MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

Tech Trade S.r.l.

Adottato dal Consiglio di Amministrazione di Tech Trade S.r.l. in data _____

PARTE SPECIALE

SOMMARIO

FINALITA' DELLA PARTE SPECIALE

Principi generali

Ai sensi di quanto disposto dall'art. 6 comma 2, lett. a) del Decreto, la Società, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera, ha identificato le Attività Sensibili (tramite il control and risk self assessment) suddivise per tipologia di reato (indicati nella Parte Generale del presente Modello) ed elencate nei paragrafi successivi, nell'ambito delle quali possano essere potenzialmente commessi reati tra quelli previsti dal Decreto.

Al fine di prevenire o di mitigare il rischio di commissione di tali reati, la Società ha dunque formulato principi generali di comportamento e protocolli generali di prevenzione, applicabili a tutte le Attività Sensibili (Codice Etico), e protocolli specifici

di prevenzione per ciascuna delle attività a rischio identificate.
Tali misure sono state assunte, in rapporto alla natura e alla dimensione della struttura organizzativa specificamente interessata nonché al tipo di attività o funzione svolta, in maniera concretamente idonea a migliorare l'efficienza nello svolgimento delle attività:
assicurando il costante rispetto della legge e di tutte le altre regole che intervengono disciplinare l'attività medesima;
verificando la capacità di contrastare efficacemente i rischi identificati.
La presente Parte Speciale ha l'obiettivo di illustrare le responsabilità, i criteri e le norme comportamentali cui i "Destinatari" del presente Modello, come definiti nella Parte Generale, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie di reato richiamate dagli artt. 24 e 25 del D. Lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione, nonché tracciabilità delle attività.

Nello specifico la presente Parte Speciale ha lo scopo di:

- definire le regole di comportamento che i Destinatari devono osservare (unitamente alle procedure specifiche di ciascun reparto operativo) al fine di applicare correttamente le prescrizioni del Modello;
- supportare l'Organismo di Vigilanza e i responsabili delle altre funzioni aziendali ad esercitare le attività di controllo, monitoraggio e verifica

Regole generali di comportamento

Tutti i destinatari del Modello, indicati nella Parte Generale, adottano regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico, al fine di prevenire il verificarsi di reati previsti dal Decreto.
In particolare, costituiscono presupposto e parte integrante dei protocolli di controllo di cui ai successivi paragrafi, i principi individuati nel Codice Etico, che qui si intende integralmente richiamato, riferiti alle varie tipologie di destinatari e/o controparti.

Aree sensibili individuate dal Risk Assessment

Come anticipato nei paragrafi precedenti, il Modello 231 è stato elaborato attraverso la rilevazione delle attività e delle prassi aziendali (tramite interviste al personale e all'analisi della documentazione interna), ipotizzando gli scenari ipotetici di commissione dei reati presupposto, e valutandone l'effettiva applicabilità reale e concreta.
Il risultato di questa attività di Risk Assessment è riportata nel Documento di Valutazione dei Rischi redatto preliminarmente al presente Modello, nel quale per ognuno dei reati presupposto è stato valutato il livello di rischio (alto – medio – basso) per ogni fattispecie di reato rilevante, tenuto conto della probabilità di accadimento e

dell'impatto sulla società.

Sulla base di questa analisi, la Società ha considerato come rilevanti, almeno in via ipotetica, i seguenti Reati Presupposto previsti dal Decreto.

Nelle sezioni seguenti, per ognuna delle sezioni sopra indicate, verranno riportati:
Fattispecie di Reato (con indicazione dei riferimenti normativi).
Aree di rischio (ossia le aree/attività nelle quali potrebbe concretamente essere commesso uno dei reati presupposto).
Principi di comportamento (linee guida e principi generali che indicano le modalità di esecuzione delle attività ritenute a rischio).
Procedure Organizzative Interne Correlate (rimando alle procedure interne aziendali contenenti i controlli ritenuti efficaci).
Flussi informativi verso l'OdV.

FATTISPECIE DI REATO RILEVANTI

A. REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (Artt. 24 e 25 D. Lgs. 231/2001)

A.1 Premessa

Per "Pubblica Amministrazione" si intendono tutti quei soggetti che svolgono una funzione pubblica o un pubblico servizio, secondo le definizioni dettagliate nel Codice Penale e nella normativa vigente. È rilevante tenere presente la distinzione tra:

- Pubblico Ufficiale: colui che esercita poteri autoritativi o certificativi (es. Forze dell'Ordine, giudici, ufficiali giudiziari, personale di pubbliche amministrazioni, ecc.).
- Incaricato di Pubblico Servizio: colui che, anche se privo di poteri autoritativi o certificativi, svolge attività mirate alla cura di interessi pubblici, sotto vigilanza di un'autorità pubblica (es. dipendenti di enti ospedalieri, dell'INPS, dell'INAIL, di aziende energetiche municipali, ecc.).

Il Decreto 231 prevede che l'ente possa essere ritenuto responsabile per reati come corruzione, concussione, truffa ai danni dello Stato, frode informatica, se tali condotte illecite sono realizzate nell'interesse o a vantaggio della Società.

A.2 Fattispecie di reato rilevanti

Secondo gli artt. 24 e 25 del D. Lgs. 231/2001, i principali reati contro la PA rilevanti per Tech Trade S.r.l. sono:

Malversazione a danno dello Stato (art. 316-bis c.p.)
Costituito dalla condotta di chi, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi,

sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità.

Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.)
Costituito dalla condotta di chi, salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.

Truffa aggravata a danno dello Stato o di un ente pubblico o dell'Unione europea (art. 640, comma 2, n. 1 c.p.)
Costituito dalla condotta di chi, con artifizi o raggiri, inducendo lo Stato o altro ente pubblico in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
Il reato si configura nel caso in cui il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Frode informatica (art. 640-ter c.p.)
Costituito dalla condotta di chi alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Frode nelle pubbliche forniture (art. 356 c.p.)
Costituito dalla condotta di chi commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo 355 c.p.

Turbata libertà degli incanti (art. 353 c.p.)
Chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni ovvero ne allontana gli offerenti

Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)
Chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione.

Peculato (art. 314 c.p.)
Costituito dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria.

Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.)
Costituito dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, li destina ad un uso diverso da quello previsto da specifiche disposizioni di legge o da atti aventi forza di legge dai quali non residuano margini di discrezionalità e intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale o ad altri un danno ingiusto.

Peculato mediante profitto dell'errore altrui (art. 316 c.p.)
Costituito dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità

Concussione (art. 317 c.p.)
Costituito dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio il quale, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità.

Corruzione per l'esercizio della funzione (art. 318 c.p.)
Costituito dalla condotta del pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)
Costituito dalla condotta del pubblico ufficiale il quale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa.

Corruzione in atti giudiziari (art. 319-ter c.p.)
Il reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p. sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
Costituito dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, salvo che il fatto costituisca più grave reato, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a terzo, denaro o altra utilità.

Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
Costituito dai fatti di cui agli artt. 318 e 319 c.p. qualora commesso dall'incaricato di un pubblico servizio.

Pene per il corruttore (art. 321 c.p.)
Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.

Istigazione alla corruzione (art. 322 c.p.)
Costituito dalla condotta di chi offre o promette denaro o altra utilità non dovuti a un pubblico ufficiale o a un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o per omettere o ritardare un atto del suo ufficio. Il reato si configura anche nell'ipotesi in cui il pubblico ufficiale o l'incaricato di un pubblico servizio sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri

A.3 Aree di rischio

Sulla base della mappatura interna delle attività aziendali, Tech Trade S.r.l. individua come aree di rischio:

1. Gestione di adempimenti, verifiche e ispezioni da parte di autorità pubbliche (ASL, NAS, Guardia di Finanza, ecc.).
2. Gestione dei rapporti con soggetti pubblici per ottenere finanziamenti, contributi, sovvenzioni.
3. Richiesta e ottenimento di autorizzazioni, licenze, certificazioni (comunali, regionali, ministeriali, ecc.).
4. Selezione e gestione dei fornitori di beni e servizi, con possibile collegamento a soggetti pubblici o procedure di gara pubbliche.
5. Gestione delle Risorse Umane, inclusa la definizione del sistema premiante, soprattutto qualora potrebbero esserci pressioni di pubblici ufficiali su assunzioni e avanzamenti di carriera.
6. Gestione di omaggi, donazioni e sponsorizzazioni, rivolte ad organismi pubblici o che coinvolgano soggetti con poteri decisionali nella PA.

A.4 Principi di Comportamento

A.4.1 Principi di carattere generale

L'Organizzazione ha adottato specifiche procedure per la gestione dei rapporti con le Pubbliche Autorità, incluse quelle relative a ispezioni, controlli e verifiche da parte di organi come NAS, ASL, Guardia di Finanza e altri enti ispettivi.

In particolare, la “Procedura Ufficio Gare” prevede:

- la gestione per fasi distinte (dalla ricezione invito alla chiusura), ciascuna delle quali è assegnata a uno o più soggetti identificabili per nome e funzione;

- la formalizzazione della matrice di responsabilità, che chiarisce i compiti e le attività di ciascun soggetto coinvolto;

- l’obbligo di archiviazione digitale e cartacea della documentazione prodotta e trasmessa, inclusi verbali, PEC e documenti ricevuti dalle stazioni appaltanti;

- la redazione di un “vademecum procedurale” per ciascuna gara, con indicazione del CIG, oggetto, scadenze, modalità e riferimenti;

- l’effettuazione, al termine di ogni procedura, di una verifica critica interna (“lessons learned”) finalizzata al miglioramento continuo.

In caso di accessi, ispezioni o controlli da parte di organi della PA (NAS, ASL, Guardia di Finanza, ecc.), il personale incaricato è tenuto ad attivare tempestivamente le misure previste dalla procedura, ivi incluso l’utilizzo di un modulo standard di segnalazione da trasmettere all’Organismo di Vigilanza in caso di situazioni anomale.

Ai Destinatari del Modello (amministratori, dirigenti, dipendenti, collaboratori e, più in generale, chiunque agisca in nome o per conto della Società) è fatto divieto di porre in essere o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di cui agli artt. 24 e 25 del D. Lgs. 231/2001 già richiamate.

In particolare, i Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione dei rapporti con la Pubblica Amministrazione devono:

1. Operare nel rispetto del Codice Etico e delle procedure interne applicabili.
2. Assicurare che i suddetti rapporti avvengano nel rispetto assoluto di leggi, regolamenti, normative vigenti e princìpi di lealtà, correttezza e chiarezza.
3. In caso di visite ispettive, garantire che agli incontri partecipino almeno due risorse in forza alla Società, ove possibile, per assicurare la trasparenza delle comunicazioni.
4. Verificare che la documentazione da inviare alla Pubblica Amministrazione sia predisposta esclusivamente da persone competenti in materia e preventivamente identificate, così da evitare qualsiasi errore o omissione.
5. Se la documentazione da inviare alla Pubblica Amministrazione è prodotta (anche parzialmente) da terzi (società di ingegneria, periti, consulenti), verificare che la selezione di tali soggetti rispetti le regole interne indicate nella sezione “Selezione e gestione delle consulenze e prestazioni professionali” della Parte Speciale.

A.4.2 Divieti di comportamento

Nell’ambito dei comportamenti sopra indicati, è fatto divieto di:

- Intrattenere rapporti con Funzionari della Pubblica Amministrazione o pubblici ufficiali senza la presenza di almeno un'altra persona (ove possibile) e senza garantire una chiara tracciabilità delle interlocuzioni (ad es. resoconti, verbali).
- Promettere, offrire o versare a qualsiasi titolo somme di denaro, beni o altre utilità (salvo doni o utilità di modico valore, conformi alla normale pratica commerciale), in particolare se finalizzati a promuovere o favorire indebitamente gli interessi della Società. Non è consentito eludere tale divieto attraverso "forme diverse" di aiuti, come incarichi, consulenze, pubblicità, sponsorizzazioni, opportunità di impiego o commerciali, ecc.
- Tenere simili comportamenti (offerte, promesse di denaro o utilità) anche nei confronti di coniugi, parenti o affini dei funzionari pubblici.
- Influenzare impropriamente le decisioni dei funzionari pubblici che trattano o prendono decisioni per conto della Pubblica Amministrazione, attraverso pressioni o vantaggi indebiti.
- Fornire o promettere di fornire, sollecitare o ottenere informazioni/documenti riservati, in violazione dei princìpi di trasparenza e correttezza professionale, tali da compromettere l'integrità di una o di entrambe le parti.
- Far rappresentare la Società da un consulente o da un soggetto "terzo" quando si possano creare conflitti d'interesse; in ogni caso costoro, ed il loro personale, sono soggetti alle stesse prescrizioni che vincolano i Destinatari del Modello.
- Presentare dichiarazioni e attestazioni non precise e/o non veritiere, esibendo documenti in tutto o in parte non corrispondenti alla realtà, od omettendo l'esibizione di documenti veri: ciò vale sia nella fase di richiesta di autorizzazioni e licenze, sia nella fase di rendicontazione verso Enti pubblici (ad esempio, per ottenere finanziamenti o contributi).
- Tenere condotte ingannevoli nei confronti della Pubblica Amministrazione, tali da indurre quest'ultima in errore di valutazione nel corso dell'analisi di richieste di autorizzazioni, licenze, bandi, oppure nell'esecuzione di ispezioni e verifiche.

A.4.3 Principi di comportamento specifici in determinati processi

A.4.3.1 Gestione di adempimenti, verifiche ed ispezioni

Quando Tech Trade S.r.l. viene sottoposta a verifiche o ispezioni da parte di pubbliche autorità (ASL, NAS, Guardia di Finanza, Ministeri competenti, ecc.) o comunque debba adempiere a obblighi amministrativi, chi vi partecipa per conto della Società è tenuto a:

1. Operare nel rispetto del Codice Etico, delle procedure interne e della normativa di riferimento.
2. Assicurare la tracciabilità dei rapporti intrattenuti con la Pubblica Amministrazione, anche attraverso la redazione di verbali o memorandum interni contenenti data, luogo, nominativi dei partecipanti e contenuto degli incontri, da inviare periodicamente (ad es. trimestralmente) al proprio superiore gerarchico.
3. In caso di visite ispettive, far sì che all'incontro siano presenti almeno due risorse della Società, ove possibile, così da garantire trasparenza e supporto reciproco.
4. Comunicare senza ritardo al proprio responsabile gerarchico e, contestualmente, all'Organismo di Vigilanza, eventuali comportamenti posti in essere da funzionari pubblici rivolti a ottenere elargizioni di denaro o altre utilità (anche indirette), nonché qualunque criticità o conflitto d'interesse che sorga nell'ambito di tali rapporti.

È vietato, in tali occasioni, assumere comportamenti volti a:

- Intrattenere colloqui con Funzionari pubblici in assenza di un'altra risorsa interna (ove possibile) o senza documentare l'incontro.
- Promettere, offrire, versare (anche in forma indiretta) somme di denaro, beni o altri benefici per agevolare o omettere atti d'ufficio a favore della Società.
- Influire impropriamente sulle decisioni o sugli esiti dell'ispezione/accertamento, con modalità contrarie alle norme di legge o ai princìpi di correttezza.

A.4.3.2 Ottenimento di finanziamenti, contributi, autorizzazioni, licenze e certificazioni

Nel caso di rapporti con la PA per la richiesta di contributi, finanziamenti, mutui agevolati, nonché per il conseguimento di autorizzazioni, licenze, certificazioni (ambientali, sanitarie, commerciali, ecc.), è fatto obbligo di:

- Assicurare che la documentazione presentata sia predisposta da persone competenti e autorizzate, evitando lacune o false dichiarazioni.
- Garantire la tracciabilità degli incontri con i funzionari pubblici, mediante stesura di note interne.
- Rispettare i criteri di lealtà, correttezza e trasparenza, non cercando scorciatoie illecite (ad es. corrispettivi o regali di valore elevato).

È vietato:

- Promettere od offrire, anche indirettamente, denaro o altra utilità ai funzionari incaricati di esaminare le pratiche, al fine di ottenere un vantaggio per la Società.
- Fornire documenti non veritieri, reticenti, incompleti, o con dati di fatto alterati, nell'ottica di influenzare la decisione della PA.

A.4.3.3 Selezione e gestione dei fornitori di beni e servizi

La selezione e la gestione dei contratti con fornitori può presentare profili di rischio nel caso in cui:

- Vengano stipulati contratti fittizi o sovrafatturati con soggetti collegati a Funzionari pubblici, per costituire "provviste" da destinare alla corruzione o a favori indebiti.
- Si crei un conflitto d'interessi non dichiarato (ad es. fornitore "gradito" a un pubblico ufficiale in cambio di vantaggi).

Pertanto, è indispensabile:

- Introdurre clausole che richiamino l'obbligo del fornitore di rispettare il Modello 231 e il Codice Etico, con possibilità di risoluzione del contratto in caso di violazione.
- Effettuare controlli sulla congruità dei prezzi, la regolarità della fornitura e la coincidenza tra i soggetti che emettono la fattura e quelli che effettivamente prestano il servizio.
- Documentare in modo trasparente i pagamenti, garantendo l'assenza di fondi non giustificati.

È vietato:

● Creare fondi extracontabili o destinare pagamenti a soggetti non identificati, allo scopo di ottenere vantaggi indebiti nei rapporti con la PA.
● Effettuare pagamenti non supportati da adeguata documentazione o riconoscere compensi sproporzionati rispetto al servizio reale svolto.

A.4.3.4 Gestione HR e sistema premiante

Nel processo di assunzione del personale, definizione dei compensi o avanzamenti di carriera, e gestione di stage o collaborazioni, è fatto obbligo di:

● Selezionare i candidati sulla base di criteri di meritocrazia e senza discriminazioni, evitando favoritismi legati a funzionari o incaricati di pubblico servizio.
● Assicurare la regolarità dei contratti di lavoro (in termini di contributi, permessi di soggiorno, ecc.).

È vietato:

● Assumere persone "indicate" dal Funzionario pubblico o da suoi congiunti, per finalità corruttive o al fine di ricevere trattamenti di favore.
● Promettere avanzamenti di carriera o bonus economici a soggetti vicini a pubblici ufficiali in cambio di vantaggi illeciti.

A.4.3.5 Gestione di omaggi, donazioni e sponsorizzazioni

Le liberalità e gli atti di cortesia (omaggi, inviti, sponsorizzazioni) rivolti a soggetti pubblici possono costituire una forma di corruzione se superano i limiti di un valore modesto e di finalità istituzionali.

● Consentiti solo regali d'uso di modico valore (es. gadget, agende, penne) in occasioni festività o ricorrenze, compatibili con le consuetudini commerciali.
● Documentare adeguatamente ogni liberalità, inviando all'OdV copia delle relative pezze giustificative, se rientrante in un piano di omaggi aziendali.
● Verificare che le sponsorizzazioni siano effettivamente giustificate da esigenze di promozione dell'immagine aziendale e non costituiscano uno strumento per finanziare indebitamente soggetti pubblici.

È vietato:

● Effettuare omaggi e liberalità, comprese sponsorizzazioni, a soggetti pubblici in violazione delle prassi, con l'intento di influenzare l'operato o le decisioni di funzionari o incaricati di pubblico servizio.
● Accordare vantaggi di qualsiasi natura (ad es. assunzioni, consulenze, abbonamenti, agevolazioni, acquisti) a funzionari pubblici o loro familiari, connessi al rapporto d'affari con la Società.

A.4.4 Clausole contrattuali e procedure organizzative

Per garantire l'effettività di tali prescrizioni, la Società inserisce nei contratti con fornitori e partner commerciali clausole che:

- Attestino la conoscenza del Modello 231 e del Codice Etico da parte del fornitore.
- Impegnino il fornitore a rispettare le norme previste dal Modello e a dotarsi di procedure anti-reato.
- Prevedano, in caso di false dichiarazioni o violazione degli obblighi, la possibilità di recesso o risoluzione contrattuale per inadempimento.

Inoltre, Tech Trade S.r.l. adotta:

- Procedure interne per la qualificazione e la selezione dei fornitori, la gestione delle consulenze e delle prestazioni professionali, con check sull'identità e la reputazione della controparte, l'analisi di congruità dei corrispettivi, la tracciabilità dei pagamenti.
- Procedure di controllo sulle attività dei dipendenti che intrattengono contatti con la PA (ad es. controllo a campione delle pratiche, obbligo di inoltrare copia delle comunicazioni inviate alla PA, registri delle visite ispettive, ecc.).

A.4.5 Sanzioni disciplinari

Qualora i comportamenti dei Destinatari violassero i principi di cui sopra (o emergessero omissioni, reticenze, dichiarazioni false nei rapporti con la PA), la Società applicherà le sanzioni disciplinari previste dalla Parte Generale del Modello 231 e dal relativo sistema disciplinare (ad esempio, richiamo scritto, sospensione, licenziamento o risoluzione del rapporto di collaborazione/consulenza).

Questi Principi di Comportamento – così come formulati e dettagliati – costituiscono parte integrante del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 e devono essere scrupolosamente osservati da tutti i Destinatari, a tutela della legalità e della reputazione di Tech Trade S.r.l.

A.5 Flussi informativi all'Organismo di Vigilanza

- Segnalazione immediata (in forma scritta) di qualsiasi comportamento anomalo o sospetto, come richieste di favori, contributi illeciti, pressioni indebite da parte di soggetti pubblici.
- Comunicazione periodica di rapporti avuti con la PA, comprendendo:
  - Elenco delle ispezioni e visite ispettive.
  - Lista di eventuali finanziamenti o contributi richiesti e ottenuti.
  - Sponsorizzazioni ed erogazioni a enti pubblici o comunque "vicini" alla PA.
  - Assunzioni effettuate, con particolare riferimento a soggetti segnalati o a parenti di funzionari pubblici.

B. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

(Art. 24-bis D. Lgs. 231/2001)

B.1 Premessa

La costante digitalizzazione dei processi aziendali rende fondamentale la protezione dei sistemi informativi e dei dati. Il D. Lgs. 231/2001 considera reato l'accesso abusivo a sistemi informatici, la diffusione di codici d'accesso, la frode informatica, il danneggiamento di dati e programmi, etc.

B.2 Fattispecie di reato rilevanti

Le fattispecie (artt. 24-bis e 25-novies) includono:

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
Costituito dalla condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'ingresso in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
Costituito dalla condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

Detenzione e diffusione abusiva di codici di accesso a sistemi informativi o telematici (art. 615- quater c.p.)
Costituito dalla condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
Costituito dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o

da altro ente pubblico, o comunque di pubblica utilità (art. 635-ter c.p.)
Costituito dalla condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo il fatto non costituisca più grave reato.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
Costituito dalla condotta di chi, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento salvo che il fatto costituisca più grave reato.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
Costituito dalla condotta descritta al precedente articolo 635-quater, qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Estorsione (art. 629 c.p.)
Chiunque, mediante le condotte di cui agli articoli 615 ter, 617 quater, 617 sexies, 635 bis, 635 quater e 635 quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno (art. 629 c.p.).

Documenti informatici falsi (art. 491-bis c.p.)
Costituito dalle ipotesi di falsità, materiale o ideologica, previste nel capo III del c.p., commesse su documenti informatici pubblici aventi efficacia probatoria.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)
Costituito dalla condotta del soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a se´ o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

B.3 Aree di rischio

1. Utilizzo dei sistemi informativi aziendali (PC, server, database, rete interna).
2. Gestione e custodia di credenziali di autenticazione (password, token, smart card).
3. Possibili installazioni non autorizzate di software o introduzione di malware.
4. Scambio di dati con terze parti o fornitori di servizi informatici.

B.4 Principi di comportamento

- La Società ha previsto un presidio di controllo mediante soggetto incaricato esterno con compiti specifici di configurazione e aggiornamento dei sistemi di sicurezza informatica, tra cui firewall, antivirus, gestione delle credenziali di accesso e aggiornamenti software periodici.
- È fatto obbligo di utilizzo della firma digitale per tutte le comunicazioni ufficiali verso soggetti pubblici e di conservazione dei log di accesso in un'infrastruttura cloud protetta, conforme agli standard di sicurezza e soggetta a backup periodico.
- L'accesso a piattaforme non autorizzate è vietato; sono ammessi esclusivamente sistemi cloud e strumenti digitali che siano conformi agli standard internazionali ISO/IEC 27001 o equivalenti in materia di gestione della sicurezza delle informazioni.
- Il responsabile IT redige con cadenza annuale un report interno che riepiloga le attività di aggiornamento, le minacce rilevate e neutralizzate, nonché gli interventi effettuati. Tali report sono resi disponibili all'Organismo di Vigilanza.
- È inoltre previsto un audit interno a campione, con frequenza almeno trimestrale, volto a verificare l'accesso non autorizzato a dati, la conformità delle credenziali utilizzate e il rispetto delle policy aziendali in tema di sicurezza informatica.
- Obbligo di utilizzare le risorse IT (reti, PC, dispositivi mobili) solo per fini lavorativi e nel rispetto delle procedure interne di sicurezza.
- Divieto di condividere password e credenziali di accesso, divulgare codici, superare le misure di protezione dei sistemi (anche di soggetti terzi).
- Dovere di custodire i dispositivi (compresi laptop e smartphone aziendali) in modo sicuro, bloccando lo schermo se si lascia la postazione.
- Assoluto divieto di introdurre software o programmi extra senza autorizzazione della Funzione IT (ad es. software P2P, tool pirata).
- Tracciabilità delle modifiche ai documenti informatici, ad es. attraverso versioning o sistemi di archiviazione con registrazione delle attività.

B.5 Flussi informativi all'Organismo di Vigilanza

- Segnalazione tempestiva di incidenti informatici (data breach, intrusioni, manomissioni) o di comportamenti anomali (download di software sospetti, uso improprio della rete).
- Report periodici (ad es. annuali) da parte della Funzione IT sulla gestione della sicurezza informatica, sugli aggiornamenti antivirus, sui backup e sulle policy di accesso ai sistemi.

C. DELITTI DI CRIMINALITÀ ORGANIZZATA (Art. 24-ter D. Lgs. 231/2001)

C.1 Premessa

Il Decreto 231 include, tra i reati presupposto, anche i reati associativi (art. 416 c.p.) e l'associazione di tipo mafioso (art. 416-bis c.p.), lo scambio elettorale politico-mafioso (art.

416-ter c.p.), l'associazione finalizzata al traffico di sostanze stupefacenti (art. 74 D.P.R. 309/1990) e altri reati connessi (es. detenzione illegale di armi).

C.2 Fattispecie di reato rilevanti

Associazione per delinquere (art. 416 c.p.c.)
Costituito dalla condotta di tre o più persone che si associano allo scopo di commettere più delitti, per il sol fatto della partecipazione.

Associazioni di tipo mafioso, anche straniere (art. 416-bis c.p.)
Costituito dalla condotta di chi fa parte di un'associazione di tipo mafioso formata da tre o più persone

Scambio elettorale politico-mafioso (art. 416-ter c.p.)
hi accetta la promessa di procurare voti mediante le modalità previste dal terzo comma dell'articolo 416-bis in cambio dell'erogazione o della promessa di erogazione di denaro o di altra utilità

C.3 Aree di rischio

1. Gestione degli acquisti, soprattutto se coinvolgono soggetti potenzialmente infiltrati dalla criminalità organizzata (ad es. fornitori "di comodo").
2. Gestione di flussi monetari e finanziari (pagamenti non tracciati, contanti, canali opachi).
3. Affidamento di servizi a società terze, in settori particolarmente a rischio (trasporti, logistica, smaltimento rifiuti, cantieri).

C.4 Principi di comportamento

- La Società adotta una procedura specifica per la qualificazione dei fornitori e degli appaltatori operanti in settori a rischio criminalità organizzata, finalizzata a prevenire il rischio di infiltrazioni mafiose o di soggetti contigui a gruppi criminali.
In particolare, la procedura prevede il controllo preventivo della visura camerale, credit safe ed eventuale Modello organizzativo ex D.Lgs. 231/2001 nonché, ove disponibile, la verifica dell'inserimento nella white list prefettizia ai sensi dell'art. 1, comma 52, della L. 190/2012.
- È richiesta un'autocertificazione antimafia da parte del legale rappresentante per tutti i contratti di fornitura o appalto aventi un valore superiore a €100.000.
- Nei contratti è inoltre inserita una clausola risolutiva espressa, che consente la cessazione automatica del rapporto in caso di accertata vicinanza del fornitore o appaltatore ad ambienti o soggetti a rischio criminale.
- Per i settori a maggiore esposizione (tra cui trasporto, logistica, smaltimento rifiuti, vigilanza privata) è obbligatorio effettuare un audit reputazionale preventivo, anche sui subappaltatori eventualmente coinvolti.
- Ogni operazione di valore superiore a €100.000, oppure ricompresa in settori classificati come critici, deve essere preventivamente comunicato all'Organismo di Vigilanza, allegando l'esito della valutazione di conformità e reputazione del soggetto contraente.

- Obbligo di trasparenza nei pagamenti, vietando ogni forma di transazione non adeguatamente documentata o effettuata in contanti.
- Clausole contrattuali che richiedano il rispetto del Modello 231 e del Codice Etico; risoluzione del rapporto in caso di accertata vicinanza mafiosa.
- Monitoraggio costante dei contratti e delle fatture, per assicurarsi che non siano fittizi o sovrafatturati finalizzati a costituire "provviste" illegali.

C.5 Flussi informativi all'Organismo di Vigilanza

- Segnalazioni immediate di appalti anomali, pagamenti sospetti, fornitori non in regola.
- Report periodici sugli esiti di eventuali verifiche antimafia e sulle procedure adottate per la selezione e la valutazione dei partner commerciali.

D. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (Art. 25-bis.1 del Decreto)

D.1 Premessa

I delitti contro l'industria e il commercio tutelano la correttezza nei rapporti commerciali e proteggono da pratiche concorrenziali scorrette, frodi commerciali, etc. Per una società che opera soprattutto nell'e-commerce, è cruciale assicurare la veridicità delle informazioni sui prodotti venduti e la regolarità dei marchi e dei brevetti utilizzati.

D.2 Fattispecie di reato rilevanti

Turbata libertà dell'industria o del commercio (art. 513 c.p.)
Costituito dalla condotta di chi adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio.

Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)
Costituito dalla condotta di chi nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia.

Frodi contro le industrie nazionali (art. 514 c.p.)
Costituito dalla condotta di chi, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagiona un nocumento all'industria nazionale.

Frode nell'esercizio del commercio (art. 515 c.p.)
Costituito dalla condotta di chi, nell'esercizio di una attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
Costituito dalla condotta di chi pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)
Costituito dalla condotta di chi, salva l'applicazione degli articoli 473 e 474, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso e chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al punto precedente. Tali condotte sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)
Costituito dalla condotta di chi contraffà o comunque altera indicazioni geografiche o denominazioni di origine di prodotti agroalimentari e chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i medesimi prodotti con le indicazioni o denominazioni contraffatte.

D.3 Aree di rischio

1. Acquisto e rivendita di prodotti (gestione e-commerce), con possibili false indicazioni sulla qualità, l'origine o la provenienza.
2. Promozione e marketing: presentazioni che potrebbero ingannare il consumatore sulla reale natura del prodotto.
3. Rapporti con concorrenti, dove pratiche scorrette (es. boicottaggi, minacce) violerebbero la libertà di commercio.

D.4 Principi di comportamento

- La Società ha previsto specifici presìdi interni volti a prevenire la commercializzazione di prodotti contraffatti, di provenienza non tracciata o difformi da quanto dichiarato.
- È fatto obbligo per il personale incaricato della redazione delle schede prodotto di indicare in maniera completa e verificabile la fonte commerciale, il codice identificativo e il fornitore di origine. Tali informazioni devono essere archiviate e conservate per un periodo minimo di cinque anni.

- È inoltre vietato l'utilizzo di immagini non originali o prive di licenza d'uso: l'inserimento di immagini senza adeguata autorizzazione costituisce violazione disciplinare, con conseguenze sanzionatorie a carico del responsabile.
- La Società adotta un sistema di controllo qualità in ingresso, finalizzato alla verifica della conformità tra la descrizione commerciale e le caratteristiche effettive del prodotto ricevuto.
- In caso di contestazioni da parte dei clienti che sollevino dubbi su autenticità, contraffazione, imitazione o provenienza dubbia del prodotto, è previsto l'obbligo di segnalazione immediata al Responsabile Legale e/o al Responsabile Compliance, affinché possano essere attivate le verifiche e le tutele previste dal Modello 231.
- Garantire elevati standard qualitativi e informativi sui prodotti, fornendo caratteristiche, provenienza e qualità in modo vero ed esaustivo.
- Verificare l'integrità dei prodotti al momento della ricezione, controllando eventuali abrasioni di numeri seriali, packaging alterati, segni distintivi contraffatti.
- Divieto di consegnare ai clienti merce diversa da quella pattuita (per qualità, quantità o origine).
- Vietato utilizzare strategie di mercato aggressive basate su minaccia o violenza ai danni di concorrenti, o vendere prodotti recanti segni di riconoscimento falsi/mendaci.

D.5 Flussi informativi all'Organismo di Vigilanza

- Segnalazione immediata di reclami o contestazioni sulla presunta contraffazione di marchi, o di avvisi da parte delle Autorità a seguito di controlli su prodotti e marchi commercializzati.
- Comunicazione e archiviazione di eventuali prodotti "non conformi" (ad es. resi dai clienti) e azioni intraprese (richiamo, sostituzione, segnalazione ai fornitori).

E. REATI SOCIETARI - REATI TRIBUTARI

(Artt. 25-ter e 25-quinquiesdecies D. Lgs. 231/2001)

E.1 Premessa

La disciplina del D. Lgs. 231/2001 ricomprende, tra i reati presupposto, anche quelli di natura societaria (art. 25-ter) e tributaria (art. 25-quinquiesdecies). Tali reati possono coinvolgere l'ente nel caso in cui soggetti apicali o sottoposti, agendo nell'interesse o a vantaggio della Società, pongano in essere condotte come:

- Falsificazioni o omissioni nei bilanci e nelle comunicazioni sociali.
- Impedimenti agli organi di controllo, operazioni in pregiudizio dei creditori, corruzione tra privati.
- Dichiarazioni fraudolente o omesse, emissione di fatture per operazioni inesistenti, sottrazione fraudolenta al pagamento di imposte, e altre condotte che violano la normativa fiscale.

L'obiettivo di questa Parte Speciale è dunque di definire i Principi di Comportamento e le procedure da seguire per prevenire la commissione di tali reati, identificare le Aree di rischio e stabilire i flussi informativi verso l'Organismo di Vigilanza.

E.2 Fattispecie di reato rilevanti

Tra i reati societari più significativi che possono fondare la responsabilità amministrativa dell'ente si annoverano:

False comunicazioni sociali (art. 2621 c.c.)
Costituito dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori i quali, fuori dai casi previsti dall'art. 2622, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore. La punibilità è estesa anche al caso in cui le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

Impedito controllo (art. 2625 c.c.)
Costituito dalla condotta degli amministratori i quali, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci e ad altri organi sociali.

Indebita restituzione dei conferimenti (art. 2626 c.c.)
Costituito dalla condotta degli amministratori i quali, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

Illegale ripartizione di utili e riserve (art. 2627 c.c.)
Costituito dalla condotta degli amministratori che, salvo che il fatto non costituisca più grave reato, ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
Costituito dalla condotta degli amministratori i quali, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge; ovvero degli

amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Costituito dalla condotta degli amministratori i quali, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

Corruzione tra privati (art. 2635 c.c.)
Costituito dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci, dei liquidatori o dei soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti precedentemente indicati, che, salvo che il fatto costituisca più grave reato, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società.

Illecita influenza sull'assemblea (art. 2636 c.c.)
Costituito dalla condotta di chi, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)
Costituito dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori di società o enti e degli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l´esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima ovvero, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)
È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.
Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili

obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)
Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:
a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.
Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.
Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)
È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.
Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.
Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)
Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili

o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)
E' punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.
E' punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000)
Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:
a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.
Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.
Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).

Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000)
È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte

sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.
È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.
Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000)
E' punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.
E' punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

E.3 Aree di rischio

Nel contesto societario e tributario, Tech Trade S.r.l. individua le seguenti aree di rischio:

1. Predisposizione del bilancio e delle altre comunicazioni sociali (relazioni, note integrative, prospetti di sintesi), con possibili omissioni o falsità.
2. Gestione delle scritture contabili e dei registri obbligatori, inclusa la conservazione e l'archiviazione dei documenti (fatture, libri sociali, registri IVA, ecc.).
3. Gestione delle operazioni straordinarie (fusioni, scissioni, conferimenti, cessioni di rami d'azienda), che possono pregiudicare i creditori se non vengono rispettate le norme di legge.
4. Rapporti con gli Organi di controllo societario (Collegio Sindacale, Revisore Legale, Società di revisione) e con le Autorità di vigilanza.
5. Rapporti con il consulente fiscale esterno, predisposizione delle dichiarazioni dei redditi e dell'IVA, compensazioni, pagamenti di imposte e contributi.
6. Gestione delle fatture attive e passive, con rischio di emissione o registrazione di fatture relative a operazioni inesistenti o documenti falsi.
7. Eventuali accordi infragruppo (se presenti) o contratti con soggetti correlati, che possano dare luogo a violazioni fiscali o elusione di norme societarie.

E.4 Principi di comportamento

E.4.1 Principi generali

La Società adotta criteri di trasparenza, tracciabilità e separazione delle funzioni nella redazione della documentazione societaria e contabile, al fine di prevenire la commissione di reati societari.

Tutti i dati inseriti nei bilanci, nei libri sociali e nei documenti previsti dalla normativa civilistica devono essere corretti, veritieri e verificabili, in conformità ai principi contabili nazionali e internazionali di riferimento.

La predisposizione delle scritture contabili e delle relazioni finanziarie è affidata a personale qualificato e soggetta a verifica incrociata da parte del Responsabile Amministrativo e, se presente, del Revisore.

È fatto divieto ai Destinatari (amministratori, dirigenti, dipendenti, collaboratori, consulenti) di:

- Porre in essere o concorrere a porre in essere condotte che integrino i reati di cui all'art. 25-ter e 25-quinquiesdecies.
- Fornire o utilizzare documentazione societaria o contabile mendace, incompleta, reticente, per indurre in errore soci, creditori, revisori o il Fisco.
- Eludere le procedure interne di controllo o occultare documenti contabili (o bloccarne l'accesso) per impedire l'esercizio delle funzioni di vigilanza e controllo.
- Creare o gestire fondi extracontabili, provviste di denaro non giustificate, voci di spesa sproporzionate, spese non documentate o per operazioni inesistenti.
- Corrompere o tentare di corrompere soggetti privati (es. manager di un'altra azienda) al fine di acquisire vantaggi commerciali, come sconti, appalti, contratti.

E.4.2 Principi specifici per i reati societari

1. Veridicità e completezza delle informazioni contabili
   - Ogni operazione deve trovare adeguato riscontro nei registri contabili e nella documentazione di supporto, che deve essere conservata e archiviata in modo ordinato.
2. Regolare tenuta dei libri e dei registri sociali
   - I libri assembleari, i libri del Consiglio di Amministrazione e i libri contabili devono contenere in maniera fedele le risultanze delle deliberazioni adottate. È vietato ostacolare la lettura, la consultazione, la verifica di tali documenti a chi ne abbia diritto (sindaci, revisori, soci secondo legge).
3. Controlli interni e flussi informativi
   - È obbligatorio rispettare le procedure per la predisposizione del bilancio, il calcolo dell'utile distribuibile, la formazione delle riserve. Laddove siano previste verifiche incrociate (es. firma congiunta, controllo di un secondo soggetto), esse vanno rigorosamente osservate.
4. Operazioni in pregiudizio dei creditori
   - In caso di riduzione del capitale, fusione o scissione societaria, è indispensabile attendere l'espletamento di tutti gli adempimenti di legge (depositi, pubblicazioni, pareri) e non procedere in modo tale da danneggiare i diritti dei creditori, che devono essere posti nelle condizioni di far valere le proprie ragioni.
5. Corruzione tra privati
   - Ogni Destinatario è tenuto a evitare di offrire, promettere o ricevere somme di denaro o altre utilità (viaggi, regali di valore elevato, consulenze fittizie) per indurre o ricompensare comportamenti contrari ai doveri di ufficio di un soggetto privato.

E.4.3 Principi specifici per i reati tributari

1. Veridicità delle dichiarazioni fiscali
   - ○ È vietato inserire in dichiarazione elementi passivi fittizi o ricavi attivi inferiori al reale, mediante fatture per operazioni inesistenti o artifizi.
   - ○ Ogni giustificativo di spesa deve corrispondere a un'operazione effettivamente avvenuta, documentata e correttamente contabilizzata.
2. Evitare emissioni fittizie
   - ○ Non si possono emettere fatture o altri documenti per operazioni inesistenti, utili a consentire a terzi (siano essi soggetti del Gruppo o estranei) di evadere le imposte.
3. Conservazione della documentazione
   - ○ Tutte le scritture contabili, incluse fatture, registri IVA, libri sociali, DEVONO essere correttamente conservate per i periodi stabiliti dalle norme, evitando distruzioni o occultamenti che rendano impossibile la ricostruzione dei redditi.
4. Divieto di sottrazione fraudolenta al pagamento di imposte
   - ○ Non è consentito compiere atti dispositivi del patrimonio (vendite simulate, donazioni fittizie, costituzione di vincoli su beni) al solo fine di eludere la riscossione coattiva da parte dell'Erario.
   - ○ Nel caso di utilizzo di compensazioni di crediti, occorre verificarne la legittimità e la capienza effettiva.
5. Procedure di controllo e rapporti con il consulente fiscale
   - ○ Il Responsabile Amministrativo deve garantire la tracciabilità di tutte le fasi di predisposizione delle dichiarazioni, e la corrispondenza dei dati inviati al consulente fiscale esterno. Eventuali anomalie o richieste sospette da parte del consulente vanno immediatamente segnalate all'OdV.

E.5 Flussi informativi all'Organismo di Vigilanza

Per assicurare un efficace sistema di vigilanza:

1. Segnalazioni immediate
   - ○ Qualunque Destinatario che rilevi potenziali violazioni dei principi summenzionati, o comportamenti sospetti (es. richiesta di emettere fatture gonfiate, uso di documenti falsi, ordini dell'alta direzione di occultare scritture) deve darne immediata comunicazione scritta all'OdV.
2. Report periodici
   - ○ Con cadenza stabilita (ad es. semestrale o annuale), il Responsabile Amministrativo invia all'OdV:
   - ■ Una sintesi delle operazioni straordinarie (fusioni, scissioni, conferimenti) che possono coinvolgere reati societari.
   - ■ Una panoramica delle dichiarazioni fiscali presentate e delle principali risultanze.
   - ■ Gli esiti di eventuali controlli o ispezioni da parte dell'Amministrazione Finanziaria o di altre Autorità competenti (ad es. GdF).
   - ■ Ogni modifica o integrazione alle procedure interne in materia contabile, finanziaria e fiscale.
3. Comunicazioni sulle attività di controllo interno

○ Laddove l'azienda adotti un sistema di audit interno o un Revisore Legale, eventuali rapporti di audit che segnalino criticità significative in materia di rappresentazione contabile, di gestione fiscale o di trasparenza societaria devono essere prontamente messi a disposizione dell'OdV.

4. Richieste di assistenza legale

○ Qualora venga avviato un procedimento penale a carico di un Destinatario per reati societari o tributari rilevanti, la persona interessata deve informare la Società (ed eventualmente chiedere assistenza legale). L'Ufficio Legale e l'OdV dovranno essere tempestivamente avvisati.

F. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA NONCHÉ AUTORICICLAGGIO

(Art. 25-octies D.Lgs. 231/2001; artt. 648, 648-bis, 648-ter, 648-ter.1 c.p.)

E.1 Premessa

La disciplina del D. Lgs. 231/2001 ricomprende, tra i reati presupposto, anche i delitti di ricettazione, riciclaggio, impiego di denaro/beni/utilità di provenienza illecita e autoriciclaggio (art. 25-octies). L'ente può risponderne quando soggetti apicali o sottoposti, nell'interesse o a vantaggio della Società, pongano in essere condotte finalizzate a sostituire, trasferire, impiegare o occultare beni di origine delittuosa, ostacolando l'identificazione della provenienza.

L'obiettivo di questa Parte Speciale è dunque di definire i Principi di Comportamento e le procedure da seguire per prevenire la commissione di tali reati, identificare le Aree di rischio e stabilire i flussi informativi verso l'Organismo di Vigilanza.

E.2 Fattispecie di reato rilevanti

Tra i reati societari più significativi che possono fondare la responsabilità amministrativa dell'ente si annoverano:

Ricettazione (art. 648 c.p.)
Costituito dalla condotta di chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque s'intromette nel farle acquistare, ricevere od occultare.

Riciclaggio (art. 648-bis c.p.)

Costituito dalla condotta di chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)
Costituito dalla condotta di chi, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

Autoriciclaggio (art. 648 ter.1 c.p.)
Costituito dalla condotta di chi chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

E.3 Aree di rischio

In relazione ai predetti reati si individuano le seguenti aree di rischio:

1. Incassi e pagamenti atipici (contante, carte prepagate, criptovalute, conti esteri; frazionamenti).
2. Gestione tesoreria e movimentazioni tra conti interni/esterni; anticipi a fornitori/intermediari; rimborsi spese.
3. Selezione e qualificazione di clienti/fornitori/intermediari, specie esteri o di settori ad alto rischio.
4. Operazioni straordinarie (acquisti di rami/partecipazioni, cessioni, joint venture) con controparti poco trasparenti.
5. Magazzino e beni ad alta mobilità/valore (facile ricollocazione, seriali mancanti, triangolazioni).
6. Rapporti con consulenti e agenti (mandati, provvigioni, success fee) e donazioni/sponsorizzazioni.
7. Gestione fatture e contratti con termini/combinazioni di pagamento incoerenti con la prassi di mercato.

E.4 Principi di comportamento

E.4.1 Principi generali

La Società adotta criteri di: Tracciabilità integrale dei flussi finanziari; conoscenza della controparte (KYC) proporzionata al rischio; separazione dei ruoli tra chi ordina, autorizza e contabilizza; no cash salvo limiti di legge e previa autorizzazione; conservazione documentale completa.

E.4.2 Principi specifici per i reati di ricettazione/riciclaggio/impiego/autoriciclaggio

1. Origine lecita dei fondi e dei beni
   - Si gestiscono solo fondi e beni di provenienza chiara e documentata (contratti, fatture, evidenze bancarie). È vietato accettare somme o asset di origine ignota o sospetta, inclusi contanti fuori policy o oltre le soglie di legge, strumenti anonimi o cripto non tracciabili. In caso di dubbio, l'operazione si ferma e si attiva il controllo.
2. Pagamenti e incassi tracciabili
   - Si utilizzano esclusivamente mezzi tracciabili (ad es. bonifico; assegno non trasferibile) su conti intestati alla controparte contrattuale. È vietato pagare o incassare su conti di terzi non giustificati, su carte ricaricabili o tramite money transfer; vietate le catene di passaggi senza causale economica e i frazionamenti artificiosi per eludere soglie di controllo.
3. KYC e due diligence sulla controparte
   - Prima di avviare o proseguire un rapporto si identificano controparte e titolare effettivo, si verificano PEP, sanzioni/embargo e Paesi ad alto rischio; si raccolgono i documenti proporzionati al rischio (visure, certificazioni fiscali, referenze). È vietato avviare o mantenere rapporti con KYC incompleta o con esito negativo, salvo mitigazioni formali approvate.
4. Coerenza economica dell'operazione
   - Prezzi, termini di pagamento e condizioni devono essere coerenti con il mercato, l'oggetto e i rischi dell'operazione. Sono vietati compensi sproporzionati, pagamenti in contanti o su conti esteri senza valida ragione, triangolazioni ingiustificate e clausole opache che rendano non verificabile la causa del pagamento.
5. Gestione di beni e magazzino
   - Tutti i movimenti devono essere tracciati (carico/scarico, inventari, numeri di serie). È vietato introdurre beni senza documentazione idonea, accettare merci con seriali abrasi/alterati, eseguire resi o sostituzioni fittizi utilizzati per 'ripulire' provenienze dubbie.
6. Consulenze e intermediazioni
   - Ogni incarico deve essere contrattualizzato (oggetto, durata, deliverable, compenso proporzionato) e rendicontato. È vietato affidare incarichi verbali o generici, riconoscere success fee non giustificate, pagare a soggetti diversi dal contraente, utilizzare retrocommissioni o fatture per prestazioni non svolte.
7. Donazioni e sponsorizzazioni
   - Si effettuano solo tramite canali autorizzati, previa verifica del beneficiario e della finalità trasparente; si documentano esiti e benefici. È vietato usare tali strumenti per trasferire fondi a soggetti collegati o non tracciabili, o per aggirare limiti su pagamenti o regali.
8. Segnalazione tempestiva e blocco cautelativo
   - Ogni operazione atipica o sospetta deve essere segnalata immediatamente all'OdV e al CFO/Responsabile Amministrazione; i pagamenti si sospendono finché i controlli non sono conclusi. È vietato ritardare, frammentare o omettere informazioni rilevanti; è garantita la tutela del segnalante secondo la policy di whistleblowing.
9. Conservazione e integrità delle evidenze
   - Contratti, fatture, mezzi di pagamento, corrispondenza, check-list KYC e approvazioni sono archiviati per i termini di legge, con tracciabilità degli accessi. È vietata qualsiasi distruzione, alterazione o occultamento di documenti che ostacoli i controlli o l'accertamento della provenienza dei fondi.

E.5 Flussi informativi all'Organismo di Vigilanza

Per assicurare un efficace sistema di vigilanza:

1. Segnalazioni immediate di operazioni anomale
   - Qualsiasi transazione che presenti profili atipici (contante oltre le soglie/policy, triangolazioni senza giustificazione economica, pagamenti a soggetti terzi non previsti dal contratto, richieste di "schermare" la provenienza dei fondi o di frammentare i pagamenti) deve essere segnalata senza indugio all'OdV e al CFO/Responsabile Amministrazione tramite i canali dedicati (e-mail/portale whistleblowing, modulistica interna). La segnalazione deve contenere i fatti essenziali, i documenti disponibili e l'eventuale blocco cautelativo già disposto. È fatto divieto di proseguire l'operazione finché non vi sia un esito formale dei controlli.
2. Report periodici strutturati del CFO/Responsabile Amministrazione
   - Con frequenza almeno annuale (o più ravvicinata in funzione del rischio), il CFO invia all'OdV un rapporto organico che includa: (i) la mappa delle controparti ad alto rischio (con indicazione dei fattori: Paese, settore, PEP, esiti KYC), (ii) l'elenco delle operazioni eccezionali o fuori standard (anche se poi autorizzate), (iii) gli esiti delle verifiche KYC svolte nel periodo (nuove attivazioni, aggiornamenti, rigetti e mitigazioni), (iv) l'elenco delle deroghe concesse rispetto alle policy, con motivazione, soggetti che le hanno approvate e misure compensative. Il report deve consentire all'OdV una valutazione di tendenza (aree, processi, controparti più esposte).
3. Flussi sugli audit interni/esterni con rilievi AML/KYC
   - Gli esiti degli audit interni e delle revisioni esterne che toccano tracciabilità dei flussi, controlli sui pagamenti, segregazione dei ruoli, conservazione documentale e adeguata verifica della clientela sono trasmessi integralmente all'OdV. Per ogni rilievo si indicano gravità, cause, azioni correttive, responsabile e tempi di chiusura; l'avanzamento dei piani di remediation è monitorato fino alla completa attuazione. Eventuali limitazioni di portata o aree non testate devono essere evidenziate, per consentire all'OdV di richiedere approfondimenti mirati.
4. Informativa legale su procedimenti e richieste delle Autorità
   - L'Ufficio Legale comunica tempestivamente all'OdV l'avvio di indagini, sequestri, ispezioni o richieste dell'Autorità (G.d.F., A.G., UIF, altre) riconducibili ai reati di cui agli artt. 648, 648-bis, 648-ter, 648-ter.1 c.p. e alle connesse violazioni amministrative. L'informativa comprende il quadro dei fatti, gli atti ricevuti, le misure cautelative adottate dall'azienda (es. sospensione rapporti, blocco pagamenti, conservazione rafforzata dei dati), nonché il piano di difesa e cooperazione predisposto con i consulenti. Ogni sviluppo (archiviazioni, richieste integrative, nuove contestazioni) è comunicato fino alla chiusura del procedimento.

G. DELITTI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME (Art. 25-septies D. Lgs. 231/2001)

G.1 Premessa

Le norme in materia di salute e sicurezza sul lavoro stabiliscono che, in caso di infortunio o di malattia professionale riconducibile a violazioni delle disposizioni antinfortunistiche, la Società possa essere chiamata a rispondere penalmente per omicidio colposo o lesioni colpose gravi o gravissime (artt. 589 e 590, comma 3 c.p.), ai sensi del D. Lgs. 231/2001. Tech Trade S.r.l.

è dunque tenuta ad adottare tutte le misure idonee a prevenire gli infortuni e le malattie professionali nel contesto delle proprie attività.

In particolare, l'azienda dispone di un laboratorio dedicato alla rigenerazione di toner e cartucce per stampanti, che comporta rischi specifici per la salute e la sicurezza dei lavoratori (ad esempio: esposizione a polveri sottili, rischi chimici e meccanici, movimentazione manuale di carichi, ecc.). Per questo motivo, Tech Trade S.r.l. ha sviluppato un sistema di gestione della sicurezza in conformità al D. Lgs. 81/2008, integrato nel Modello 231, per prevenire gli infortuni e le patologie correlate all'attività lavorativa.

G.2 Fattispecie di reato rilevanti

Le fattispecie contemplate dall'art. 25-septies del D. Lgs. 231/2001 sono:

Omicidio colposo (art. 589 c.p.)
Costituito dalla condotta di chi cagiona per colpa la morte di una persona, con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Lesioni colpose gravi o gravissime (art. 590, 3° comma, c.p.)
Costituito dalla condotta di chi cagiona ad altri per colpa una lesione personale grave o gravissima, con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

G.3 Aree di rischio

Tech Trade S.r.l. ha individuato, in base all'analisi dei propri processi, le seguenti aree di rischio in materia di salute e sicurezza sul lavoro, con particolare riguardo al laboratorio di rigenerazione toner:

1. Valutazione dei rischi e stesura del DVR
   - ○ Identificazione e analisi dei pericoli connessi all'uso di sostanze chimiche (inchiostri, polveri di toner), alla manipolazione dei contenitori esausti, allo smontaggio e rimontaggio di componenti, alla movimentazione manuale dei carichi, all'utilizzo di attrezzature e macchinari (compressori, apparecchi per aspirazione polveri, ecc.).
2. Organizzazione e gestione del laboratorio
   - ○ Procedure di lavoro in sicurezza per il personale addetto alla rigenerazione delle cartucce (utilizzo di DPI, contenimento delle polveri, corretta ventilazione/aspirazione, stoccaggio dei materiali, uso corretto di sostanze chimiche compatibili con le normative di sicurezza).
3. Formazione e informazione dei lavoratori
   - ○ Addestramento specifico sulle attività di rigenerazione toner (rischi da polveri fini, rischi chimici, misure di prevenzione, procedure di emergenza in caso di sversamento o contatto accidentale, utilizzo corretto dei DPI quali mascherine filtranti, guanti, occhiali protettivi, ecc.).
4. Sorveglianza sanitaria

○ Visite periodiche per i lavoratori esposti a particolari sostanze (polveri di toner, eventuali solventi), finalizzate a monitorare la funzionalità respiratoria e cutanea, oltre alla valutazione di eventuali allergie.

5. Gestione delle emergenze

○ Procedure di pronto soccorso (presenza di kit di primo soccorso in laboratorio, addetti formati, segnaletica di sicurezza), piani di evacuazione e di intervento in caso di incendio (specie se presenti sostanze infiammabili o comburenti).

6. Manutenzione dei macchinari, DPI e impianti di aspirazione

○ Svolgimento periodico e documentato di controlli e manutenzioni (verifica dell'efficienza dei sistemi di aspirazione, pulizia e sostituzione filtri, stato di conservazione dei DPI, funzionamento dei macchinari in sicurezza).

7. Gestione dei rifiuti da laboratorio

○ Corretto smaltimento di cartucce esauste, toner residui, contenitori di sostanze chimiche, nel rispetto delle procedure ambientali (D. Lgs. 152/2006) e di sicurezza, evitando accumuli pericolosi o sversamenti accidentali.

G.4 Principi di comportamento

F.4.1 Principi generali

La Società riconosce la salute e la sicurezza dei lavoratori come valori primari e imprescindibili e si impegna a garantire un ambiente di lavoro conforme alla normativa vigente, in particolare al D.Lgs. 81/2008.

Tutti i lavoratori, collaboratori, dirigenti e soggetti terzi sono tenuti a:

- rispettare scrupolosamente le disposizioni contenute nel Documento di Valutazione dei Rischi (DVR) e nei protocolli interni di sicurezza;
- utilizzare correttamente i dispositivi di protezione individuale (DPI) e mantenere in efficienza gli strumenti e le attrezzature di lavoro;
- segnalare tempestivamente al RSPP e/o al Datore di lavoro ogni condizione di pericolo, anomalia o mancato rispetto delle norme antinfortunistiche riscontrato nei luoghi di lavoro;
- partecipare obbligatoriamente alla formazione in materia di sicurezza, secondo il programma stabilito dall'azienda.

La Società adotta un sistema periodico di controllo e aggiornamento delle misure di prevenzione e protezione, e prevede audit interni a cadenza almeno annuale per la verifica dell'applicazione effettiva delle regole di sicurezza.

Eventuali infortuni, anche lievi, e situazioni di rischio devono essere immediatamente documentati e trasmessi all'Organismo di Vigilanza, che ne verifica la corretta gestione e tracciabilità.

È fatto divieto di:

● Omesso rispetto delle normative in materia di prevenzione infortuni, antincendio, igiene, sorveglianza sanitaria, formazione e addestramento dei lavoratori;

- Ostacolare o eludere i controlli e le verifiche interne o esterne;
- Compromettere la sicurezza del laboratorio (es. disattivando dispositivi di protezione collettiva, ignorando le procedure di lavoro in sicurezza, non segnalando guasti o anomalie);
- Minimizzare o nascondere le segnalazioni di rischio per evitare spese o rallentamenti nella produzione.

G.4.2 Principi di organizzazione e vigilanza

Tech Trade S.r.l. assicura un sistema organizzativo conforme al D. Lgs. 81/2008, prevedendo:

1. Individuazione del Datore di Lavoro
   - Il Datore di Lavoro è definito nell'organigramma aziendale; possiede i poteri di spesa e decisionali in ambito sicurezza.
2. Designazione del RSPP e del Medico Competente
   - Il Responsabile del Servizio di Prevenzione e Protezione deve possedere i requisiti di legge ed essere formalmente nominato, collaborando con il Datore di Lavoro per l'elaborazione del DVR e la definizione delle misure di prevenzione.
   - Il Medico Competente effettua la sorveglianza sanitaria, in particolare per i lavoratori esposti a polveri di toner o sostanze chimiche, ed emette i giudizi di idoneità specifici.
3. Valutazione dei rischi per il laboratorio di rigenerazione
   - Il DVR deve includere una sezione dedicata ai rischi chimici e aerodispersi (polveri sottili), ai rischi meccanici (uso di utensili e macchine), ai rischi ergonomici (sollevamento e trasporto di cartucce) e alle misure di prevenzione (ventilazione, aspirazione localizzata, DPI).
   - Le procedure di lavoro in sicurezza devono definire:
     - Tipologia di DPI obbligatori (mascherine FFP2/FFP3 per polveri, guanti protettivi, occhiali, tute).
     - Modalità di movimentazione e stoccaggio di cartucce e toner.
     - Modalità di pulizia e manutenzione degli strumenti (compressori, aspiratori, etc.).
4. Informazione e formazione dei lavoratori
   - I lavoratori addetti alla rigenerazione di toner devono ricevere formazione specifica su:
     - Rischi correlati alle polveri di toner e alle sostanze chimiche.
     - Uso e manutenzione dei DPI.
     - Procedure di emergenza (sversamenti, contatto accidentale con sostanze, infortuni).
   - L'azienda registra la formazione erogata (nomi dei partecipanti, data, argomenti trattati, test di verifica), conservando gli attestati.
5. Sorveglianza sanitaria e registrazione dei near-miss
   - Il Medico Competente stabilisce il protocollo sanitario per i lavoratori del laboratorio, valutando i rischi respiratori, cutanei, allergici e definendo le visite periodiche.
   - Ogni near-miss (quasi incidente) o infortunio deve essere comunicato al RSPP e al Datore di Lavoro, che redigono una relazione con le cause e le azioni correttive.
6. Verifiche periodiche e manutenzione
   - Tech Trade S.r.l. pianifica ispezioni regolari per garantire l'efficacia dei sistemi di aspirazione, la corretta gestione dei rifiuti, l'efficienza dei DPI, l'integrità delle apparecchiature (compressori, macchine di refill, bilance, ecc.).
   - Tali verifiche vengono documentate e archiviate (rapporti di manutenzione, check-list, scadenziari).

G.4.3 Obblighi di comportamento dei Destinatari

Tutti i lavoratori, dirigenti e preposti che operano nel laboratorio, e più in generale in Tech Trade S.r.l., devono:

- Rispettare in ogni momento le procedure di sicurezza previste dall'azienda (utilizzo DPI, regole di comportamento nell'uso delle macchine).
- Segnalare immediatamente al RSPP o al Datore di Lavoro qualsiasi situazione di pericolo, anomalia, guasto o non conformità riscontrata.
- Sottoporsi alle visite mediche previste dal piano di sorveglianza sanitaria e collaborare con il Medico Competente fornendo informazioni veritiere sullo stato di salute.
- Collaborare con gli organi di vigilanza (interni ed esterni) fornendo dati e documentazione richiesta.

È vietato:

- Disattivare i dispositivi di protezione o le misure di sicurezza, come aspiratori o filtri, per semplificare o velocizzare le operazioni.
- Utilizzare macchinari o strumenti senza aver ricevuto adeguato addestramento o in assenza delle protezioni prescritte.
- Ostacolare i controlli o la verifica dell'applicazione dei protocolli di sicurezza.

G.5 Flussi informativi all'Organismo di Vigilanza

1. Comunicazioni di anomalie e non conformità
   - Il Datore di Lavoro, il RSPP e tutti i soggetti aziendali che rilevino situazioni di pericolo, eventi infortunistici, near-miss o violazioni delle procedure di sicurezza, sono tenuti a darne tempestiva comunicazione scritta all'OdV.
2. Report periodici
   - Con cadenza annuale (o altra periodicità stabilita), il RSPP, in coordinamento con il Datore di Lavoro, deve trasmettere all'OdV un report contenente:
     - Statistiche degli infortuni e dei near-miss (con cause e misure correttive intraprese).
     - Eventuali visite e ispezioni da parte degli Organi di Vigilanza (es. ASL, Vigili del Fuoco) e relativi esiti/verbali.
     - Aggiornamenti del DVR, con particolare riguardo alle attività del laboratorio di rigenerazione toner.
     - Piano di formazione erogata in tema di sicurezza e registro della sorveglianza sanitaria (nel rispetto della privacy dei lavoratori).
     - Interventi di manutenzione straordinaria o acquisto di nuovi macchinari e DPI effettuati nel periodo di riferimento.
3. Segnalazione di incidenti gravi
   - In caso di infortunio grave o gravissimo, o di un incidente che coinvolga più lavoratori, con rischio concreto per la loro incolumità, l'OdV deve essere informato immediatamente e fornito di tutte le informazioni necessarie (dinamica, cause ipotizzate, misure urgenti adottate).
4. Informazioni su modifiche organizzative
   - L'apertura di nuovi reparti o l'introduzione di nuove linee di lavoro, specie se implicano utilizzo di sostanze chimiche o apparecchiature non precedentemente valutate, devono essere comunicate all'OdV, affinché possa valutarne gli impatti sui rischi già mappati.

H. INDUZIONE A NON RENDERE DICHIARAZIONI O MENDACI ALL'AUTORITÀ GIUDIZIARIA (Art. 25-decies del Decreto)

H.1 Premessa

L'art. 377-bis c.p. punisce chi, con violenza, minaccia, offerta o promessa di denaro o altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni false alla magistratura. L'ente è responsabile se la condotta è posta in essere da soggetti che agiscono nell'interesse o vantaggio della Società.

H.2 Aree di rischio

Non esistono settori specifici, ma qualsiasi procedimento penale in cui dipendenti o collaboratori siano chiamati a testimoniare rappresenta un rischio di potenziale condizionamento o di pressioni illecite.

H.3 Principi di comportamento

La Società vieta qualsiasi condotta volta a influenzare, ostacolare o condizionare persone chiamate a rendere dichiarazioni all'autorit√† giudiziaria nell'ambito di procedimenti che coinvolgano l'ente o i suoi esponenti, sia come indagati che come persone informate sui fatti.

Viene fatto espresso divieto a tutti i destinatari del Modello di:

- indurre altri soggetti (dipendenti, collaboratori, fornitori, consulenti) a non rendere dichiarazioni, o a renderle in modo non veritiero o reticente, dinanzi all'autorit√† giudiziaria;
- suggerire versioni dei fatti o fornire indicazioni atte a inquinare le prove in caso di indagini, ispezioni o procedimenti;
- minacciare, promettere vantaggi o esercitare pressioni indebite nei confronti di testimoni o coindagati.
- Qualsiasi procedura interna, ispezione o attivit√† di audit che possa essere oggetto di accertamento giudiziario deve essere tracciata e documentata in modo da assicurare la piena trasparenza e disponibilit√† verso l'autorit√† competente.
- Il personale √® tenuto a collaborare in modo leale, completo e veritiero con l'autorit√† giudiziaria in ogni fase dell'indagine o del processo, anche quando la Societ√† riveste la posizione di persona offesa.
- Eventuali tentativi di pressione, induzione o alterazione delle dichiarazioni devono essere immediatamente segnalati all'Organismo di Vigilanza, anche in forma riservata.

H.4 Flussi informativi all'Organismo di Vigilanza

- Comunicazione di citazioni a testimoniare, avvisi di garanzia e ogni iniziativa dell'Autorità Giudiziaria verso dipendenti o collaboratori della Società.
- Segnalazioni di anomalie (pressioni, minacce, "offerte" di denaro) da parte o a carico del personale.

I. REATI AMBIENTALI (Art. 25-undecies D. Lgs. 231/2001)

I.1 Premessa

Il D. Lgs. 231/2001 ha inserito, tra i reati presupposto della responsabilità amministrativa degli enti, anche i delitti ambientali (art. 25-undecies). Tali fattispecie di reato traggono origine principalmente dalle disposizioni del D. Lgs. 152/2006 (Testo Unico Ambientale) e da ulteriori norme speciali. Tech Trade S.r.l. si impegna a prevenire ogni forma di inquinamento, abuso o gestione illecita di rifiuti e di sostanze pericolose, tutelando così l'ambiente, la salute pubblica e la reputazione aziendale.

In particolare, l'attività di rigenerazione di toner e cartucce per stampanti comporta la produzione di rifiuti quali cartucce esauste, residui di toner, inchiostri, componenti plastici o metallici: la gestione di questi materiali richiede una corretta classificazione e smaltimento secondo quanto previsto dalle normative ambientali. Inoltre, occorre valutare il rischio di emissioni (polveri di toner o vapori di solventi) e di scarichi se vengono utilizzate sostanze chimiche.

I.2 Fattispecie di reato rilevanti

A titolo esemplificativo, le principali fattispecie di reato in materia ambientale che rilevano ai fini del D. Lgs. 231/2001 sono:

Scarichi illeciti di acque reflue industriali (art. 137, D.Lgs. 152/2006)
Costituito dalla condotta di chi apra o comunque effettui nuovi scarichi di acque reflue industriali, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata.

Attività di gestione di rifiuti non autorizzata (art. 256, commi 1, 3, 5, 6, primo periodo, D.Lgs. 3 aprile 2006, n. 152)
Tale ipotesi di reato si configura nei seguenti casi:
- attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti – sia pericolosi che non pericolosi – in mancanza della prescritta autorizzazione, iscrizione o comunicazione (art. 256, comma 1);
realizzazione o gestione di una discarica non autorizzata, anche eventualmente destinata allo smaltimento di rifiuti pericolosi (art. 256, comma 3);
effettuazione di attività non consentite di miscelazione di rifiuti (art. 256, comma 5);
deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi con violazione delle disposizioni di cui all'articolo 227, comma 1, lett. b) (art. 256, comma 6, primo periodo).

Bonifica dei siti (art. 257, commi 1 e 2, d.lgs. 3 aprile 2006, n. 152)
Tale ipotesi di reato si configura nel caso in cui si cagioni l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle

concentrazioni soglia di rischio e il responsabile dell'inquinamento non provveda alla comunicazione alle autorità competenti entro i termini previsti ovvero alla bonifica del sito secondo il progetto approvato dall'autorità competente.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulatori (art. 258, comma 4, secondo periodo, D.Lgs. 3 aprile 2006 n. 152)
Tale ipotesi di reato si configura nei casi in cui nella predisposizione di un certificato di analisi di rifiuti si forniscano false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, ovvero si faccia uso di un certificato falso durante il trasporto.

Traffico illecito di rifiuti (art. 259, comma 1 D.Lgs. 3 aprile 2006 n. 152)
Tale ipotesi di reato si configura nel caso in cui venga effettuata una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259, ovvero tale spedizione tratti i rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), e) e d) del regolamento stesso.

Attività organizzate per il traffico illecito di rifiuti (art. 260 D.Lgs. 3 aprile 2006, n. 152)
Tale ipotesi di reato si configura nel caso in cui, al fine di conseguire un ingiusto profitto, vengano effettuate, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, la cessione, il ricevimento, il trasporto, l'esportazione o l'importazione o, comunque, la gestione abusiva di ingenti quantitativi di rifiuti (anche ad alta radioattività).

Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, commi 6, 7, secondo e terzo periodo e 8, D.Lgs. 3 aprile 2006 n. 152)
Tale ipotesi di reato si configura nel caso in cui:
- nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, siano fornite false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, nonché si inserisca un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti;
il trasportatore ometta di accompagnare il trasporto dei rifiuti (pericolosi o non pericolosi) con la copia cartacea della scheda SISTRI - AREA MOVIMENTAZIONE e, ove necessario sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti;
durante il trasporto si faccia uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati;
il trasportatore accompagni il trasporto di rifiuti (pericolosi o non pericolosi) con una copia cartacea della scheda SISTRI – AREA Movimentazione fraudolentemente alterata.

Sanzioni (art. 279 comma 5, D.Lgs. 3 aprile 2006 n. 152)

Tale ipotesi di reato si configura nel caso in cui le emissioni in atmosfera prodotte dalla Società superando i valori limite di emissione, determinino altresì il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

Cessazione e riduzione dell'impiego di sostanze lesive (art. 3, comma 6, L. 28 dicembre 1993, n. 549)
Tale ipotesi di reato si configura nel caso in cui si effettuino attività di: produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive dello strato atmosferico di ozono.

Inquinamento ambientale (art. 452 bis c.p.)
Costituito dalla condotta di chi abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:
delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;
di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Disastro ambientale (art. 452 quater c.p.)
Costituito dalla condotta di chi abusivamente cagiona un disastro ambientale.
Costituisce disastro ambientale:

1. l'alterazione irreversibile dell'equilibrio di un ecosistema;
2. l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;
3. l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o per il numero delle persone offese o esposte a pericolo.

Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)
Se i fatti di cui agli articoli 452-bis e 452-quater sono commessi per colpa, le pene ivi previste sono diminuite da un terzo a due terzi.

I.3 Aree di rischio

Alla luce della specifica attività di Tech Trade S.r.l., si individuano le seguenti aree di rischio in tema ambientale:

1. Laboratorio di rigenerazione toner e cartucce
   - ○ Produzione di rifiuti speciali (cartucce esauste, residui di polveri di toner, parti in plastica/ferro, eventuali solventi).
   - ○ Presenza di aspiratori e filtri per la raccolta di polveri, con potenziali emissioni in atmosfera se la manutenzione non è adeguata.
2. Stoccaggio temporaneo dei rifiuti

○ Modalità di identificazione dei rifiuti (codici CER), conservazione in contenitori etichettati, gestione dei registri di carico/scarico, formulari di identificazione, controllo delle scadenze e dei volumi accumulati.

3. Eventuali scarichi idrici

○ Qualora il laboratorio utilizzi acqua per il lavaggio di componenti o per la diluizione di inchiostri, si deve verificare la conformità degli scarichi alla normativa (limiti tabellari, eventuale autorizzazione allo scarico).

4. Emissioni in atmosfera

○ L'uso di macchine per la pulizia o l'asciugatura delle cartucce, o di sostanze chimiche, può generare fumi, vapori o polveri. Occorre valutare se è necessaria un'autorizzazione alle emissioni e rispettare i valori soglia.

5. Emergenze ambientali

○ Rischio di sversamenti o dispersione di toner o inchiostri, incendi, malfunzionamenti negli impianti di aspirazione, con potenziali danni al suolo, all'aria e alla salute dei lavoratori e della comunità.

I.4 Principi di comportamento

La Società riconosce la tutela dell'ambiente come valore fondamentale e si impegna a svolgere la propria attività nel rispetto della normativa ambientale vigente, delle autorizzazioni amministrative rilasciate e dei principi di prevenzione e precauzione.

È fatto divieto assoluto di porre in essere condotte che possano provocare danno, deterioramento o pericolo concreto per l'ambiente, l'ecosistema, le risorse naturali o la salute della collettività.

Tutti i destinatari del Modello sono tenuti a:

- rispettare le disposizioni contenute nelle autorizzazioni ambientali (AUA, AIA, scarichi, emissioni, gestione rifiuti);
- gestire i rifiuti prodotti secondo le normative vigenti, assicurando la tracciabilità completa dei flussi, lo smaltimento attraverso soggetti autorizzati e la corretta tenuta dei registri;
- monitorare periodicamente le emissioni e gli scarichi prodotti, in conformità alle soglie e prescrizioni fissate;
- comunicare tempestivamente eventuali anomalie o superamenti dei limiti ai referenti aziendali e all'Organismo di Vigilanza;
- verificare che tutti i fornitori, subappaltatori e gestori ambientali esterni siano in possesso di titoli autorizzativi validi.

La Società adotta inoltre un sistema di controlli interni e, ove previsto, di audit ambientale, volto a prevenire situazioni di rischio e a garantire la tracciabilità dei comportamenti e delle decisioni a rilevanza ambientale.

Qualsiasi comportamento non conforme o potenzialmente lesivo dell'ambiente deve essere oggetto di segnalazione immediata all'OdV e comporta l'attivazione di apposite misure correttive e, se del caso, sanzionatorie.

I.4.1 Divieti generali

È fatto divieto di:

- Porre in essere o concorrere a porre in essere condotte che concretizzino i reati ambientali di cui all'art. 25-undecies D. Lgs. 231/2001.
- Gestire i rifiuti in modo non conforme alla legge (D. Lgs. 152/2006), ad esempio omettendo l'iscrizione all'Albo Gestori Ambientali per il trasporto, o affidandosi a soggetti non autorizzati.
- Scaricare sostanze chimiche o reflui di lavorazione del laboratorio in rete fognaria, su suolo o corsi d'acqua senza le necessarie autorizzazioni o in violazione dei limiti imposti.
- Disattendere gli obblighi di bonifica o di comunicazione in caso di incidenti ambientali che superino le soglie di contaminazione previste.
- Nascondere o minimizzare eventi di contaminazione, emissioni anomale o sversamenti, eludendo le procedure di segnalazione interna e le prescrizioni di legge.

I.4.2 Principi specifici per Tech Trade S.r.l.

1. Gestione rifiuti derivanti dalla rigenerazione
   - Classificare correttamente i rifiuti (es. residui di toner come rifiuti speciali potenzialmente pericolosi, cartucce esauste, contenitori contaminati da inchiostri).
   - Stoccarli in un'area apposita, su pavimentazione impermeabile, in contenitori etichettati, evitando commistioni tra rifiuti pericolosi e non.
   - Aggiornare i registri di carico/scarico e compilare i formulari di identificazione in fase di consegna a trasportatori autorizzati, conservando la documentazione per i periodi di legge.
   - Verificare la regolarità del soggetto che effettua trasporto e smaltimento/recupero (iscrizione all'Albo Gestori Ambientali, presenza di autorizzazioni in corso di validità).
2. Emissioni in atmosfera
   - Se il processo di rigenerazione comporta emissioni di polveri, vapori o sostanze chimiche, Tech Trade S.r.l. deve:
     - Dotarsi di impianti di aspirazione e filtraggio adeguati (filtri a carboni attivi, filtri a manica, ecc.), gestendo la manutenzione periodica e la sostituzione dei filtri entro le scadenze previste.
     - Accertarsi se è necessaria un'Autorizzazione alle Emissioni in Atmosfera (ai sensi del D. Lgs. 152/2006) e, in tal caso, rispettarne le condizioni (limiti, autocontrolli, registrazioni).
     - Monitorare eventuali segnalazioni di odori o dispersioni anomale di polveri.
3. Scarichi idrici
   - Nel caso vi siano lavaggi di cartucce o utilizzo di sostanze detergenti, occorre verificare la natura degli scarichi (assimilabili a domestici o classificati come industriali), l'eventuale presenza di sostanze inquinanti e la conformità ai limiti tabellari.
   - Vietato lo scarico di inchiostri, toner liquidi o residui solventi se non espressamente autorizzato.
4. Procedure di emergenza ambientale
   - In caso di sversamenti, incendi, malfunzionamenti di aspiratori o filtri, Tech Trade S.r.l. deve disporre di un piano di intervento: isolamento dell'area, contenimento del materiale versato, utilizzo di assorbenti e contenitori idonei, comunicazione immediata al Responsabile Ambientale/ RSPP.

○ Nei casi più gravi, le Autorità competenti (ARPA, Vigili del Fuoco) vanno allertate per valutare il danno ambientale e adottare misure straordinarie.

5. Formazione e informazione dei lavoratori

○ L'azienda assicura che i dipendenti operanti nel laboratorio siano formati sulle procedure ambientali, sui DPI necessari e sulle norme per la corretta gestione dei rifiuti e delle sostanze chimiche.

○ La formazione avviene in occasione dell'assunzione o di cambiamenti organizzativi, con aggiornamenti periodici.

I.5 Flussi informativi all'Organismo di Vigilanza

1. Segnalazioni immediate

○ Tutti i Destinatari che ravvisino violazioni potenziali o effettive della normativa ambientale (p.es. gestione impropria dei rifiuti, emissioni fuori controllo, incidenti, sversamenti, accumuli di materiali sospetti) devono avvisare subito l'OdV in forma scritta (email o canale dedicato), indicando data, luogo e descrizione dei fatti.

2. Report periodici

○ Con cadenza annuale o infrannuale, il Responsabile Ambientale (o la funzione equivalente) trasmette all'OdV un report che includa:

■ Dati sui rifiuti prodotti (quantità, codici CER, impianti di destino) e sulle eventuali misure di riduzione degli scarti.

■ Risultati di controlli su emissioni (manutenzione, sostituzioni filtri, eventuali analisi eseguite) e su scarichi idrici (autocontrolli, rispetto dei parametri).

■ Esito di ispezioni o verifiche da parte di enti esterni (ARPA, NOE, Polizia Provinciale) e, se presenti, i relativi verbali e prescrizioni.

■ Eventuali incidenti o "quasi-incidenti" ambientali, con indicazione delle cause e delle azioni correttive.

■ Elenco delle attività formative in materia ambientale, con dettaglio dei partecipanti, date e argomenti.

3. Comunicazione di nuovi progetti o modifiche organizzative

○ Laddove Tech Trade S.r.l. intenda ampliare il laboratorio o introdurre nuovi macchinari o sostanze potenzialmente impattanti, l'OdV deve esserne informato per verificare la necessità di aggiornare il Documento di Valutazione dei Rischi e/o richiedere nuove autorizzazioni ambientali.

4. Incidenti rilevanti

○ In caso di incidente ambientale rilevante (sversamento di toner o solventi su larga scala, incendio che provochi emissioni pericolose, danni strutturali con rischio di contaminazione), è obbligatorio avvisare immediatamente l'OdV, fornendo tutti i dati necessari per valutare l'accaduto e le misure di contenimento.

J. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (Art. 25-duodecies D. Lgs. 231/2001)

J.1 Premessa

Il D. Lgs. 231/2001, integrato dal D. Lgs. 109/2012, punisce il datore di lavoro che impieghi alle proprie dipendenze cittadini extra-UE privi di regolare permesso di soggiorno, con sanzioni pecuniarie elevate quando i lavoratori irregolari siano più di tre, minori o esposti a grave sfruttamento.

J.2 Aree di rischio

1. Selezione e assunzione del personale straniero, soprattutto in settori a bassa qualificazione.
2. Rapporti con agenzie interinali o cooperative.

J.3 Principi di comportamento

La Società si impegna a garantire il rispetto delle norme sull'immigrazione e a impedire l'impiego di lavoratori stranieri privi di regolare permesso di soggiorno o in condizione di soggiorno irregolare sul territorio dello Stato.

È fatto divieto assoluto di instaurare rapporti di lavoro, anche autonomo o occasionale, con cittadini di Paesi terzi che non siano in possesso di permesso di soggiorno valido per l'attività lavorativa esercitata.

La funzione Risorse Umane, in coordinamento con l'Amministrazione e il Datore di Lavoro, è tenuta a:

- verificare preventivamente la documentazione identificativa e di soggiorno di tutti i lavoratori stranieri prima dell'instaurazione del rapporto contrattuale;
- conservare in archivio copia della documentazione acquisita per almeno cinque anni;
- monitorare la scadenza dei titoli di soggiorno e verificare il loro rinnovo in tempo utile;
- revocare ogni collaborazione o incarico in caso di accertata irregolarità della posizione del lavoratore.

La Società si impegna a operare esclusivamente con fornitori e appaltatori che rispettino le disposizioni in materia di lavoro regolare, richiedendo dichiarazioni di conformità normativa e riservandosi di effettuare verifiche a campione.

Ogni violazione o anomalia riscontrata deve essere immediatamente segnalata all'Organismo di Vigilanza, affinché siano attivate le verifiche e misure previste dal Modello.

J.4 Flussi informativi all'Organismo di Vigilanza

- Comunicazione periodica di tutte le nuove assunzioni, specificando se il personale è cittadino di Paese terzo.
- Segnalazioni immediate se emergono irregolarità nella documentazione (permesso scaduto, revocato, ecc.) per valutare azioni di adeguamento.

Conclusioni

La presente Parte Speciale, suddivisa per ciascuna categoria di reati rilevanti ai sensi del D. Lgs. 231/2001, integra la Parte Generale del Modello e il Codice Etico di Tech Trade S.r.l., illustrando:

- Principi di comportamento (obblighi e divieti) per prevenire la commissione dei reati.
- Aree di rischio individuate in base ai processi operativi dell'azienda.
- Flussi informativi all'OdV, indispensabili per consentire un monitoraggio continuo delle aree sensibili e intervenire tempestivamente in caso di anomalie o violazioni.

I Destinatari (dipendenti, dirigenti, collaboratori, fornitori e partner) devono rispettare tali disposizioni e agire in coerenza con i protocolli aziendali che ne disciplinano l'applicazione pratica (procedure organizzative, deleghe di potere, procedure di controllo, protocolli di sicurezza, ecc.).

Il mancato rispetto di questi principi comporta l'applicazione di sanzioni disciplinari, secondo quanto previsto nella Parte Generale del Modello 231 e nei contratti di lavoro e collaborazione in vigore, nonché la possibile compromissione del rapporto di lavoro o fornitura.

Soltanto un corretto e costante rispetto di queste Parti Speciali, unito alla collaborazione con l'Organismo di Vigilanza (OdV) e alla formazione di tutto il personale sui rischi e i comportamenti vietati, consente a Tech Trade S.r.l. di prevenire efficacemente la commissione dei reati contemplati dal D. Lgs. 231/2001 e di preservare la reputazione e la solidità dell'azienda.