle attività di commessa

L'esecuzione della fornitura deve avvenire nel rispetto del principio della buona fede nell'esecuzione dei contratti evitando qualsiasi raggirio volto a ingannare la controparte o qualunque modifica dolosa all'esecuzione della prestazione da cui consegua la consegna di cose in tutto o in parte difformi dalle caratteristiche convenute con riferimento sia alla specie sia alla qualità o quantità delle cose o opere fornite, sia la cattiva esecuzione dei lavori.

Una volta concluse le attività, il responsabile di commessa/Area Commerciale e Acquisti/Contratti, con il supporto della direzione tecnica, predispone un verbale di chiusura lavori da condividere con la controparte al fine di confermare la corretta conclusione della commessa.

5.6. Gestione dei rapporti con i Subappaltatori

In fase di qualifica e selezione dell'appaltatore viene quindi verificato il possesso dei requisiti di onorabilità e reputazionali previsti dal Codice Appalti e dal Codice Antimafia, in linea con quanto formalizzato nel "Regolamento Fornitori" e nelle procedure più sopra richiamate, oltreché l'idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione ai sensi della vigente normativa (art. 26 Titolo I d.lgs. 81/2008, normativa applicabile ai cantieri prevista dal medesimo Testo Unico, nonché adempimenti previsti dal Protocollo di Legalità). Nella valutazione dei fornitori devono essere considerati anche gli aspetti fiscali e contributivi.

Con riferimento alle prestazioni effettuate presso i luoghi di lavoro della Società o presso i cantieri, la Società, tramite le funzioni delegate, effettua al primo ingresso un controllo di regolarità rispetto alla documentazione ricevuta in fase di selezione e contrattualizzazione del fornitore (elenco dei nominativi dei lavoratori che accedono ai luoghi di lavoro della Società e copia dei relativi documenti di identità in corso di validità, documentazione attestante la regolarità giuslavoristica del rapporto di lavoro nonché, specificatamente per i lavoratori extra comunitari, copia dei documenti attestanti la regolarità della permanenza sul territorio italiano), nonché gli ulteriori controlli previsti dal Protocollo di Legalità. La verifica sull'identità dei lavoratori che accedono ai luoghi di lavoro deve comunque essere realizzata ad ogni accesso.

In fase di contrattualizzazione la Società avverte l'appaltatore che, in mancanza dei suddetti documenti, potrà rifiutare gli accessi ai propri luoghi di lavoro, salve le azioni legali ritenute più opportune, inclusa la risoluzione per inadempimento del fornitore.

I contratti stipulati con gli appaltatori prevedono specifiche clausole contrattuali a presidio dei rischi connessi alla gestione degli appalti d'opera, previste dal documento "Clausole Contrattuali ex D.Lgs. 231/2001", al quale si rimanda.

Devono essere inoltre inserite le clausole previste dai Protocolli di Legalità applicabili.

Con specifico riferimento agli aspetti legati all'idoneità tecnico-professionale del sub-appaltatore si rimanda a quanto disposto nella Parte Speciale G – Gestione degli adempimenti in materia di salute e sicurezza sui luoghi di lavoro, paragrafo 5.4.

5.7. Gestione del personale di cantiere (interno ed esterno)

Qualora RO.S.S. si trovi ad essere aggiudicatario diretto di un appalto, al fine di una corretta gestione del personale di cantiere, sia interno alla Società, sia di terzi sub-appaltatori,

dovranno essere registrati tutti gli accessi alle aree di cantiere, sia di personale interno alla società, sia esterno (sub-appaltatori). In fase di accesso dovrà essere verificata e registrata l'identità dei lavoratori tramite l'apposita tessera di riconoscimento, corredata di fotografia e contenente le generalità del lavoratore e l'indicazione del datore di lavoro, unitamente agli orari di ingresso e di uscita dal cantiere.

Nei casi in cui vi sia un diverso appaltatore, ROSS dovrà comunicare preventivamente l'elenco del proprio personale ingaggiato che accederà alle aree di cantiere, fornendo tutti i dati necessari per la loro registrazione muniti di tesserino di riconoscimento cartaceo o digitale.

5.8. Gestione dei rapporti con il Committente nell'ambito della gestione delle commesse, anche in occasione di visite ispettive

Nell'ambito della gestione delle commesse, i rapporti con il Committente sono curati dal Responsabile di commessa. Tutta la documentazione condivisa con il Committente è sottoscritta dall'Amministratore Delegato o da persona da lui delegata/procurata.

In tale contesto devono essere rispettati, oltre ai principi di comportamento indicati nella presente Parte Speciale, anche i principi di comportamento di cui alla precedente Parte Speciale A – Gestione dei rapporti con la Pubblica Amministrazione.

6. TRACCIABILITÀ E ARCHIVIAZIONE

Tutta la documentazione prodotta a supporto del processo di gestione delle commesse è archiviata presso il protocollo aziendale..

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE F: GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI, DI TERZI E DELLA P.A.

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Gestione dei sistemi informativi aziendali, di terzi e della Pubblica Amministrazione.
- Gestione delle licenze d'uso per applicazioni software.

Alla data di redazione del presente documento, le attività sensibili di: "gestione delle infrastrutture informatiche di gruppo" sono svolte da SITAF S.p.A. in forza di uno specifico contratto di service¹⁵, che prevede:

- una descrizione sintetica delle attività esternalizzate;
- i criteri di determinazione dei compensi per i servizi resi.

3. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati contro la Pubblica Amministrazione (art. 24 del D.Lgs. 231/01):
 - Frode informatica a danno dello Stato o di altro ente pubblico.
- Reati informatici e trattamento illecito dei dati (art. 24 bis).
 - Accesso abusivo ad un sistema informatico o telematico;
 - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
 - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
 - Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
 - Danneggiamento di informazioni, dati e programmi informatici;
 - Danneggiamento di sistemi informatici o telematici;
 - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità;
 - Falsità in un documento informatico pubblico o avente efficacia probatoria.

¹⁵ Sottoscritto in data 17/12/2011 e in fase di revisione alla data di emissione del presente documento.

- Reati in materia di violazione del diritto d'autore (art. 25 novies del D.Lgs 231/01).
 - Delitti in materia di violazione del diritto d'autore.
- Reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/01):
 - Occultamento o distruzione di documenti contabili
- Delitti contro la personalità individuale (art. 25 quinquies del D.Lgs. 231/01):
 - Detenzione di materiale pornografico-pornografia virtuale.
- Delitti in materia di strumenti di pagamento diversi dal contante (art. 25 octies 1 del D.Lgs 231/01)
 - Frode informatica a danno dello Stato o di altro ente pubblico;
 - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dal contante.

Si rimanda all'Allegato 1 del Modello ("I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001") per una descrizione di dettaglio di ciascuna fattispecie richiamata.

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- garantire il rispetto della normativa a tutela del diritto d'autore, sia attraverso la richiesta di idonee garanzie sulla titolarità dei diritti, sia utilizzando tali opere nel rispetto della normativa e dei contratti con gli autori stessi;
- adottare modalità di gestione delle opere tutelate dal diritto d'autore che ottemperano ai principi di verificabilità, congruità, tracciabilità;
- documentare e verificare ogni fase del processo di acquisizione dei diritti patrimoniali d'autore;
- valutare la corretta implementazione tecnica delle abilitazioni / profili utente ai principali sistemi aziendali, verificandone la corrispondenza con le relative mansioni ed il rispetto del principio generale di segregazione dei compiti;
- monitorare il corretto utilizzo degli accessi ai sistemi informativi aziendali di dipendenti e terze parti;
- garantire il back-up periodico dei dati;
- verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità del sistema dei controlli IT;
- gestire la manutenzione software e hardware dei sistemi secondo le prassi esistenti;
- vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e il trattamento illecito dei dati, suggerendo ogni più opportuno adeguamento;

- garantire che non sia consentito l'accesso alle aree riservate (e.g. sala server) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente e, in ogni caso, nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali.

In particolare, tutti i dipendenti della Società **devono**:

- custodire accuratamente le risorse informatiche aziendali o di terze parti (es. personal computer fissi o portatili) utilizzate per l'espletamento delle attività lavorative;
- utilizzare gli strumenti informatici aziendali e assegnati nel rispetto delle procedure aziendali in vigore ed esclusivamente per l'espletamento della propria attività lavorativa;
- utilizzare la navigazione in internet e la posta elettronica esclusivamente per le attività lavorative;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le password.

È inoltre espressamente **vietato**:

- detenere, diffondere o utilizzare abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- utilizzare gli strumenti informatici assegnati dalla Società esclusivamente per finalità diverse da quelle aziendali, salvo specifica autorizzazione che ne consenta l'uso privato. È comunque vietata l'esportazione/copia di qualunque dato aziendale su qualsiasi supporto informatico privato;
- diffondere a soggetti esterni, salvo non abbiano ricevuto specifico mandato all'accesso ai sistemi informatici della Società, codici di accesso ai sistemi informatici interni o di controparti;
- prestare o cedere a terzi qualsiasi apparecchiatura informatica della Società, senza la preventiva autorizzazione delle funzioni competenti;
- utilizzare password di altri utenti aziendali, salvo espressa e motivata autorizzazione;
- distruggere o alterare documenti informatici archiviati sulle directory di rete o sugli applicativi aziendali e, in particolare, i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario nonché documenti contabili o aventi rilevanza fiscale;
- sopprimere programmi informatici contenuti nei sistemi della Società, in violazione dei protocolli aziendali;
- lasciare documenti incustoditi contenenti informazioni riservate o codici di accesso ai sistemi;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei suddetti sistemi informativi;
- danneggiare, distruggere gli archivi o i supporti relativi all'esecuzione delle attività di back-up;

- utilizzare i sistemi informativi a disposizione per attività non autorizzate nell'ambito dell'espletamento delle attività lavorative;
- acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei sistemi informativi aziendali o di terze parti;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- rivelare ad altri le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- aggirare o tentare di eludere i meccanismi di sicurezza aziendali (Antivirus, Firewall, Proxy Server, ecc.) di terze parti;
- porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali o di terze parti;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore;
- utilizzare o installare programmi diversi da quelli autorizzati e privi di licenza;
- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- accedere ad aree riservate (e.g. sala CED) senza idonea autorizzazione, temporanea o permanente;
- utilizzare firme elettroniche di altri utenti aziendali, nonché l'accesso ad aree protette in nome e per conto di terzi, salvo espressa autorizzazione del titolare della firma o dell'accesso. L'autorizzazione deve essere scritta e circoscritta entro specifica attività o tipologia di attività e deve essere motivata da ragioni oggettive di impedimento del titolare allo svolgimento personale dell'attività;
- alterare, mediante l'utilizzo di firma elettronica altrui o in qualsiasi altro modo, documenti informatici della Società;
- produrre e trasmettere documenti in formato elettronico della Società con dati falsi e/o alterati;
- falsificare documenti aventi efficacia probatoria.

5. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

5.1. Gestione dei sistemi informativi aziendali

Gestione dei profili di accesso ai sistemi informativi aziendali

La gestione dei profili di accesso (creazione, modifica, cessazione) ai sistemi informativi aziendali è in capo all'Ufficio Servizi Informatici di RO.S.S., che si avvalgono del supporto della Funzione ICT della Capogruppo SITAF S.p.A. ove necessario. In particolare, per quanto riguarda applicativi informatici adottati a livello di Gruppo (e.g. ARPA), i Servizi Informatici comunicano il nominativo dei soggetti le cui utenze devono essere create / modificate / cessate alla Funzione ICT di SITAF S.p.A., che si occupa della relativa implementazione.

Con riferimento agli applicativi adottati direttamente da RO.S.S., invece, la gestione delle utenze è demandata interamente ai Servizi Informatici.

Tutte le utenze sono composte da UserID e password. Quest'ultima deve essere aggiornata ogni 60 giorni e deve rispettare i criteri di complessità previsti (e.g. minimo di 8 caratteri maiuscoli, minuscoli e speciali; impossibilità di ripetere una delle ultime 12 password utilizzate, etc.). Nel caso in cui l'utenza rimanga inattiva per un periodo superiore a 60 giorni, questa viene automaticamente disabilitata.

L'eventuale accesso agli applicativi informatici della Società da parte di soggetti esterni a RO.S.S. è ammesso previa doppia autenticazione con User-ID e Password per l'accesso in VPN appositamente fornita e successivamente con autenticazione a dominio.

Periodicamente, la Funzione ICT di SITAF S.p.A. trasmette all'Ufficio Servizi Informatici di RO.S.S. un'estrazione riepilogativa delle utenze attive sui sistemi informativi di Gruppo e delle relative abilitazioni, ai fini della verifica, da parte dei Servizi Informatici di RO.S.S. (con il supporto delle Funzioni interessate), della correttezza o meno di quanto implementato nei sistemi. Qualsiasi incongruenza rispetto alla corrente prassi organizzativa viene tempestivamente notificata alla Funzione ICT di SITAF per l'effettuazione delle rettifiche necessarie.

Gestione delle dotazioni informatiche

Il materiale informatico (pc e telefoni cellulari) fornito in dotazione ai dipendenti della Società viene configurato per la consegna a cura dei Servizi Informatici. La consegna di tali dotazioni a dipendenti, accompagnata da formale lettera di consegna contenente indicazioni sul corretto utilizzo degli strumenti, avviene a cura dell'Area Risorse Umane, Segreteria e Formazione.

Gestione della sicurezza delle reti

Tutti i PC sono dotati di antivirus aggiornati centralmente, che non possono essere disattivati dagli utilizzatori. Periodicamente avviene una scansione automatica delle postazioni utente per verificare la presenza di virus.

L'accesso alla rete internet dai PC avviene solo previo passaggio attraverso sistemi di protezione perimetrale e di protezione ed autenticazione dell'accesso.

Le macchine che offrono servizi direttamente esposti in internet sono confinate su reti DMZ ("Demilitarized Zone") dedicate, al fine di incrementare il livello di separazione con gli elementi presenti sulle altre reti.

L'accesso ai sistemi informativi aziendali da rete esterna è consentito solo attraverso il passaggio da firewall di perimetro (Fortinet, dotato di soluzione UTM).

Gestione dei backup

La gestione dei backup dei sistemi è in capo alla Capogruppo SITAF S.p.A. (con riferimento ai sistemi che risiedono negli apparati di storage dislocati nei Data Center di Susa e Bardonecchia). Con specifico riferimento al CED situato presso gli uffici di RO.S.S., le operazioni di backup avvengono secondo le medesime modalità.

Periodicamente, la Funzione ICT di SITAF S.p.A. incarica soggetti esterni dell'esecuzione di specifiche azioni tese a verificare il corretto funzionamento delle procedure di backup e di restore.

Gestione della sicurezza fisica

Per tutto quanto attiene alla sicurezza fisica dei Data Center di Susa e Bardonecchia, si rimanda a quanto disciplinato nel Protocollo ex D.Lgs. 231/01 "Gestione dei Sistemi Informativi" della Capogruppo SITAF S.p.A.

La sala CED situata presso gli uffici di RO.S.S. è protetta da porta chiusa a chiave, custodita esclusivamente dal Responsabile Sistemi Informatici. La sala CED è dotata inoltre di misure di sicurezza fisica quali impianto di condizionamento, impianto antincendio, sistema di rilevazione fumi e pavimento sollevato.

5.2. Gestione delle licenze d'uso per applicazioni software

La gestione delle licenze dei software utilizzati a livello di Gruppo (incluso il monitoraggio delle relative scadenze) è in capo alla Funzione ICT di SITAF S.p.A., che periodicamente riceve dai Servizi Informatici di RO.S.S. indicazioni sugli specifici fabbisogni per la Società.

L'Ufficio Servizi Informatici di RO.S.S. si occupano direttamente dell'approvvigionamento e del monitoraggio delle licenze eventualmente utilizzate esclusivamente da RO.S.S..

L'installazione di software sui dispositivi aziendali può avvenire solo da parte del consulente incaricato (CONNECT), che provvede a verificarne la compatibilità con i sistemi aziendali in essere.

Gli interventi di manutenzione, anche non programmati, svolti su tali software da fornitori esterni avvengono sempre con il coinvolgimento del consulente informatico di supporto (CONNECT). Gli aggiornamenti sui software sono effettuati in conformità con quanto previsto dai fornitori.

5.3. Gestione della posta elettronica

I soggetti esterni a cui vengono trasmessi messaggi di posta elettronica mediante i sistemi aziendali possono attribuire carattere istituzionale alla corrispondenza ricevuta dalla Società. Gli utenti sono pertanto responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente alle seguenti regole.

I sistemi di posta elettronica aziendale **non possono** essere utilizzati per:

- creare, trasmettere o ricevere materiale (es. messaggi, immagini) con contenuti sessuali espliciti e denigratori, diffamatori, osceni od offensivi, quali, a titolo esemplificativo, insulti, epiteti ovvero qualsiasi altro contenuto o testo che possa essere considerato una molestia ovvero una discriminazione fondata sull'origine razziale, il colore della pelle, la nazionalità, il sesso, preferenze sessuali, età, infermità fisiche o psichiche, stato di salute, stato civile rispetto al matrimonio, convinzioni politiche o religiose;
- sollecitare o fare proseliti per finalità commerciali, di propaganda in favore di organizzazioni esterne, catene di lettere, ovvero per altre finalità estranee all'attività della Società;
- scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività della Società;
- inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie, o altro materiale appartenente ad organizzazioni diverse dalla Società, salvo che tali attività costituiscano parte integrante di obblighi contrattuali in essere con i Clienti. La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari della Società ovvero ad azioni legali dei legittimi titolari del diritto d'autore;
- tentare di rappresentare la posizione della Società, mediante l'uso di sistemi di posta elettronica, su qualsiasi questione di carattere pubblico attraverso forum di discussione che possano compromettere l'immagine pubblica della Società.
- utilizzare a fini aziendali, a meno che ciò non sia permesso dalla Società o in caso di emergenza, la posta elettronica personale;
- effettuare download di software, senza previa autorizzazione.

Inoltre, gli utenti **devono**:

- utilizzare i sistemi di posta elettronica aziendali esclusivamente per condurre affari ufficiali nonché per corrispondere comunicazioni comunque correlate agli affari condotti dalla Società;
- vigilare al fine di evitare la rivelazione attraverso e-mail, news-group o forum pubblici di informazioni confidenziali;
- verificare che il contenuto di messaggi, file di testo, immagini, file audio pubblicati o trasmessi attraverso i sistemi di posta elettronica aziendali non violino la presente procedura, i diritti di terzi o siano illeciti;
- conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla pubblica amministrazione;
- prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo.
- in caso di errore nella spedizione o ricezione di un messaggio di posta, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuarne copia;
- inviare preferibilmente files in formato PDF.

6. TRACCIABILITÀ E ARCHIVIAZIONE

Tutta la documentazione prodotta a supporto del processo di gestione dei sistemi informativi aziendali è archiviata presso l'Ufficio Servizi Informatici di RO.S.S. o presso la Funzione ICT di SITAF S.p.A., secondo competenza.

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE G: GESTIONE DEGLI ADEMPIMENTI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro nonché ad agenti chimici, fisici e biologici.
- Valutazione dei rischi e predisposizione delle relative misure di prevenzione e protezione conseguenti, metodologia adottata e mappatura dei fattori di rischio individuati.
- Attività di natura organizzativa, comprese emergenze, primo soccorso, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.
- Gestione degli appalti e delle forniture.
- Attività di sorveglianza sanitaria.
- Informazione, formazione e addestramento in materia di salute e sicurezza sul lavoro.
- Attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori.
- Sistemi di registrazione implementati.
- Sorveglianza e sistema disciplinare.

3. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies del D.Lgs. 231/01) Si rimanda all'Allegato 1 del Modello ("*I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001*") per una descrizione di dettaglio di ciascuna fattispecie richiamata.

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- rispettare gli obblighi dalla legislazione applicabile in materia di salute e sicurezza sul lavoro, nonché osservare scrupolosamente le disposizioni e le istruzioni impartite dai soggetti preposti al fine di preservare la salute e la sicurezza propria e di tutti i lavoratori;
- rispettare le linee guida aziendali e le procedure/protocolli a regolamentazione delle tematiche in materia di salute, igiene e sicurezza sul lavoro;
- collaborare, mediante i propri rappresentanti, alla valutazione di tutti i rischi per la sicurezza e salute sul lavoro;
- segnalare tempestivamente alle strutture individuate e con le modalità definite nelle procedure/protocolli aziendali in vigore, eventuali situazioni di pericolo e rischio, infortuni, malattie professionali o situazioni di *near miss* (o quasi incidenti), e violazioni alle regole di comportamento e alle procedure aziendali;
- utilizzare, secondo le istruzioni, le attrezzature presenti sul luogo di lavoro, nonché i dispositivi di protezione individuali e collettivi, ove previsti;
- utilizzare macchine e attrezzature nel rispetto delle indicazioni fornite dal costruttore;
- non compiere di propria iniziativa operazioni o manovre che possano compromettere la sicurezza propria o di altri lavoratori o che possano esporre sé stessi, i propri colleghi o terzi a situazioni di pericolo;
- segnalare ogni anomalia, situazione o rischio per la sicurezza e salute differenti da quelli noti o particolarmente significativi;
- partecipare alle sessioni formative e di addestramento organizzate dalla società sui rischi per la sicurezza e salute del lavoro.

Gli esponenti aziendali di RO.S.S. specificatamente responsabili **devono** inoltre:

- mantenere aggiornato e rispettare il corpo regolamentare ed il sistema di nomine e deleghe in materia di salute e sicurezza in vigore;
- perseguire l'eliminazione dei rischi e, ove ciò non è possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;
- garantire la programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione le condizioni produttive e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro;
- perseguire l'obiettivo di "nessun danno alle persone" e la riduzione dei rischi alla fonte e promuovere una cultura nella quale tutti i lavoratori partecipino a questo impegno;
- garantire il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro;
- contenere l'utilizzo di agenti chimici sul luogo di lavoro;
- garantire la definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori in caso di pericolo grave e immediato;

- garantire l'idoneità delle risorse umane - in termini di numero, qualifiche professionali e formazione - e dei materiali, necessaria al raggiungimento degli obiettivi prefissati dalla società per il mantenimento e/o miglioramento dei livelli di sicurezza e salute dei lavoratori;
- garantire l'acquisizione e la gestione dei mezzi, delle attrezzature, degli impianti e, in generale, delle strutture aziendali nel rispetto degli standard tecnico-strutturali di legge, anche attraverso un processo continuo di manutenzione (ordinaria e straordinaria) degli stessi;
- definire gli obiettivi per la sicurezza e la salute dei lavoratori, valutando i rischi connessi con l'attività svolta presso la sede della Società, identificando i pericoli e i rischi introdotti presso RO.S.S. da attività ivi svolte da terzi attraverso un efficace e preventivo scambio di informazioni e cooperazione / coordinamento con il datore di lavoro delle società esterne che dovessero operare presso RO.S.S.;
- garantire un adeguato livello di formazione, addestramento e informazione ai lavoratori, nonché richiedere che un adeguato livello di formazione, addestramento e informazione sia garantito dai datore di lavoro delle ditte terze in appalto/subappalto per quanto di loro competenza e relativamente ai rischi da interferenza, sul sistema di gestione aziendale della sicurezza definito dalla società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla società stessa;
- segnalare tempestivamente alle strutture individuate a norma di legge e/o internamente eventuali segnali / eventi di rischio / pericolo indipendentemente dalla loro gravità.

5. PRESIDI DI CONTROLLO

Premessa

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

La Società dispone di un Sistema di Gestione della Salute e Sicurezza sul Lavoro implementato secondo lo Standard ISO 45001:2018, definito e formalizzato in un manuale che rimanda a procedure e istruzioni operative di dettaglio per la gestione degli aspetti specifici rilevanti in materia di salute e sicurezza sul lavoro.

Il modello organizzativo secondo la ISO 45001, evoluzione dello Standard OHSAS 18001:2007, si configura come il generale presidio di controllo, da rispettare ad opera di tutti i lavoratori, integrato dal presente protocollo per completare i presidi di controllo ed i conseguenti adempimenti.

Premesso che tutti i controlli previsti dalle policy / procedure e dal Sistema di Gestione della salute e sicurezza sul lavoro devono essere pienamente garantiti, è necessario in ogni caso assicurare che siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza, i seguenti presidi di controllo, ritenuti maggiormente rilevanti al fine di mitigare potenziali rischi-reato ai sensi del D.Lgs. 231/2001.

5.1. Rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro nonché ad agenti chimici, fisici e biologici

Il Datore di Lavoro e il Delegato del Datore di Lavoro per la salute e sicurezza, in collaborazione con il Responsabile del Sistema di Gestione Integrato (RGSI), il RSPP, l'ASPP, il MC ed i Responsabili di Funzione competenti **provvedono** a:

- individuare, anche a seguito della redazione del Documento di Valutazione dei Rischi (DVR) e successivi aggiornamenti, lo stato di conformità (e le eventuali azioni di miglioramento) rispetto agli standard tecnico-strutturali di legge, di attrezzature, impianti (ad esclusivo titolo esemplificativo, impianti termici ed elettrici, di messa a terra, di prevenzione incendi), luoghi di lavoro, agenti chimici, fisici e biologici, e le relative responsabilità di attuazione;
- effettuare controlli periodici dei luoghi di lavoro finalizzati a garantire il mantenimento nel tempo degli standard di legge;
- pianificare ed effettuare, o verificare che siano effettuate da società/professionisti esterni qualificati (anche quelle rilevanti a carico della proprietà degli uffici utilizzati), le manutenzioni periodiche e straordinarie delle macchine e delle attrezzature di lavoro utilizzate, registrandone l'avvenuta effettuazione in idonea documentazione, garantendone la coerenza con le indicazioni dei manuali d'uso e manutenzione dei singoli impianti tecnologici e delle informazioni acquisite dai fornitori/produttori delle macchine e attrezzature;
- definire i requisiti di sicurezza che i referenti aziendali preposti devono verificare preliminarmente all'approvvigionamento di attrezzature, impianti, agenti chimici, fisici e biologici, per lo sviluppo e realizzazione dei prodotti;
- garantire un monitoraggio continuo sull'evoluzione degli standard tecnico-strutturali e della normativa.

5.2. Valutazione dei rischi e predisposizione delle relative misure di prevenzione e protezione conseguenti, metodologia adottata e mappatura dei fattori di rischio individuati

Il Datore di Lavoro, coadiuvato dal RSPP, dall'ASPP, dal Medico Competente e dal RLS, con la collaborazione del Delegato del Datore di Lavoro per la salute e sicurezza, effettua la valutazione dei rischi per la salute e la sicurezza, al fine di identificare ed attuare le misure di prevenzione e protezione dei lavoratori, riducendo a livelli accettabili i rischi connessi, in relazione alle conoscenze acquisite ed alla priorità definita.

Tale analisi deve essere formalizzata in apposito "Documento di Valutazione dei Rischi" ("DVR"), così come previsto dal D.Lgs. 81/2008 e s.m.i., contenente, tra l'altro, l'identificazione e la valutazione dei rischi per ogni mansione aziendale, le misure di prevenzione e protezione ed i dispositivi di protezione individuale assegnati a ciascun lavoratore nonché quanto previsto in materia di DVR dall'art. 28 comma 2 del D.Lgs. 81/2008 e s.m.i..

Il "Documento di Valutazione dei Rischi" deve essere sottoscritto a cura del Datore di Lavoro.

Il Datore di Lavoro, in collaborazione con i succitati referenti della sicurezza, **provvede** a:

- valutare tutti i rischi associati alle attività ed alle mansioni dei lavoratori della Società e ad elaborare e formalizzare il documento di valutazione dei rischi sia per gli uffici che per le lavorazioni in esterno, presso i clienti;
- riesaminare il DVR con periodicità non superiore all'anno e procedere al suo aggiornamento per sopravvenuti mutamenti organizzativi, operativo e procedurali, per modifiche tecniche, introduzione di nuove lavorazioni, apertura di nuove sedi, modifiche rese necessarie da evoluzione normative, nonché a seguito di infortuni significativi che ne evidenzino la necessità, in tempi brevi e comunque non oltre un mese dagli avvenuti mutamenti e modifiche;
- formalizzare una valutazione dei rischi specifica per ogni mansione e/o attività svolta dai propri lavoratori con identificazione e valutazione di ogni specifico pericolo e rischio connesso e delle misure per la loro mitigazione e riduzione;
- garantire il diritto di accesso e utilizzo per ogni lavoratore, senza costi, a idonei Dispositivi di Protezione Individuale (DPI) - e/o collettivi - adeguati alla mansione svolta, assicurando anche la registrazione dei dispositivi di sicurezza assegnati;
- assicurare l'attuazione delle metodologie per l'analisi e la classificazione degli incidenti e degli eventi pericolosi eventualmente registrati;
- assicurare la definizione delle responsabilità per l'attuazione di misure atte a mitigare le conseguenze a seguito di incidenti o non conformità, nonché per l'avvio e il completamento di misure correttive.

Con particolare riferimento alla gestione delle attività e dei servizi erogati da terzi presso le unità produttive o prima di avviare i lavori, la Società è tenuta a predisporre - in coordinamento con il/i Datore/i di Lavoro delle società terze e/o delle società prestatrici di opera in appalto/subappalto - un documento, da allegare al contratto, che indichi le misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi da interferenze, al fine di promuovere la cooperazione ed il coordinamento per la sicurezza, provvedendo anche alla stima dei relativi oneri delle misure preventive e protettive finalizzate alla sicurezza e salute dei lavoratori.

Tale documento, in funzione delle richieste normative, potrà configurarsi in:

- Piano di Sicurezza e Coordinamento (PSC), nel caso di appalti che ricadano nell'ambito di applicazione del Titolo IV del D.Lgs. 81/08 e s.m.i., redatto dal Coordinatore per la Sicurezza in fase di Progettazione (CSP), nominato dal soggetto Committente;
- Piano Operativo di Sicurezza (POS), fornito dai terzi in regime di appalto o subappalto che ricadano nell'ambito di applicazione del titolo IV del TUS. Il POS deve essere sottoscritto dal Datore di Lavoro o da Delegato del Datore di Lavoro di RO.S.S. e consegnato al Datore di Lavoro della appaltatrice, in caso di subappalto, o appaltante (committente) in caso di appalto.

- Documento Unico per la Valutazione dei Rischi da Interferenze (DUVRI), per le restanti tipologie di appalti, redatto, ove previsto dall'art. 26 del D.Lgs. 81/2008 e s.m.i., dal Datore di Lavoro Committente.

5.3. Attività di natura organizzativa, comprese emergenze, primo soccorso, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza

La Società si è dotata di un sistema di nomine e deleghe che definisce le responsabilità, i compiti e i poteri in materia di sicurezza, prevenzione infortuni e igiene sul lavoro.

Il Datore di Lavoro deve provvedere al mantenimento ed eventuale aggiornamento (e connesse comunicazioni e flussi informativi) delle individuazioni del Delegato del Datore di Lavoro per la salute e sicurezza, dei Preposti, del RSPP, dell'ASPP e del Medico Competente. Devono inoltre essere designati i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza (addetti al primo soccorso e addetti alle emergenze in caso d'incendio, ecc.). A supporto della gestione delle emergenze sono predisposti Piani di Emergenza.

Il Delegato del Datore di Lavoro per la salute e sicurezza, con il supporto del RSPP e dell'ASPP, deve garantire l'adequatezza, efficacia di ruolo, indipendenza e aggiornamento formativo delle squadre di emergenza, secondo l'Accordo Stato-Regioni sulla formazione del 21 dicembre 2011 (Pubblicato in GU n° 8 dell'11/01/2012).

Inoltre:

- i responsabili in materia di sicurezza sul lavoro sopra identificati esercitano, per l'area di loro competenza, tutti i poteri attribuiti ed adempiere a tutti gli obblighi previsti dal D.Lgs. 81/2008 e s.m.i., nonché da tutte le altre leggi e regolamenti in materia di sicurezza, prevenzione infortuni ed igiene ambientale applicabili;
- tutti i lavoratori devono essere opportunamente formati (ed addestrati in occasione delle esercitazioni di emergenza) in merito ai riferimenti (sia interni che esterni) da contattare in caso di emergenza e alle azioni da compiere per una sicura evacuazione.

In particolare, sono definite e divulgate adeguate istruzioni e/o procedure operative finalizzate a:

- garantire la sicurezza e salute sul luogo di lavoro;
- gestire le attività in appalto e subappalto ed i relativi rischi di interferenza;
- regolamentare i flussi informativi;
- garantire l'effettuazione di attività operative e definire istruzioni per svolgere correttamente ed in sicurezza le attività relative ad ogni figura professionale;
- garantire la corretta gestione delle situazioni d'emergenza e prevedere prove di emergenza/evacuazione periodiche.

Il Datore di Lavoro e il Delegato del Datore di Lavoro per la salute e sicurezza, con il supporto del RSPP e dell'ASPP, assicurano:

- almeno una volta all'anno - come previsto dall'art. 35 del D.Lgs. 81/2008 e s.m.i. - l'effettuazione di riunioni periodiche alle quali partecipino tutte le figure chiave della sicurezza;
- continua informazione, formazione e addestramento in materia di sicurezza e salute del lavoro di tutti i lavoratori, per le linee guida generali e sui rischi specifici connessi alla loro mansione, nonché del personale responsabile, per le relative specifiche competenze;
- la registrazione dell'avvenuta effettuazione delle suddette attività, nonché l'archiviazione della documentazione relativa.

Nel corso della riunione annuale, il Datore di Lavoro sottopone all'esame dei partecipanti almeno i seguenti argomenti:

- il documento di valutazione dei rischi e conseguenti misure di prevenzione;
- l'andamento degli infortuni, delle malattie professionali e della sorveglianza sanitaria;
- i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale;
- i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute.

5.4. Gestione degli appalti e delle forniture

In generale, l'attività di affidamento di lavori a terzi è disciplinata dalla normativa di riferimento, per quanto attiene i criteri per la verifica dei requisiti, le modalità di assegnazione e i controlli previsti.

Il processo di qualifica dei fornitori effettuato dalla Società impone la richiesta e la verifica, con il supporto del RSPP e dell'ASPP, del Responsabile Ufficio Commerciale Acquisti e Gare, dell'Ufficio Amministrazione, Finanza e Controllo e del Responsabile Operativo Cantieri, del possesso dei requisiti di idoneità tecnico-professionale dell'impresa appaltatrice o dei lavoratori autonomi per lo svolgimento dell'attività nonché l'acquisizione di documentazione specifica quale ad es. l'iscrizione alla Camera di Commercio, così come indicato all'art. 26 *Obblighi connessi ai contratti d'appalto o d'opera o di somministrazione* (nel caso di appalti di servizi e manutenzione) e art. 90 *Obblighi del committente o del responsabile dei lavori* del D.Lgs. 81/2008 e s.m.i. (nel caso di appalti operanti in cantieri temporanei o mobili).

Per l'area interessata all'appalto, il Delegato del Datore di Lavoro per la salute e sicurezza, coadiuvato dal RSPP, dall'ASPP e dai Preposti per la sicurezza/ Responsabile Operativo Cantieri o dalle Funzioni Competenti che hanno attivato l'appalto, deve assicurare, durante l'esecuzione dei lavori:

- la cooperazione tra i Datori di Lavoro per all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro di incidenti sull'attività lavorativa oggetto dell'appalto.
- il coordinamento degli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori (reciprocamente scambio di informazioni anche al fine di ridurre i rischi dovuti

alle interferenze - qualora si presentassero - tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva).

- che il personale di RO.S.S. non coinvolto con l'appalto sia informato di non interferire con il lavoro del personale esterno di manutenzione, di non prestare supporto e non fare utilizzare le attrezzature di lavoro della società.

In caso di appalti ricadenti nel Titolo IV del D.Lgs. 81/2008, il Committente dei lavori, o il Responsabile dei Lavori, se individuato, deve ottemperare ai disposti dell'art. 90 *Obblighi del committente o del responsabile dei lavori* del D.Lgs. 81/2008, nel periodo di attività del cantiere.

5.5. Attività di sorveglianza sanitaria

È responsabilità del Datore di Lavoro e del Delegato del Datore di Lavoro per la salute e sicurezza, con il supporto del RSPP, dell'ASPP e dell'Ufficio del Personale, assicurare al Medico Competente le condizioni necessarie per lo svolgimento della sorveglianza sanitaria dei lavoratori alle dipendenze della Società, dotandoli di adeguati spazi per l'esecuzione dell'attività di propria competenza e per la registrazione dell'avvenuto adempimento degli obblighi di legge indicati di seguito, nonché per l'archiviazione della relativa documentazione.

È responsabilità del Medico Competente, purché non a scapito degli accertamenti obbligatori previsti a norma di legge, valutare l'adeguatezza del programma di sorveglianza, ed eventualmente procedere al relativo aggiornamento in base alle eventuali sopravvenute esigenze. In particolare, il Medico Competente deve, così come previsto dall'art. 25 del D.Lgs. 81/2008 e s.m.i., tra l'altro:

- collaborare con il Datore di Lavoro, con il RSPP, l'ASPP e con il RLS nella valutazione dei rischi;
- programmare ed effettuare (i) accertamenti preventivi intesi a constatare l'assenza di controindicazioni al lavoro cui i lavoratori sono destinati, ai fini della valutazione della loro idoneità alla mansione specifica, (ii) accertamenti periodici volti a controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica;
- istituire, aggiornare e custodire la cartella sanitaria e di rischio di ogni lavoratore;
- visitare gli ambienti di lavoro una o due volte all'anno in base ai dettami legislativi e produrre il verbale delle verifiche effettuate;
- collaborare alle attività di formazione e informazione;
- collaborare alla predisposizione del servizio di Primo Soccorso;
- formalizzare e comunicare al lavoratore l'esito delle analisi svolte, contenente giudizi di idoneità o inidoneità, rilasciandone duplice copia (una al lavoratore e una al Datore di Lavoro per la relativa archiviazione);
- partecipare alla riunione periodica di sicurezza ex art. 35 del D.Lgs. 81/2008 e s.m.i., rendicontando sulle visite effettuate, l'andamento degli infortuni e delle malattie professionali, ecc.

Gli obblighi di sorveglianza sanitaria sono riferiti a tutti i lavoratori della Società.

5.6. Informazione, formazione e addestramento in materia di salute e sicurezza sul lavoro

Il Delegato del Datore di Lavoro per la salute e sicurezza, con il supporto del RSPP, del ASPP e del Servizio Personale Formazione e Protocollo e anche con il supporto di professionisti specializzati in materia, deve garantire che siano attivate le azioni necessarie a:

- predisporre il Piano Annuale di Addestramento e Formazione con individuazione delle necessità di formazione ai lavoratori;
- organizzare ed erogare programmi di formazione/addestramento ai lavoratori neoassunti/soggetti a cambio mansione;
- organizzare ed erogare programmi di formazione specifici e periodici anche per gruppi particolari (es. Antincendio e primo soccorso);
- registrare le attività di formazione e conservare le tabelle riassuntive della formazione svolta nel corso dell'anno con relativa documentazione (fogli presenza dei partecipanti, eventuali schede di verifica apprendimento, materiale didattico distribuito);
- effettuare periodicamente verifiche volte ad accertare il livello di apprendimento e la consapevolezza in ambito di sicurezza dei lavoratori, formalizzando e archiviando i risultati, previa condivisione con il RLS;
- organizzare prove di simulazione di emergenza e di evacuazione con periodicità almeno annuale;
- comunicare ai fornitori e agli appaltatori dettagliate informazioni sui rischi specifici esistenti nella sede della Società nonché le regole comportamentali e di controllo adottate dalla Società, definite nel presente documento e nelle procedure aziendali;
- provvedere all'erogazione della necessaria formazione, informazione ed addestramento dei lavoratori a seguito di aggiornamenti normativi ed a seguito di mutamenti organizzativi, tecnici o procedurali con impatto sulla attività lavorativa ai fini della sicurezza.

5.7. Attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori

Il Datore di Lavoro e il Delegato del Datore di Lavoro per la salute e sicurezza devono vigilare sul corretto espletamento delle attività in materia di salute e sicurezza sul lavoro.

I Preposti, ciascuno nell'ambito delle proprie competenze, devono sovrintendere e vigilare sull'osservanza, da parte dei lavoratori, degli obblighi di legge e delle disposizioni aziendali in materia di salute e sicurezza sul lavoro.

La vigilanza può esplicitarsi anche mediante sopralluoghi svolti dal RSPP, dall'ASPP nonché dal Medico Competente presso i luoghi di lavoro.

Nel caso di audit in materia di salute e sicurezza sul lavoro, Il Datore di Lavoro e il Delegato del Datore di Lavoro per la salute e sicurezza, con il supporto del RSPP, del ASPP e del RSGI assicurano che:

- sia effettuata l'attività di verifica periodica sul sistema di gestione della salute e sicurezza, nel rispetto del piano di verifica definito, anche con l'eventuale supporto di professionisti esterni formalmente incaricati nel rispetto delle regole comportamentali e di controllo definite nel presente Modello;
- siano esaminati i verbali delle verifiche periodiche, con particolare riferimento ai rilievi emersi (non conformità e/o osservazioni) e al relativo piano di azione, in cui sono indicati gli interventi necessari per rimuovere le non conformità riscontrate, il soggetto responsabile della loro attuazione e le tempistiche.

5.8. Sistemi di registrazione implementati

La documentazione rilevante in materia salute e sicurezza è predisposta in forma cartacea ed informatica (data base e programmi gestionali aziendali) dalle rispettive figure aziendali competenti.

5.9. Sorveglianza e sistema disciplinare

Il Datore di Lavoro e il Delegato del Datore di Lavoro per la salute e sicurezza, anche attraverso i Preposti, il RSGI, l'ASPP e il RSPP, assicurano l'applicazione, da parte dei lavoratori, della normativa e degli adempimenti previsti in materia di salute e sicurezza sul lavoro, nonché effettuano periodiche attività di controllo atte a verificare l'efficacia delle procedure/protocolli adottate, e a garantire il mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

È presente un sistema disciplinare della società, in coerenza con il Contratto Collettivo Nazionale applicato. È previsto un flusso informativo concernente i provvedimenti disciplinari in materia antinfortunistica adottati, al fine di consentire, se del caso ed in collaborazione con il RSPP, la definizione di adeguate misure di controllo del rischio.

ADEMPIMENTI EX ART. 30 DEL D.LGS. 81/08	PROTOCOLLI PREVENTIVI ADOTTATI DA RO.S.S.
Rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici	<ul style="list-style-type: none"> • La manutenzione mezzi è gestita attraverso uno scadenziario che contiene gli interventi per ogni mezzo; la gestione è a cura del responsabile Mezzi/Attrezzature in collaborazione con il RSGI. Tutti i veicoli sono inseriti in uno specifico piano di manutenzione Excel con una scheda per mezzo contenente oltre al codice del mezzo stesso, anche i vari dati rilevanti (sullo storico degli interventi e sulle necessità di controllo o manutenzione periodica). • PGS-013 - Procedura gestione delle attrezzature • PGS-028 - Procedura per verifica funi e catene

ADEMPIMENTI EX ART. 30 DEL D.LGS. 81/08	PROTOCOLLI PREVENTIVI ADOTTATI DA RO.S.S.
	<ul style="list-style-type: none"> PGS 013 - Procedura Gestione delle Attrezzature PGS 016 - Procedura Gestione Sostanze e Miscele Pericolose. Non sono utilizzati prodotti chimici, viene solo utilizzata della colla per fissare i delineatori flessibili di corsia (chiamati de.fle.co), della vernice per realizzare la segnaletica orizzontale e il gasolio per i generatori a bordo dei mezzi antincendio
Attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti	<ul style="list-style-type: none"> Documento di Valutazione dei rischi (DVR) a firma del Delegato del Datore di Lavoro, RSPP, Medico Competente e RLS, con all'interno le valutazioni specifiche dei rischi; è presente un programma delle misure per il miglioramento ed il controllo dei livelli di rischio. Le scadenze in merito alle valutazioni dei rischi specifiche sono gestite da parte del RSPP. Il DVR contiene la metodologia applicata e le misure compensative del rischio. La data certa è sancita con l'apposizione delle firme delle figure chiave della sicurezza. PGS 002 - Procedura di Valutazione dei Rischi PGS 003 - Procedura Gestione delle Prescrizioni Legali e Altre. PGS 012 - Procedura Gestione dei Dispositivi di Protezione Individuali PGS 021 - Procedura Gestione rifiuti
Attività di natura organizzativa, quali emergenze, primo soccorso	<ul style="list-style-type: none"> Piano di Emergenza PGS 007 - Procedura Preparazione e Risposta alle Emergenze PGS 014- Procedura Presidi Antincendio
Attività di natura organizzativa, quali gestione degli appalti	<ul style="list-style-type: none"> PGS 023 - Procedura di gestione degli approvvigionamenti
Attività di natura organizzativa, quali riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza	<ul style="list-style-type: none"> Verbale di riunione periodica annuale ex art. 35 D.Lgs. 81/08
Attività di sorveglianza sanitaria	<ul style="list-style-type: none"> Verballi di sopralluoghi sui luoghi di lavoro presso le sedi aziendali

ADEMPIMENTI EX ART. 30 DEL D.LGS. 81/08	PROTOCOLLI PREVENTIVI ADOTTATI DA RO.S.S.
	<ul style="list-style-type: none"> PGS 008 - Procedura Gestione Infortuni, Incidenti, Comportamenti Pericolosi PGS 006 - Procedura Gestione Sorveglianza e Misurazioni Sicurezza
Attività di informazione e formazione dei lavoratori	<ul style="list-style-type: none"> PGS 004 - Procedura Gestione della Formazione dell'aggiornamento professionale Archivio attestati di formazione per area aziendale e per nome del dipendente a cura dell'Ufficio Personale
Attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori	<ul style="list-style-type: none"> PGS 010 - Procedura Gestione Audit Interni PGS 020 - Analisi ambientale e valutazione degli aspetti ambientali – PGS 021 - Procedura Gestione rifiuti
Acquisizione di documentazioni e certificazioni obbligatorie di legge	<ul style="list-style-type: none"> PGS 001 - Procedura Tenuta Sotto Controllo dei Documenti e delle Registrazioni
Periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate	<ul style="list-style-type: none"> PGS 001 - Procedura Tenuta Sotto Controllo dei Documenti e delle Registrazioni PGS 010 - Procedura Gestione Audit Interni PGS 020 - Analisi ambientale e valutazione degli aspetti ambientali

6. TRACCIABILITÀ E ARCHIVIAZIONE

La documentazione prodotta a supporto del processo di gestione della salute e sicurezza sul lavoro deve essere archiviata, in formato elettronico o cartaceo, a cura dei soggetti di volta in volta competenti.

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE H: GESTIONE DEGLI ADEMPIMENTI IN MATERIA AMBIENTALE

1. FINALITÀ

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

2. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati in materia ambientale:
 - attività di gestione di rifiuti non autorizzata;
 - Cessazione e riduzione dell'impiego delle sostanze lesive dell'ozono;
 - abbandono di rifiuti;
 - violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari;
 - Sistema informatico di controllo della tracciabilità dei rifiuti;
 - Combustione illecita di rifiuti;
 - Inquinamento ambientale;
 - Disastro ambientale;
 - Delitti colposi contro l'ambiente;
 - Circostanze aggravanti;
 - Attività organizzate per il traffico illecito di rifiuti.

Si rimanda all'Allegato 1 del Modello ("*I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001*") per una descrizione di dettaglio di ciascuna fattispecie richiamata.

3. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Gestione dei rifiuti.
- Gestione dei gas ozono lesivi e gas ad effetto serra (FGAS).

4. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- rispettare la normativa ambientale vigente ed applicabile alla realtà operativa;
- osservare le indicazioni aziendali atte a garantire la prevenzione dell'inquinamento;
- segnalare tempestivamente alle strutture individuate eventuali situazioni di pericolo per l'ambiente;

- perseguire l'obiettivo di "nessun danno all'ambiente";
- essere informati, formati, consultati e resi partecipi delle questioni riguardanti la tutela ambientale, con particolare riferimento ai rischi specifici della società, sulle misure di prevenzione, nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del d.lgs. 231/2001;
- ricevere istruzioni adeguate, anche attraverso corsi di formazione dedicati, sulla prevenzione ambientale;
- Redigere, aggiornare e rispettare le procedure ed istruzioni operative per la gestione degli aspetti ambientali significativi (in particolare, PGS 020 – Procedura analisi e valutazione degli aspetti ambientali; PGS 021 – Procedura gestione rifiuti; DRS 023 – Piano dei controlli sicurezza e ambiente; PGS 016 – Procedura gestione sostanze e miscele pericolose).
- partecipare alle sessioni formative e di addestramento organizzate dalla società sui rischi per l'ambiente.

Gli esponenti aziendali individuati quali Responsabili, a vario titolo e con differenti responsabilità, degli adempimenti in materia ambientale, ognuno nell'ambito di propria competenza, **devono** inoltre:

- attenersi alle regole impartite attraverso modalità operative consolidate, procedure e istruzioni operative scritte al fine di prevenire ogni impatto ambientale derivante dalle proprie lavorazioni;
- preventivamente richiedere, acquisire e rinnovare nei tempi indicati dall'autorità competente le eventuali autorizzazioni ambientali necessarie per lo svolgimento della propria attività, laddove applicabile;
- diffondere ad ogni livello dell'organizzazione i principi della buona pratica ambientale e sensibilizzare tutti i propri fornitori affinché assicurino prodotti e servizi in linea con tali principi.

5. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

La Società dispone di un Sistema di Gestione Ambientale implementato secondo lo Standard ISO 14001:2015, definito e formalizzato in un manuale che rimanda a procedure e istruzioni operative di dettaglio per la gestione degli aspetti specifici rilevanti in materia di ambiente.

Il modello organizzativo ISO 14001 si configura come il generale presidio di controllo, da rispettare ad opera di tutti i lavoratori, integrato dal presente protocollo per completare i presidi di controllo ed i conseguenti adempimenti.

Premesso che tutti i controlli previsti dalle policy / procedure e dal Sistema di Gestione Ambientale devono essere pienamente garantiti, è necessario in ogni caso assicurare che siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza, i seguenti presidi di controllo, ritenuti maggiormente rilevanti al fine di mitigare potenziali rischi-reato ai sensi del D.Lgs. 231/2001.

5.1. Gestione dei rifiuti

Il Delegato in materia ambientale, con il supporto e la collaborazione del Responsabile del Sistema di Gestione Integrato (RGSI), del Responsabile parco mezzi e deposito e del personale operativo, deve:

- identificare le aree da utilizzare come deposito temporaneo dei rifiuti prodotti dall'unità operativa, garantendo il rispetto delle prescrizioni normative;
- supervisionare lo svolgimento di un controllo del volume e del tempo di giacenza dei rifiuti collocati nei depositi temporanei affinché siano rispettate le prescrizioni di legge in materia;
- supervisionare la corretta collocazione dei rifiuti stoccati, evitando che gli stessi vengano miscelati (ove questi dovessero essere miscibili) o riposti su suolo nudo, assicurando inoltre idonei contenitori e la presenza dei contrassegni indicanti le aree di stoccaggio;
- verificare l'esistenza dei requisiti ex legge dei fornitori dei servizi di smaltimento dei rifiuti (quali, a titolo esemplificativo, autorizzazioni e iscrizione all'albo nazionale gestori rifiuti), acquisendo copia cartacea conforme della relativa documentazione - laddove non fosse possibile ottenere la copia in originale, oppure tramite gli elenchi ufficiali degli enti che hanno rilasciato l'autorizzazione;
- verificare che i mezzi di trasporto rifiuti siano effettivamente autorizzati per il trasporto dello specifico rifiuto. In caso contrario non procedere all'operazione di consegna del rifiuto;
- verificare che i contratti sottoscritti con fornitori dei servizi di smaltimento dei rifiuti contengano idonee clausole 231 atte a manlevare la Società qualora il fornitore di servizi non si adegui ai principi di comportamento definiti dal codice etico di RO.S.S.;
- effettuare periodiche verifiche del mantenimento nel tempo dei requisiti ex *lege* degli smaltitori verificati in fase di selezione;
- supervisionare e predisporre ogni azione necessaria affinché la caratterizzazione dei rifiuti e la definizione delle specifiche modalità di smaltimento avvenga secondo i principi di accuratezza e nel rispetto delle prescrizioni autorizzative e normative, avvalendosi di laboratori terzi accreditati ai quali sono fornite chiare ed esaustive informazioni in merito al processo di produzione del rifiuto e garantendo la veridicità e completezza delle dichiarazioni inerenti;
- verificare la correttezza dei dati registrati nella dichiarazione annuale dei rifiuti (MUD) prima di sottoscriverla e predisporre l'invio agli enti preposti;

- assicurarsi periodicamente della avvenuta ricezione, entro i termini di legge, della quarta copia del formulario di identificazione rifiuti;
- verificare che la movimentazione dei rifiuti (produzione, stoccaggio, esitazione) avvenga in condizioni di massima prevenzione ambientale;
- definire formalmente i ruoli, le responsabilità e le modalità operative per la verifica della corretta gestione operativa dei rifiuti speciali prodotti;
- inserire nei contratti con le ditte terze o negli ordini di lavoro una clausola nella quale riportare:
 - che il fornitore si configura, ai sensi del D.Lgs. 152/2006, quale produttore dei rifiuti derivanti dall'attività commissionata da RO.S.S.;
 - l'obbligo di fornire, con richiesta a discrezione di RO.S.S., copia fotostatica del formulario, dal quale si dovrà evincere la compilazione del campo dedicato al produttore con i dati del fornitore;
 - l'obbligo di dotarsi delle necessarie autorizzazioni per il trasporto del rifiuto;
 - il rispetto e la responsabilità della corretta gestione del proprio rifiuto, da affidare a soggetti debitamente autorizzati per il relativo recupero/smaltimento;
 - la non responsabilità, da parte di RO.S.S., per inadempienze del fornitore in merito alla corretta gestione dei rifiuti prodotti dall'attività svolta per RO.S.S.;
- erogare specifiche sessioni formative dedicate al personale destinato alla gestione dei rifiuti, durante le quali illustrare le attività in termini di gestione stessa dei rifiuti consentite e vietate.

5.2. Gestione dei gas ozono lesivi e dei gas a effetto serra (FGAS)

Il Delegato in materia ambientale, con il supporto e la collaborazione del RGSI e del personale operativo, deve:

- garantire che gli impianti contenenti FGAS siano sottoposti a periodiche manutenzioni da parte di ditta specializzata iscritta al Registro Nazionale Gas fluorurati a effetto serra, al fine di garantirne l'efficienza e periodiche verifiche di tenuta per preservare l'ambiente da eventuali fughe;
- controllare che i dati di targa, la quantità di FGAS e le informazioni relative alla manutenzione siano correttamente archiviati e periodicamente aggiornati, e inseriti, da parte della ditta incaricata per le manutenzioni, nella Banca Dati Gas fluorurati ad effetto serra.

5.3. Sorveglianza e sistema disciplinare

Il Delegato in materia ambientale, anche attraverso i Preposti e il RGSI, assicura l'applicazione, da parte dei lavoratori, della normativa e degli adempimenti previsti dalla legislazione in materia ambientale applicabile, nonché effettua periodiche attività di controllo atte a verificare l'efficacia delle procedure/protocolli adottate, e a garantire il mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

È presente un sistema disciplinare della società, in coerenza con il Contratto Collettivo Nazionale applicato. È previsto un flusso informativo concernente i provvedimenti disciplinari in materia ambientale adottati, al fine di consentire, se del caso ed in collaborazione con il RSGI, la definizione di adeguate misure di controllo del rischio.

6. TRACCIABILITÀ E ARCHIVIAZIONE

La documentazione prodotta a supporto del processo di gestione degli adempimenti ambientali deve essere archiviata, in formato elettronico o cartaceo, a cura dei soggetti di volta in volta competenti.

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

PARTE SPECIALE I: GESTIONE DEGLI ADEMPIMENTI RELATIVI AL PROCESSO FREE-FLOW

1. FINALITÀ

Nel corso dei primi mesi del 2024 la società RO.S.S ha deciso di ampliare le attività previste nel suo oggetto sociale, includendo anche "l'attività di informazione e assistenza all'utenza inerente le modalità di pagamento dei pedaggi autostradali nel nuovo sistema del free-flow" da attivarsi in particolare per una tratta autostradale specifica della autostrada Asti-Cuneo in forza di specifico mandato che le era stato all'uopo conferito dalla stessa società concessionaria Autostrada Asti Cuneo S.p.A.

Il sistema free flow è un metodo di esazione del pedaggio che permette di pagare senza rallentamenti né soste al casello, grazie ad appositi portali installati lungo il percorso. Il free flow apporta vantaggi agli utenti e benefici all'ambiente: senza code e rallentamenti alle barriere, aumentano i livelli di sicurezza e si riducono le emissioni inquinanti dei veicoli in attesa. Chi non dispone di un dispositivo di telepedaggio, potrà pagare il proprio pedaggio online entro 15 giorni dall'avvenuto passaggio sotto i nuovi portali dedicati, registrandosi al sistema Conto Targa, o regolarizzando la propria posizione come utente ospite sul sito della concessionaria autostradale. Nel sito della società (concessionaria), saranno disponibili per il pagamento i transiti effettuati entro le 24 ore dall'avvenuto passaggio in autostrada. Sarà inoltre possibile regolarizzare il pedaggio recandosi all'infopoint della concessionaria sito a Govone, o nei due terminali di pagamento predisposti nelle aree pubbliche di Alba e Asti.

Ove tutto ciò non avvenisse, trascorsi i 15 giorni utili per la regolarizzazione spontanea del pagamento, è previsto l'intervento della società RO.S.S., la quale effettuerà un'attività di "sollecito di pagamento" mediante l'invio di una comunicazione contenenti i dati e le coordinate bancarie della Concessionaria per l'effettuazione del pagamento medesimo.

Al fine di poter operare nell'ambito del settore del c.d. "recupero dei crediti" da mancato pagamento, RO.S.S. ha dovuto richiedere - e ha ottenuto dalla Questura di Torino - il rilascio di una specifica licenza attestante la sua qualità (in sostanza) di agenzia di recupero crediti.

La presente Parte Speciale del Modello 231 ha la finalità di definire le regole che tutti i Destinatari del Modello coinvolti nell'ambito delle attività "sensibili" di seguito dettagliate, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

1. LE FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato e di illecito amministrativo che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto, come dettagliato nel "Documento di Mappatura dei Rischi" cui si rimanda per maggiori dettagli, sono relative alle seguenti famiglie di reato:

- Reati contro la Pubblica Amministrazione (art. 25 del D.Lgs. 231/01):
 - Reati corruttivi;
 - Concussione;

- Induzione indebita a dare o promettere utilità;
- Istigazione alla corruzione;
- Traffico di influenze illecite.
- Reati Societari (art. 25-ter del D.Lgs. 231/01):
 - Corruzione tra privati;
 - Istigazione alla corruzione tra privati;
- Reati informatici e trattamento illecito dei dati (art. 24 bis).
 - Accesso abusivo ad un sistema informatico o telematico;
 - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.

Si rimanda all'Allegato 1 del Modello (*"I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001"*) per una descrizione di dettaglio di ciascuna fattispecie richiamata.

2. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di mappatura dei rischi, ha considerato sensibili ai sensi del D.Lgs. 231/2001 sono:

- Gestione del processo Free-Flow.

3. PRINCIPI DI COMPORTAMENTO

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività in oggetto **devono**:

- rispettare la normativa privacy vigente ed applicabile alla realtà operativa;
- monitorare il corretto utilizzo degli accessi ai sistemi informativi di terzi;
- rispettare i principi di comportamento previsti dalle parti speciali A "Gestione dei rapporti con la Pubblica Amministrazione" (nei confronti di soggetti pubblici e privati) ed F "Gestione dei sistemi informativi aziendali, di terzi e della Pubblica Amministrazione".

È inoltre espressamente **vietato**:

- corrispondere o offrire, direttamente o indirettamente, anche sotto forme diverse di aiuti o contribuzioni (ad esempio, sponsorizzazioni e liberalità), pagamenti o benefici materiali a pubblici ufficiali o incaricati di pubblico servizio o a persone a questi vicini, o a intermediari o mediatori per influenzare il loro comportamento e assicurare vantaggi di qualunque tipo alla Società;
- corrispondere, promettere o offrire, direttamente o indirettamente, pagamenti impropri o altre utilità non dovute a rappresentanti di fornitori / potenziali fornitori / consulenti, o a persone a questi vicini, con la finalità di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;

- detenere, diffondere o utilizzare abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- diffondere a soggetti esterni, codici di accesso ai sistemi informatici interni o di controparti.

4. PRESIDI DI CONTROLLO

Di seguito sono riportati tutti i presidi di controllo da porre in essere al fine di mitigare i potenziali rischi-reato identificati ai sensi del D.Lgs. 231/2001. È necessario assicurare che tali controlli siano formalmente tracciabili e documentati, anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza.

La Società RO.S.S. ha individuato al suo interno una responsabile a cui è stato affidato il servizio in via esclusiva.

Periodicamente la responsabile del processo condivide con l'Amministratore Delegato della Società lo stato dei crediti insoluti da presentare alla società concessionaria per la valutazione delle eventuali azioni da intraprendere.

La Società ha predisposto un apposito sistema di archiviazione e conservazione delle operazioni di sollecito poste in essere nell'ambito della gestione del processo Free-Flow.

5. TRACCIABILITA' E ARCHIVIAZIONE

La documentazione prodotta a supporto del processo di gestione del processo Free-Flow deve essere archiviata, in formato elettronico o cartaceo, a cura dei soggetti di volta in volta competenti.

Nei casi in cui la documentazione prodotta includa il trattamento di dati personali, le modalità di conservazione devono essere conformi a quanto previsto dalle policy adottate dal Gruppo SITAF in materia di privacy, in ottemperanza alla vigente normativa in vigore.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

1. SCOPO

Nella presente sezione sono disciplinati i flussi informativi periodici facenti parte, in aggiunta alle “segnalazioni” da effettuarsi al verificarsi di particolari eventi, dell’informativa verso l’Organismo di Vigilanza prevista dal Modello di Organizzazione, Gestione e Controllo ex D.lgs 231/2001 adottato da RO.S.S..

In particolare, sono disciplinate le informazioni generiche o notizie e/o dati utili richiesti dall’OdV con riferimento ad ogni area a rischio rilevante nell’ambito del D.Lgs. 231/01, da predisporre e inviare, da parte dei Responsabili delle suddette aree, nel rispetto delle modalità e tempistiche definite nel presente documento.

Tale informativa ha come obiettivo principale quello di permettere all’OdV di meglio assolvere le proprie funzioni e di vigilare sull’osservanza delle prescrizioni previste nel Modello.

2. FLUSSI INFORMATIVI PERIODICI

Sono oggetto di comunicazione periodiche, da parte delle singole Funzioni aziendali, le informazioni che l’OdV ha identificato come rilevanti ai fini della comprensione delle attività sensibili disciplinate dal Modello e che sono riportate nella tabella di seguito rappresentata.

Nello specifico, i flussi informativi definiti dovranno essere indirizzati all’Organismo di Vigilanza di RO.S.S., tramite l’apposita mailbox odv@roadsafetyservices.com con la periodicità indicata all’interno della medesima tabella.

Ciascun Responsabile di Ufficio, per quanto di propria competenza, è tenuto a verificare periodicamente l’allineamento della Parte Speciale in vigore rispetto alle prassi operative in essere e a segnalare all’Organismo di vigilanza:

- fatti o circostanze interni e/o esterni per i quali si ravvisa la necessità di aggiornare la sezione della Parte Speciale di propria competenza;
- segnalazioni di eventuali eccezioni e/o situazioni di mancata applicazione della sezione della Parte Speciale di propria competenza.



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
1	Gestione dei rapporti con la Pubblica Amministrazione	Gestione degli adempimenti verso la Pubblica Amministrazione	Responsabile dell'Ufficio di volta in volta coinvolto	Semestrale	<ul style="list-style-type: none"> Numero di verifiche ispettive subite e di rapporti intrattenuti con la Pubblica Amministrazione (incluse le Amministrazioni Comunitarie) nel periodo di riferimento. Numero e % di verifiche ispettive / rapporti con la Pubblica Amministrazione verificatesi nel periodo di riferimento in cui sono state segnalate criticità / non sia stato possibile garantire la partecipazione di due soggetti aziendali.
		Gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza in occasione di visite ispettive			
		Gestione del contenzioso	Alta Direzione	Semestrale	<ul style="list-style-type: none"> Numero e valore, anche stimato, dei contenziosi in essere
2	Gestione delle Attività Amministrative	Tenuta della contabilità e predisposizione del bilancio d'esercizio	Responsabile Ufficio Amministrazione, Finanza e Controllo	Annuale	<ul style="list-style-type: none"> Elenco degli scostamenti rispetto ai criteri di valutazione e registrazione previsti dai criteri contabili italiani e aziendali per le voci di bilancio maggiormente significative. Sintesi delle modifiche apportate al Bilancio in occasione dell'approvazione dello stesso da parte del Consiglio di Amministrazione. Numero e valore dei crediti stralciati e dei piani di rientro negoziati nel periodo di riferimento.
		Gestione degli adempimenti fiscali	Responsabile Ufficio Amministrazione, Finanza e Controllo	Annuale	<ul style="list-style-type: none"> Numero di eventuali verifiche fiscali subite da parte dell'Agenzia dell'Entrata e della Guardia di Finanza nel periodo di riferimento.



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
		Gestione dei rapporti infragruppo	Responsabile Ufficio Amministrazione, Finanza e Controllo	Annuale	<ul style="list-style-type: none"> Numero e valore dei contratti stipulati con parti correlate. Operazioni infragruppo che per natura, importo e/ motivazione economica risultano essere “sospette” e/o “anomale”
		Gestione dei rapporti con il Sindaco Unico e la Società di Revisione	Responsabile Ufficio Amministrazione, Finanza e Controllo	Annuale	<ul style="list-style-type: none"> Eventuali criticità segnalate dal Sindaco Unico nel corso delle attività di verifica svolte nel periodo.
		Gestione della finanza e della tesoreria	Responsabile Ufficio Amministrazione, Finanza e Controllo	Trimestrale	<ul style="list-style-type: none"> Eventuali differenze di cassa e banca rilevate a seguito dell'attività di riconciliazione e non giustificate. Numero e volume di finanziamenti e investimenti accesi o estinti nel periodo di riferimento. Eventuali conti corrente aperti/chiusi nel periodo, con dettaglio di conti aperti/chiusi all'estero.
		Gestione delle operazioni societarie straordinarie	Responsabile Ufficio Amministrazione, Finanza e Controllo	Annuale	<ul style="list-style-type: none"> Numero di operazioni straordinarie pianificate, in corso o concluse nel periodo in oggetto.
		Gestione delle locazioni passive	Responsabile Ufficio Tecnico	Annuale	<ul style="list-style-type: none"> Numero e valore dei contratti di locazione passiva stipulati nel periodo di riferimento.
		Gestione delle informazioni rilevanti e privilegiate	Alta Direzione	Semestrale	<ul style="list-style-type: none"> Numero di richieste di diffusione di informazioni privilegiate ricevute nel periodo di riferimento.



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
					<ul style="list-style-type: none"> Numero di documenti aziendali contenenti informazioni potenzialmente privilegiate consegnati nel periodo di riferimento.
3	Selezione e Gestione del Personale	Selezione e assunzione del personale	Responsabile Area Risorse Umane, Segreteria e Formazione	Trimestrale	<ul style="list-style-type: none"> Numero delle assunzioni effettuate e dei dipendenti in forza nel periodo con indicazione delle relative mansioni e distinzione per tipologia di contratto. Numero dei dipendenti stranieri in forza nel periodo con indicazione della data di scadenza del permesso di soggiorno.
		Gestione di livelli retributivi, avanzamenti di carriera, riconoscimenti ad personam	Responsabile Area Risorse Umane, Segreteria e Formazione	Annuale	<ul style="list-style-type: none"> Numero e valore dei riconoscimenti ad personam / passaggi di livello concessi nel periodo di riferimento.
		Elaborazione paghe e contributi	Responsabile Area Risorse Umane, Segreteria e Formazione	Annuale	<ul style="list-style-type: none"> Valore del costo del personale dell'anno di riferimento con indicazione della variazione % rispetto al periodo precedente.
		Assegnazione e gestione dei beni aziendali	Responsabile Ufficio Tecnico	Semestrale	<ul style="list-style-type: none"> Numero delle autovetture ad uso promiscuo assegnate nel periodo. Numero delle autovetture di servizio assegnate nel periodo; Numero delle carte carburante (sia per autovetture ad uso promiscuo che per autovetture di servizio) assegnate nel periodo;



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
					<ul style="list-style-type: none"> • Valore delle spese sostenute con carta carburante (sia per autovetture ad uso promiscuo che per autovetture di servizio) nel periodo.
		Predisposizione e trasmissione della documentazione necessaria per l'ottenimento di finanziamenti pubblici / contributi agevolati per la realizzazione di corsi di formazione	Responsabile Area Risorse Umane, Segreteria e Formazione	Semestrale	<ul style="list-style-type: none"> • Numero e valore dei finanziamenti richiesti per corsi di formazione. • Numero e valore dei finanziamenti ottenuti per corsi di formazione. • Numero di visite ispettive subite da parte dell'ente finanziatore. • Indicazione, per ogni finanziamento in corso, degli importi incassati e degli importi per i quali richiedere l'erogazione del contributo.
		Gestione dei rapporti con le Organizzazioni Sindacali	Responsabile Area Risorse Umane, Segreteria e Formazione	Semestrale	<ul style="list-style-type: none"> • Numero di incontri e accordi con le rappresentanze sindacali avvenuti nel periodo
		Gestione di omaggi e liberalità	Responsabile Area Risorse Umane, Segreteria e Formazione	Annuale	<ul style="list-style-type: none"> • Numero e valore degli omaggi erogati. • Numero e valore degli eventuali omaggi ricevuti da terzi. • Numero e valore delle erogazioni liberali effettuate nel periodo.
4	Gestione degli Acquisti di Beni, Servizi e Incarichi Professionali		Responsabile Area Commerciale e Acquisti/Contratti	Trimestrale	<ul style="list-style-type: none"> • Numero fornitori qualificati nel periodo • Numero, valore e % degli acquisti extra-budget effettuati nel periodo.



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
		Gestione degli Acquisti di Beni, Servizi e Incarichi Professionali			<ul style="list-style-type: none"> Numero, valore e % degli approvvigionamenti tramite affidamento diretto effettuati nel periodo. Numero e valore dei contratti di consulenza stipulati nel periodo di riferimento
5	Gestione delle Commesse	Partecipazione a bandi di gara e gestione delle commesse	Responsabile Area Commerciale e Acquisti/Contratti	Trimestrale	<ul style="list-style-type: none"> Numero di gare aggiudicate / non aggiudicate) alle quali la Società ha partecipato nel periodo con indicazione, per le gare aggiudicate, della percentuale di ribasso applicata e per le gare non aggiudicate delle motivazioni che ne hanno determinato l'esclusione e/o la mancata aggiudicazione.
		Gestione dei rapporti con il Committente nell'ambito della gestione delle commesse, anche in occasione di visite ispettive			<ul style="list-style-type: none"> Numero delle visite ispettive subite da parte del Committente.
6	Gestione dei Sistemi Informativi Aziendali	Gestione dei sistemi informativi aziendali	Responsabile Servizi Informatici	Trimestrale	<ul style="list-style-type: none"> Numero di utenze abilitate al sistema gestionale Arpa. Numero di personal computer assegnati. Variazioni del sistema di controllo interno relative alla gestione dei sistemi informativi.
7	Gestione degli Adempimenti in Materia	Gestione degli adempimenti in materia di salute e sicurezza nei luoghi di lavoro	Delegati in materia di salute e sicurezza	Ad evento	<ul style="list-style-type: none"> Informativa tempestiva dell'accadimento di incidenti che hanno provocato il decesso o lesioni gravi o gravissime di personale



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
	di Salute e Sicurezza sul Lavoro			Semestrale	<ul style="list-style-type: none">• Informativa tempestiva su verbali con prescrizioni o sanzioni comminati da Enti di Controllo durante visite ispettive in materia di salute e sicurezza nel luogo di lavoro.• Verbali relativi alle visite ispettive da parte dei funzionari della Pubblica Amministrazione ed Enti di Controllo in generale, contenenti gli eventuali rilievi emersi a seguito di verifiche e accertamenti.• Statistiche relative agli incidenti verificatisi sul luogo di lavoro, specificandone la causa, l'avvenuto riconoscimento di infortunio e la relativa gravità e dettaglio degli infortuni con prognosi superiore ai 40 giorni.• Nuove nomine / rinunce di soggetti operanti nell'ambito della gestione della sicurezza sul lavoro.• Variazioni che hanno richiesto l'aggiornamento del documento di valutazione dei rischi.• Risultanze delle verifiche interne svolte in materia di salute e sicurezza nel luogo di lavoro• Elenco degli investimenti previsti in materia di salute e sicurezza sul lavoro, integrato dall'elenco delle spese effettuate in situazioni di emergenza.• Piano di formazione in materia di sicurezza.



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
					<ul style="list-style-type: none"> Verbale della riunione annuale di sicurezza ai sensi dell'art. 35 del D.Lgs. 81/08. Report di verifica ispettiva di Enti Certificatori sul sistema di Gestione ISO 45001:2018, se presente un Sistema Certificato Inosservanze delle disposizioni in materia di salute e sicurezza dell'ambiente di lavoro e relativi a provvedimenti adottati, da parte di personale dipendente e del personale delle imprese appaltatrici (in particolare sanzioni disciplinari comminate).
8	Gestione degli Adempimenti in Materia Ambientale	Gestione dei rifiuti Gestione dei gas ozono lesivi e dei gas a effetto serra (FGAS) Sorveglianza e sistema disciplinare	Delegati in materia ambientale	Semestrale	<ul style="list-style-type: none"> Informativa tempestiva in merito ad eventi di cagionato inquinamento delle matrici ambientali (aria, acqua, suolo). Informativa tempestiva su verbali con prescrizioni o sanzioni comminati da Enti di Controllo durante visite ispettive in materia di tutela ambientale. Informativa tempestiva in caso di mancato rientro della quarta copia del Formulario dei rifiuti nei tempi di legge Verbali relativi alle visite ispettive da parte dei funzionari della Pubblica



#	PARTE SPECIALE	ATTIVITÀ SENSIBILE	RESPONSABILE INVIO DEL FLUSSO INFORMATIVO	PERIODICITÀ DEI FLUSSI	CONTENUTO DEL FLUSSO INFORMATIVO
					<p>Amministrazione ed Enti di Controllo in generale, contenenti gli eventuali rilievi emersi a seguito di verifiche e accertamenti.</p> <ul style="list-style-type: none">• Nuove nomine / rinunce di soggetti operanti nell'ambito della salvaguardia ambientale.• Piano di formazione in materia di ambiente.• Segnalazioni di potenziale inquinamento delle matrici ambientali suolo, aria, acqua.• Riscontrati abbandoni di rifiuti da parte di terzi/ignoti nelle aree di proprietà della società.• Individuazione di nuovi fornitori nella gestione dei rifiuti e verifiche effettuate.• Risultanze di verifiche interne in materia di ambiente.• Report di verifica ispettiva di Enti Certificatori sul sistema di Gestione ISO 14001:2015, se presente un Sistema Certificato• Inosservanze delle disposizioni in materia di tutela ambientale e relativi provvedimenti adottati, da parte di personale dipendente e del personale delle imprese appaltatrici (in particolare sanzioni disciplinari comminate).• Risultanze di verifiche interne in materia di ambiente.