

CAPITOLO III
IL MODELLO DI CHEMI S.P.A.
PARTE SPECIALE

1. Premessa

In conformità all'art. 6 del DECRETO, il sistema dei controlli interni deve prevedere, in relazione ai reati da prevenire:

- i)* specifici protocolli per programmare la formazione e l'attuazione delle decisioni della SOCIETÀ;
- ii)* l'individuazione di modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

La SOCIETÀ è dotata di un sistema procedurale che compone il sistema di prevenzione e controllo. Le procedure sono costantemente aggiornate, anche su proposta o segnalazione dell'ORGANISMO.

L'ORGANISMO verifica che le procedure siano idonee al rispetto dei principi contenuti nel MODELLO, propone le eventuali modifiche e concorre a definire, con le funzioni aziendali interessate, le operazioni di carattere *significativo* alle quali si applicano le procedure.

Sono indici di *significatività* dell'operazione: il suo valore e portata economica rispetto all'attività della SOCIETÀ nel comparto interessato, la sua incidenza sui processi decisionali e produttivi, la sua rilevanza rispetto alla ordinaria attività di impresa.

Sono ammesse, nei casi di particolare urgenza o in caso di impossibilità temporanea di rispetto delle procedure, sotto la responsabilità di chi le attua, eventuali deroghe a quanto previsto nella presente *Parte speciale*, nella formazione o nell'attuazione delle decisioni. In tale evenienza è inviata immediata informazione all'ORGANISMO e, in ogni caso, è richiesta la successiva ratifica da parte del soggetto competente.

2. Identificazione delle aree e delle operazioni a rischio

Nell'ambito delle attività e della complessiva operatività aziendale della SOCIETÀ, sono individuate, per tipologia di reato, le seguenti attività *sensibili*, per ciascuna delle quali

risultano essere dettagliate le singole occasioni di realizzazione del reato, le funzioni coinvolte, le fattispecie di reato (Mappatura – Allegato 2).

2.1. Reati contro la Pubblica Amministrazione (artt. 24 e 25 del DECRETO)

Fatte salve le definizioni di soggetto “attivo” ai fini delle fattispecie di reato contemplate dal D. Lgs. 231/2001 e delle conseguenti prescrizioni del *Modello di Organizzazione Gestione e Controllo della Società*, qualificate:

- dall’art. 357 del Codice penale in riferimento al pubblico ufficiale, inteso come colui il quale “esercita una pubblica funzione legislativa, giudiziaria o amministrativa”⁹;
- dall’art. 358 del Codice penale in riferimento all’incaricato di pubblico servizio, inteso come colui il quale “a qualunque titolo, presta un pubblico servizio”¹⁰;

l’accezione con cui intendere la Pubblica Amministrazione e la conseguente configurazione dei soggetti attivi in essa operanti deve intendersi, ai presenti fini, come estensiva.

Dottrina e giurisprudenza hanno, infatti, affrontato il tema della qualificazione degli “Enti pubblici” e dei soggetti in essi operanti in tutti i casi in cui la natura “pubblica” dell’Ente non sia configurata direttamente dalla legge, derivando da tali analisi definizioni allargate rispetto a quella di “Ente pubblico in senso stretto”¹¹.

⁹ Dallo stesso articolo la “funzione pubblica amministrativa” è definita come “disciplinata da norme di diritto pubblico e da atti autorizzativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autorizzativi o certificativi”;

¹⁰ Per “pubblico servizio” deve intendersi “*un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*”;

¹¹ L’Ente Pubblico è definito, tra l’altro, dall’art. 1 comma 2 del D. Lgs. 165/2000 laddove si precisa che “per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende

Tali definizioni vertono sulla valutazione di una serie di elementi, da realizzare “in concreto” e non solo “in astratto”, rispetto alla natura, alle attività e alle funzioni attribuite alle diverse tipologie di soggetti con cui la SOCIETÀ si trova ad interloquire.

Tra tali elementi, che devono costituire oggetto di analisi da parte di tutti i destinatari dei presenti protocolli e che, nel dubbio, devono essere interpretati secondo un principio estensivo di prudenza, si menziona a titolo esemplificativo e non esaustivo:

- il fatto che l’attività dell’Ente sia finanziata in modo maggioritario dallo Stato, dalle Regioni, dagli Enti Locali, da altri enti pubblici o da organismi di diritto pubblico o che la gestione dello stesso sia sottoposta al loro controllo ovvero condotta con organismi di amministrazione, direzione o vigilanza costituiti in misura non inferiore alla metà da componenti designati dai medesimi soggetti;
- il fatto che l’Ente derivi dalla trasformazione di “ente pubblico economico” (ad es. IRI, INA, ENI, ENEL) fino a quando sussista una partecipazione esclusiva o maggioritaria dello Stato al capitale azionario;
- il fatto che l’Ente sia sottoposto ad un regime di controllo pubblico, di carattere funzionale o strutturale, da parte dello Stato o di altra Pubblica Amministrazione;
- il fatto che l’Ente possa o debba compiere atti in deroga al diritto comune ovvero che possa godere di c.d. “istituti di privilegio” ovvero che sia titolare di poteri amministrativi in senso tecnico (ad esempio in virtù di concessioni, diritti speciali o esclusivi concessi loro dall’autorità secondo le norme vigenti)¹²;
- il fatto che l’Ente ed i soggetti attivi in esso operanti, svolgano attività ricollegabili a interessi pubblici e, in particolare, siano incaricati di servizi pubblici essenziali quali, a titolo esemplificativo e non esaustivo:
 - la sanità;
 - l’igiene pubblica;

e gli enti del Servizio sanitario nazionale, l’Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300”.

¹² In tal senso un indicatore significativo può, tra l’altro, essere la sottoposizione dell’Ente alla normativa in materia di Appalti Pubblici.

- la protezione civile;
- la raccolta e lo smaltimento dei rifiuti;
- le dogane;
- l'approvvigionamento di energie, risorse naturali e beni di prima necessità nonché la gestione e la manutenzione dei relativi impianti;
- i trasporti pubblici urbani ed extraurbani, autoferrotranviari, ferroviari aerei, aeroportuali e marittimi;
- i servizi di supporto ed erogazione in merito all'assistenza e la previdenza sociale;
- l'istruzione pubblica;
- le poste, le telecomunicazioni e l'informazione radiotelevisiva pubblica.

A titolo esemplificativo, rivestono la qualifica di Pubblico Ufficiale e/o di Incaricato di Pubblico Servizio: dipendenti comunali non esercenti attività meramente materiale, componenti della Commissione Gare d'Appalto indette dalla P.A., Militari della Guardia di Finanza o NAS, Militari dei Carabinieri, Vigili Urbani, componenti dell'ufficio tecnico del Comune, curatore (in qualità di organo del fallimento), operatore amministrativo addetto al rilascio di certificati presso la cancelleria di un Tribunale, medico dipendente del Servizio Sanitario Nazionale, ispettore ASL, ecc.

Inoltre, ai sensi di quanto stabilito dalla Direttiva (UE) 2017/1371 (c.d. "Direttiva PIF"), in riferimento alla tutela degli interessi finanziari dell'Unione Europea (ovvero delle spese e dei beni ai danni del bilancio generale dell'Unione europea), è necessario includere nella definizione di "funzionario pubblico" tutti coloro che ricoprono un incarico formale nell'Unione, negli Stati membri o nei paesi terzi ovvero persone che, pur non ricoprendo un incarico formale, sono tuttavia investite di funzioni di pubblico servizio e le esercitano in maniera analoga, relativamente a fondi o beni dell'Unione, quali contraenti coinvolti (in quanto incaricati direttamente o indirettamente) nella gestione di tali fondi o beni. Nello specifico, s'intende per "funzionario pubblico":

- a) un funzionario dell'Unione o un funzionario nazionale, compresi i funzionari nazionali di un altro Stato membro e i funzionari nazionali di un paese terzo;
 - i) per "funzionario dell'Unione" s'intende una persona che rivesta la qualifica

di funzionario o di altro agente assunto per contratto dall'Unione o distaccata da uno Stato membro o da qualsiasi organismo pubblico o privato presso l'Unione, che vi eserciti funzioni corrispondenti a quelle esercitate dai funzionari o dagli altri agenti dell'Unione;

- ii) per “funzionario nazionale” s'intende il “funzionario” o il “funzionario pubblico” secondo quanto definito nel diritto nazionale dello Stato membro o del paese terzo in cui la persona in questione svolge le sue funzioni. Il termine “funzionario nazionale” comprende qualsiasi persona che eserciti una funzione esecutiva, amministrativa o giurisdizionale a livello nazionale, regionale o locale. È assimilata a un funzionario nazionale qualsiasi persona che eserciti una funzione legislativa a livello nazionale, regionale o locale;
- b) qualunque altra persona a cui siano state assegnate o che eserciti funzioni di pubblico servizio che implicino la gestione degli interessi finanziari dell'Unione, o decisioni che li riguardano, negli Stati Membri o in paesi terzi.

Pertanto, relativamente ai reati di corruzione e di appropriazione indebita, contemplati dagli artt. 24 e 25 del D. Lgs. 231/2001, considereremo la definizione di “Pubblica Amministrazione” comprensiva di tutte le specifiche sopra riportate.

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Gestione dei rapporti, degli adempimenti e delle comunicazioni con Enti regolatori (ad es. AIFA, FDA, ecc.) e con le autorità di P.S. (ad es. NAS) relativamente al processo produttivo e alle *Good Manufacturing Practices*, anche in occasione di visite o ispezioni;
- Utilizzo di sostanze e di prodotti sottoposti a regolamentazione specifica (ad esempio precursori di armi chimiche, di stupefacenti, prodotti sottoposti a licenze UTF, sostanze oggetto del regolamento REACH, ecc.), anche in occasione di visite o ispezioni;

- Gestione dei rapporti con Enti pubblici locali per gli aspetti che riguardano la normativa urbanistica ed edilizia (autorizzazioni, concessioni, permessi, ecc.);
- Gestione degli adempimenti fiscali e dei rapporti con l'Amministrazione finanziaria e gli organi di polizia tributaria in occasione di ispezioni e accertamenti;
- Gestione delle attività di presentazione dell'azienda al pubblico, anche in occasione di incontri istituzionali;
- Acquisto di beni e servizi afferenti alla produzione (acquisti diretti);
- Consulenze, altri acquisti indiretti e appalti;
- Attività relative alla gestione delle risorse umane;
- Gestione dei rimborsi spese a dipendenti e delle spese di rappresentanza;
- Gestione di omaggi, donazioni, sponsorizzazioni, contributi e liberalità;
- Gestione rapporti con agenti e distributori;
- Percezione e gestione di contributi/finanziamenti agevolati erogati da Enti pubblici e comunitari;
- Gestione contenziosi giudiziali e stragiudiziali (civili, penali, amministrativi, tributari, giuslavoristici);
- Gestione dei rapporti con le Autorità amministrative indipendenti (ad es. Autorità Garante per la Privacy, AGCM);
- Gestione degli adempimenti relativi a salute e sicurezza sul luogo di lavoro e dei rapporti con Enti pubblici per il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni;
- Gestione di attività e processi rilevanti ai fini ambientali anche in rapporto con terze parti;
- Ricerca e sviluppo, processo produttivo e distributivo.

2.2. Reati informatici (art. 24-bis del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Utilizzo di risorse e informazioni di natura informatica o telematica ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore.

2.3. Reati di falsità in monete (art. 25-bis del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Gestione delle attività di presentazione dell'azienda al pubblico, anche in occasione di incontri istituzionali;
- Ricerca e sviluppo, processo produttivo e distributivo;
- Acquisto di beni e servizi afferenti alla produzione (acquisti diretti);
- Consulenze, altri acquisti indiretti e appalti.

2.4. Reati contro l'industria e il commercio (art. 25-bis.1 del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Gestione delle attività di presentazione dell'azienda al pubblico, anche in occasione di incontri istituzionali;
- Ricerca e sviluppo, processo produttivo e distributivo.

2.5. Reati societari (art. 25-ter del DECRETO)

Il presente paragrafo tratta i reati contemplati dall'art. 25-ter del D. Lgs. 231/2001 (Reati societari).

In considerazione dell'introduzione nel novero di tali reati degli artt. 2635, 2635 bis e 2635 ter relativi alla c.d. "corruzione tra privati" nonché dell'art. 2635 bis c.c. relativo all'"istigazione alla corruzione tra privati", e degli aspetti di peculiarità di tali delitti nell'ambito della categoria dei reati societari presupposto ex D. Lgs. 231/01, il presente paragrafo è distinto in due sezioni, la prima dedicata specificamente alla "corruzione tra privati" e alla "istigazione alla corruzione tra privati" e la seconda agli altri reati societari.

2.5.1. Corruzione e istigazione alla corruzione tra privati

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Gestione delle attività di presentazione dell'azienda al pubblico, anche in occasione di incontri istituzionali;
- Gestione delle attività inerenti alla vendita di prodotti e i rapporti con i clienti;
- Acquisto di beni e servizi afferenti alla produzione (acquisti diretti);
- Consulenze, altri acquisti indiretti e appalti;
- Attività relative alla gestione delle risorse umane;
- Gestione dei rimborsi spese a dipendenti e delle spese di rappresentanza;
- Gestione di omaggi, donazioni, sponsorizzazioni, contributi e liberalità;
- Gestione rapporti con agenti e distributori.

2.5.2. Altri reati societari

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Redazione del bilancio di esercizio;
- Gestione degli adempimenti e delle operazioni in materia societaria;
- Gestione dei rapporti con le Autorità amministrative indipendenti (ad es. Autorità Garante per la Privacy, AGCM).

2.6. Reati di terrorismo e di eversione dell'ordine democratico (art. 25-*quater* del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, la principale attività "sensibile" a rischio di commissione dei reati in oggetto è la seguente:

- Utilizzo di sostanze e di prodotti sottoposti a regolamentazione specifica (ad esempio precursori di armi chimiche, di stupefacenti, prodotti sottoposti a licenze UTF, sostanze oggetto del regolamento REACH, ecc.), anche in occasione di visite o ispezioni.

2.7. Reati di favoreggiamento dell'immigrazione clandestina e di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (25-*duodecies* del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, la principale attività "sensibile" a rischio di commissione dei reati in oggetto è la seguente:

- Attività relative alla gestione delle risorse umane.

2.8. Reati di criminalità organizzata, anche transnazionale, e di riciclaggio (art. 24-ter, art. 25-octies del DECRETO e Legge 16 marzo 2006, n. 146)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Gestione dei rapporti con interlocutori terzi – pubblici o privati – nello svolgimento delle proprie attività lavorative per conto e/o nell’interesse della Società;
- Acquisto di beni e servizi afferenti alla produzione (acquisti diretti);
- Consulenze, altri acquisti indiretti e appalti;
- Gestione degli adempimenti e delle operazioni in materia societaria;
- Rapporti con clienti/fornitori/partner per la gestione di accordi negoziali e relative operazioni amministrative, contabili e di tesoreria;
- Gestione dei flussi finanziari.

In riferimento alla fattispecie di autoriciclaggio, occorre tenere in considerazione che, oltre alle attività sopra elencate, l’autoriciclaggio potrebbe trovare realizzazione anche in conseguenza di altre fattispecie presupposto ai sensi del D. Lgs. 231/01 di natura non-colposa collegate alle diverse attività sensibili mappate (solo a titolo di esempio si pensi alla corruzione, alla truffa ai danni dello stato, alla frode in commercio ai reati contro la proprietà intellettuale e industriale, ai delitti informatici, ecc. i cui proventi potrebbero essere oggetto di “autoriciclaggio” nel caso di condotte mirate ad ostacolare concretamente l’identificazione della provenienza delittuosa).

Per semplicità di rappresentazione e per non appesantire la mappatura delle attività sensibili e dei processi strumentali, essendo tale profilo di rischio potenzialmente “trasversale” a tutte le fattispecie presupposto ai sensi del D. Lgs. 231/01 di natura non-colposa mappate, lo stesso non è stato abbinato ad ogni attività a rischio identificata.

2.9. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, la principale attività "sensibile" a rischio di commissione dei reati in oggetto è la seguente:

- Gestione degli adempimenti relativi a salute e sicurezza sul luogo di lavoro e dei rapporti con Enti pubblici per il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni.

2.10. Reati in materia di violazione di diritto d'autore (art. 25-novies del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- Gestione delle attività di presentazione dell'azienda al pubblico, anche in occasione di incontri istituzionali;
- Utilizzo di risorse e informazioni di natura informatica o telematica ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore.

2.11. Reati ambientali (art. 25-undecies del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, la principale attività "sensibile" a rischio di commissione dei reati in oggetto è la seguente:

- Gestione di attività e processi rilevanti ai fini ambientali anche in rapporto con terze parti.

2.12. Reati tributari (art. 25-*quinquiesdecies* del DECRETO)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" a rischio di commissione dei reati in oggetto sono le seguenti:

- Gestione degli adempimenti fiscali e dei rapporti con l'Amministrazione finanziaria e gli organi di polizia tributaria in occasione di ispezioni e accertamenti;
- Gestione delle attività inerenti alla vendita di prodotti e i rapporti con i clienti;
- Acquisto di beni e servizi afferenti alla produzione (acquisti diretti);
- Consulenze, altri acquisti indiretti e appalti;
- Gestione dei rimborsi spese a dipendenti e delle spese di rappresentanza;
- Gestione di omaggi, donazioni, sponsorizzazioni, contributi e liberalità;
- Gestione rapporti con agenti e distributori;
- Redazione del bilancio di esercizio;
- Gestione degli adempimenti e delle operazioni in materia societaria;
- Gestione contenziosi giudiziari e stragiudiziali (civili, penali, amministrativi, tributari, giuslavoristici).

2.13. Reati di contrabbando (art. 25-*sexiesdecies*)

In considerazione delle peculiarità del business aziendale svolto da CHEMI S.P.A. e della struttura interna adottata, le principali attività "sensibili" a rischio di commissione dei reati in oggetto sono le seguenti:

- Ricerca e sviluppo, processo produttivo e distributivo;
- Acquisto di beni e servizi afferenti alla produzione (acquisti diretti).

3. Principi generali

I seguenti principi generali informano le procedure che devono essere inderogabilmente osservate dagli organi sociali di CHEMI S.P.A., dai dirigenti e dai dipendenti, nonché, in forza di apposite clausole contrattuali, dai Collaboratori, Agenti, Consulenti e altre controparti.

In linea generale, il sistema di organizzazione della SOCIETÀ deve essere ispirato al rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale. Deve essere fondato sui requisiti fondamentali di chiara, formale e conoscibile descrizione ed individuazione dei compiti e dei poteri attribuiti a ciascuna funzione, alle diverse qualifiche e ruoli professionali; sulla precisa descrizione delle linee di riporto; sulla tracciabilità di ciascun passaggio decisionale e operativo rilevante.

In particolare:

- le responsabilità della gestione (e le relative modalità operative) di una operazione o di un processo aziendale devono essere chiaramente definite e conosciute all'interno della SOCIETÀ;
- deve esservi una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando la SOCIETÀ e manifestando la sua volontà;
- i poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- all'interno di ogni processo aziendale rilevante, devono essere separate le funzioni e individuati soggetti diversi competenti per la decisione, l'attuazione, la registrazione o il controllo di una operazione.

In sostanza, deve essere garantita la separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto; altrettanto, va perseguita una chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio ed in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa.

Inoltre:

- i documenti rilevanti devono essere adeguatamente formalizzati e riportare la data di compilazione, di presa visione del documento e la firma riconoscibile del compilatore/supervisore; gli stessi devono essere archiviati in luoghi idonei alla loro conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti. Lo stesso vale per i documenti su supporto elettronico;
- le operazioni sensibili e/o rilevanti devono essere documentate, in modo coerente e congruo, così che in ogni momento sia possibile identificare le responsabilità di coloro che hanno operato, valutato, deciso, autorizzato, effettuato, registrato, controllato l'operazione;
- i controlli effettivamente svolti devono essere precisamente documentati in modo che sia possibile identificare chi li ha eseguiti, quando sono stati svolti e con quale esito;
- devono essere previsti meccanismi di sicurezza che garantiscano una adeguata protezione/accesso fisico-logistico ai dati e ai beni aziendali.

Più specificamente, al fine di prevenire la commissione dei reati nell'ambito delle aree, attività e operazioni a rischio sopra identificata, la SOCIETÀ elabora e adotta procedure che devono in ogni caso rispettare i seguenti principi generali:

3.1. Decisioni dei soggetti apicali e conflitti di interessi

la formazione e l'attuazione delle decisioni degli amministratori sono disciplinate dai principi e dalle prescrizioni contenute nelle disposizioni di legge vigenti, nell'atto costitutivo, nello Statuto, nel CODICE ETICO, nel MODELLO, nel sistema di controllo Interno;

gli amministratori hanno l'obbligo di comunicare tempestivamente al C.d.A., al Collegio Sindacale e all'ORGANISMO, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative alle cariche assunte o alle partecipazioni di cui sono titolari, direttamente o indirettamente, in altre società o imprese, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia,

possono lasciare ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.;

vi è il medesimo obbligo di comunicazione di cui al punto precedente a carico dei Dirigenti che si trovino in posizione apicale, i quali dovranno informare l'Amministratore Delegato e l'ORGANISMO;

vi è il medesimo obbligo di comunicazione per gli esponenti di CHEMI S.P.A. nominati negli organi sociali di partecipate estere con riferimento all'esistenza di vincoli di parentela o affinità con esponenti della P.A. locale e/o fornitori, clienti o terzi contraenti della SOCIETÀ medesima;

gli esponenti della SOCIETÀ - Amministratori, Direttori Generali e Dirigenti - hanno altresì l'obbligo di astenersi dall'accettare regalie od omaggi di non modico valore da parte di interlocutori istituzionali, controparti contrattuali o comunque da soggetti con cui la SOCIETÀ intrattenga rapporti di *business*; in ogni caso, hanno l'obbligo di comunicare al C.d.A., al Collegio Sindacale e all'ORGANISMO, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative a proprio pregressi o attuali rapporti economico-finanziari con i soggetti di cui sopra;

3.2. Comunicazioni all'esterno della società e rapporti con Autorità pubbliche di vigilanza

sono tempestivamente e correttamente effettuate, in modo veridico e completo, le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità o organi di vigilanza o controllo (italiani, sovranazionali o stranieri), del mercato o dei soci;

è prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;

la corrispondenza intrattenuta con le autorità di vigilanza è formalmente protocollata; la sua archiviazione è demandata, a seconda della materia trattata, all'Internal Auditing o altra funzione competente identificata;

3.3. Formalizzazione e separazione delle fasi: tracciabilità delle operazioni

devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate;

non deve esservi identità soggettiva tra coloro che assumono e attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;

deve essere individuato un responsabile delle operazioni (Responsabile del procedimento e della sua attuazione); se non diversamente ed eccezionalmente indicato, esso corrisponde al responsabile della funzione competente per la gestione dell'operazione considerata;

il Responsabile del procedimento può chiedere informazioni e chiarimenti a tutte le articolazioni funzionali, alle unità operative, ancorché dotate di autonomia, o ai singoli soggetti che si occupano o si sono occupati dell'operazione;

il Responsabile del procedimento deve informare periodicamente l'ORGANISMO di tutte le operazioni di carattere significativo che rientrano nell'area delle attività sensibili, fornendo, sotto la sua responsabilità, le informazioni necessarie per valutare la rischiosità dell'operazione e i suoi aspetti critici;

l'articolazione funzionale o l'unità organizzativa, alla quale sia richiesta un'informazione dai soggetti competenti, deve fornire la documentazione idonea a rispondere al quesito formulato, attestando la provenienza e, ove possibile, la completezza e la veridicità delle informazioni, o indicando i soggetti che possono fornire tale attestazione;

3.4. Tracciabilità delle operazioni e sistema informatico

è prevista l'adozione di sistemi informatici, che garantiscano la corretta e veridica imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile, ai soggetti che vi partecipano ed al cliente, controparte o ente interessati;

il sistema deve prevedere l'impossibilità di modifica delle registrazioni senza che ne risulti evidenza;

ogni accesso alla rete informatica aziendale — sia *intranet* che *internet* — per l'effettuazione di operazioni ovvero per la documentazione di dette operazioni deve avvenire almeno con l'utilizzo di doppia chiave asimmetrica (*user ID* e *password* personale), periodicamente variata, o con altra procedura di non minore efficacia, che consenta all'operatore di collegarsi alla rete limitatamente alla fase della procedura di sua competenza e di lasciare evidenza non modificabile dell'intervento effettuato e dell'autore;

3.5. Archiviazione e conservazione documenti

i documenti riguardanti l'attività di CHEMI S.P.A., ed in particolare i documenti o la documentazione informatica riguardanti l'attività di gestione del denaro e dei valori, sono archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;

ciascuna funzione garantisce la corretta archiviazione della documentazione aziendale al fine di assicurarne la tracciabilità e la documentabilità;

qualora il servizio di archiviazione o conservazione dei documenti sia svolto, per conto di CHEMI S.P.A., da un soggetto ad essa estraneo, il servizio è regolato da un contratto nel quale si prevede, tra l'altro, che il soggetto che presta il servizio alla SOCIETÀ rispetti specifiche procedure di controllo idonee a non permettere la modificazione successiva dei documenti, se non con apposita evidenza;

l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a loro delegato, al Collegio Sindacale od organo equivalente o ad altri organi di controllo interno, alla società di revisione eventualmente nominata e all'ORGANISMO;

3.6. Accesso e utilizzo del sistema informatico

sono previste modalità di utilizzo del sistema informatico basate su adeguato riscontro delle *password* di abilitazione per l'accesso ai sistemi informativi della P.A. eventualmente posseduti da determinati dipendenti appartenenti a specifiche funzioni o strutture aziendali;

sono predisposti strumenti informatici che impediscano l'accesso e/o la ricezione del materiale relativo alla pornografia minorile e in generale limitino gli accessi a siti *internet* potenzialmente a rischio di reato;

è stabilito con chiarezza, e comunicato ai dipendenti e a tutti coloro che hanno accesso al sistema, l'ambito del corretto e consentito utilizzo, ovvero per fini aziendali, degli strumenti informatici in possesso dei dipendenti;

non deve essere possibile l'installazione personale di *software sui personal computer* di ciascun dipendente, ma solo tramite intervento degli addetti al sistema informatico;

3.7. Trattamento dei dati personali

l'accesso ai dati personali in possesso di CHEMI S.P.A. ed il loro trattamento devono essere conformi al D. Lgs. n. 196/2003 e successive modifiche e integrazioni, anche regolamentari, e dunque anche al Regolamento (UE) n. 679/2016 e al D. Lgs. n. 101/2018;

l'accesso e il trattamento dei dati medesimi devono essere consentiti esclusivamente alle persone autorizzate e deve essere garantita la riservatezza nella trasmissione delle informazioni;

la Società ha adottato una serie di policy e di procedure in materia di privacy e data protection in conformità alla vigente normativa in materia (tra cui il Reg. EU 679/2016) che coprono i processi di data retention, gli aspetti organizzativi del privacy compliance framework, la gestione delle terze parti (data processor) e l'esercizio dei diritti degli interessati.

3.8. Sistema delle deleghe e delle procure

le procure devono essere coerenti con le deleghe interne;

sono previsti meccanismi di pubblicità delle procure nei confronti degli interlocutori esterni;

le deleghe sono attribuite secondo i principi di:

- autonomia decisionale e finanziaria del delegato;
- idoneità tecnico-professionale del delegato;
- disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni;

il soggetto munito di delega deve disporre di:

- poteri decisionali coerenti con le deleghe formalmente assegnate; un *budget* per l'efficace adempimento delle funzioni delegate, con la previsione di impegnare risorse eccedenti tale *budget* nel caso di eventi o situazioni di carattere eccezionale;
- di un obbligo di rendicontazione formalizzata, con modalità prestabilite, sulle funzioni delegate sufficienti a garantire un'attività di vigilanza senza interferenze;

3.9. Selezione di dipendenti, agenti, consulenti, collaboratori

la scelta dei dipendenti, dei consulenti e dei collaboratori avviene a cura e su indicazione dei Responsabili delle Funzioni della SOCIETÀ, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a questi criteri, la scelta deve essere motivata;

il processo di selezione dei candidati deve prevedere almeno due colloqui conoscitivi:

- il primo svolto da consulenti esterni o dalla funzione di risorse umane rivolto alla selezione di una rosa di candidati;
- il secondo colloquio di natura tecnica è svolto dal responsabile della Funzione interessata dall'assunzione o dall'A.D.;

successivamente al colloquio è prevista la compilazione da parte dell'intervistatore del modulo "intervista" di selezione, nel quale sono riassunte le caratteristiche del candidato;

le professionalità attestate dal candidato devono essere verificate da fonti terze; deve essere definito per iscritto il profilo tipo della risorsa da selezionare prima dell'avvio dei colloqui conoscitivi;

le assunzioni devono avvenire con regolare contratto di lavoro, nel rispetto di tutte le disposizioni normative vigenti nonché degli accordi contrattuali collettivi in essere, favorendo l'inserimento del lavoratore nell'ambiente di lavoro. In particolare, le funzioni competenti della SOCIETÀ devono verificare il possesso, da parte del soggetto con cui si intende avviare il rapporto di lavoro, di tutti i requisiti richiesti dalla legge per la permanenza e lo svolgimento dell'attività lavorativa richiesta nel territorio italiano. Analoghe verifiche devono essere esperite prima della conclusione di contratti di consulenza, agenzia, forme di lavoro parasubordinato, ovvero di appalto.

devono essere formalizzate le procedure al momento dell'assunzione: deve essere predisposto un *set* di documentazione tra cui informativa sulla c.d. *privacy* e dichiarazione del consenso; recente certificato del casellario generale; recente certificato dei carichi pendenti, ecc.

3.10. Formazione del personale

sono previste modalità efficienti per la formazione ed il costante aggiornamento dei dipendenti e dei collaboratori sulle regole e i presidi vigenti all'interno della struttura della SOCIETÀ posti a prevenzione dei reati di cui al DECRETO;

3.11. Formazione del personale in materia di sicurezza e salute dei lavoratori

è diffuso tra i dipendenti un documento di politica interna, che stabilisca gli indirizzi e gli obiettivi generali del sistema di prevenzione e protezione volti a perseguire obiettivi di adeguata tutela in materia di salute e sicurezza;

è previsto che si svolgano riunioni periodiche dei funzionari coinvolti per la verifica della situazione nella gestione delle tematiche afferenti alla salute e sicurezza;

è prevista una procedura che disciplini ruoli, responsabilità e modalità operative relativamente alla diffusione ai lavoratori delle informazioni periodiche e delle informazioni in caso di pericolo grave e immediato;

è prevista una disciplina relativa all'informativa al medico competente relativamente ai processi e rischi connessi all'attività produttiva;

3.12. Sistema delle retribuzioni e dei premi

eventuali sistemi premianti ai dipendenti e collaboratori devono rispondere ad obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate e con la struttura operativa disponibile;

non devono essere previsti né corrisposti compensi, provvigioni o commissioni a consulenti, collaboratori, e a soggetti pubblicisticamente qualificati in misura non congrua rispetto alle prestazioni rese alla SOCIETÀ e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e con riferimento alle condizioni e alle prassi esistenti sul mercato nell'area geografica di riferimento o determinate da tariffe;

è valutata e disciplinata con particolare attenzione l'organizzazione diretta o indiretta di viaggi o di periodi di permanenza in località estere con specifico riguardo ai principi della morale;

3.13. Selezione di fornitori, controparti commerciali e partners

la scelta dei fornitori di beni o servizi avviene, a cura della funzione competente, sulla base di requisiti di professionalità, affidabilità, economicità, pari trattamento, trasparenza nelle procedure di selezione;

sono sempre definiti i requisiti minimi in possesso dei soggetti offerenti e la fissazione dei criteri di valutazione delle offerte prima della ricezione delle stesse;

è prevista una procedura di qualificazione e certificazione dei fornitori che tenga conto della rispondenza di quanto fornito con le specifiche di acquisto;

il principio di economicità non può mai prevalere sul criterio dell'affidabilità;

3.14. Regolamentazione dei rapporti con fornitori, consulenti, controparti contrattuali e partners

nei contratti con le controparti commerciali, con i consulenti e con i *partners* è contenuta apposita clausola con cui questi dichiarino:

- di essere a conoscenza della normativa di cui al DECRETO e delle sue implicazioni per la SOCIETÀ;
- di impegnarsi al rispetto del DECRETO;
- se si tratta di società, di avere adottato il Modello organizzativo previsto dal DECRETO, documento analogo o adeguato sistema di procedure di controllo;

nei contratti con le controparti commerciali, con i consulenti e con i *partners* è contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al DECRETO (es. clausole risolutive espresse, penali);

è verificato il rispetto, da parte dei fornitori, della normativa vigente in materia di lavoro con particolare attenzione al lavoro minorile e a quanto disposto dalla legge in tema di igiene, salute e sicurezza;

è richiesto e verificato il rispetto, da parte dei propri *partners*, degli obblighi di legge in tema di tutela del lavoro minorile e delle donne; di condizioni igienico – sanitarie e di sicurezza; di diritti sindacali o comunque di associazione e rappresentanza;

3.15. Gestione del processo di approvvigionamento beni e servizi

non vi deve essere identità tra chi richiede la prestazione, chi la autorizza e chi esegue il pagamento della stessa. Devono essere chiaramente formalizzati i compiti, i poteri e le responsabilità attribuiti a ciascuno;

è effettuata la precisa identificazione di una funzione/unità responsabile della definizione delle specifiche tecniche e della valutazione delle offerte;

è prevista l'autorizzazione da parte di posizione superiore abilitata diversa dal gestore del contratto, in caso di modifiche sostanziali /integrazioni e/o rinnovi dello stesso;

è previsto il divieto, nei confronti di fornitori o consulenti, di cedere a terzi il diritto alla esecuzione della prestazione dedotta nel contratto, alla riscossione del compenso o di attribuire a terzi il mandato all'incasso;

3.16. Gestione risorse finanziarie

sono stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone;

il processo inerente al pagamento dei fornitori deve essere formalizzato e improntato al principio di *segregation of duties*, in forza del quale il censimento del fornitore, l'entrata merce, la contabilizzazione della fattura ed il relativo pagamento devono essere svolte da soggetti distinti;

le operazioni che comportano utilizzazione o impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità con i principi di professionalità e correttezza gestionale e contabile. Il processo decisionale deve essere verificabile;

l'impiego di risorse finanziarie deve essere motivato dal soggetto richiedente, che ne attesta la congruità;

in caso di operazioni ordinarie, se comprese entro la soglia quantitativa stabilita, la motivazione può essere limitata al riferimento alla classe o tipologia di spesa alla quale appartiene l'operazione;

il superamento dei limiti di cui al punto precedente può avvenire previa adeguata motivazione e relativa autorizzazione. Comunque, in caso di operazioni diverse dalle ordinarie o eccedenti la soglia quantitativa stabilita, la motivazione deve essere analitica;

tutte le operazioni di acquisizione, gestione e trasferimento di denaro o valori devono essere documentate, in ogni loro fase, a cura delle funzioni competenti, con la possibilità di individuare le persone fisiche intervenute nei passaggi;

deve essere verificata la regolarità dei pagamenti nel rispetto delle vigenti procedure con riferimento alla piena coincidenza dei destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione;

l'Ufficio contabilità deve per ogni acquisto verificare la coincidenza tra contratto/ordine di acquisto, fattura e documenti di trasporto nonché accertare, con la Funzione che ha emesso l'ordine, l'effettiva consegna del bene o fornitura del servizio, contabilizzare l'operazione;

il dipendente deve ottenere l'autorizzazione del proprio responsabile per il rimborso delle spese sostenute nell'ambito lavorativo; tale rimborso è accreditato tramite bonifico contestualmente all'erogazione degli stipendi;

la tipologia di spese rimborsabili dalla SOCIETÀ ai DIPENDENTI deve essere espressamente disciplinata;

devono essere effettuati periodici controlli formali e sostanziali dei flussi aziendali, con riferimento a pagamenti verso terzi e ai pagamenti delle operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte, degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e istituti che non hanno insediamenti fisici in alcun paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni ed operazioni straordinarie;

3.17. Rapporti economico-finanziari con la P.A. o suoi esponenti

i contatti con esponenti della P.A. devono essere specificamente motivati;

deve essere previsto un obbligo di immediata informativa all'ORGANISMO in caso di proposte o richieste illecite o sospette avanzate da appartenenti alla P.A. o da soggetti pubblicisticamente qualificati;

3.18. Rapporti con intermediari finanziari

la SOCIETÀ, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie ed ai fini dell'attuazione delle operazioni di acquisizione, gestione o trasferimento di denaro o valori, deve avvalersi di intermediari finanziari e bancari sottoposti a una

regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;

è obbligatorio utilizzare esclusivamente, nell'ambito della gestione delle transazioni finanziarie, operatori finanziari muniti di presidi manuali e informatici idonei a prevenire fenomeni di riciclaggio nazionale o internazionale;

deve essere previsto il divieto di utilizzo del contante per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie;

deve essere previsto il divieto di accettazione ed esecuzione di ordini di pagamento provenienti da soggetti non identificabili;

deve essere previsto che il pagamento relativo a beni o servizi acquistati dalla SOCIETÀ debba essere effettuato esclusivamente sul conto corrente intestato al fornitore. Deve in generale essere previsto che i pagamenti non possano, in nessun caso, essere effettuati su conti correnti cifrati;

deve essere fornita adeguata giustificazione circa la specifica legittimità e congruenza dei pagamenti effettuati su conti correnti di banche appartenenti od operanti in paesi elencati tra i così detti "paradisi fiscali" o in favore di società *off shore*;

è previsto che il pagamento corrisponda esattamente a quanto indicato nel contratto, salvo eccezioni autorizzate;

è previsto che il pagamento relativo a beni o servizi acquistati dalla Società non possa essere effettuato in favore di un soggetto diverso dalla controparte contrattuale o in un paese terzo rispetto a quello delle parti contraenti o a quello di esecuzione del contratto, salvo che sia fornita adeguata giustificazione circa la specifica legittimità e congruenza dei pagamenti medesimi;

3.19. Trasferimenti di beni aziendali

per le operazioni di acquisizione e dismissione di società o rami d'azienda, è preventivamente verificata la provenienza dei beni conferiti nel patrimonio della società

o del ramo di azienda da acquistare nonché l'identità, la sede, la natura giuridica, la certificazione antimafia del soggetto cedente;

3.20. Rilevazione, registrazione e rappresentazione dell'attività societaria nelle scritture contabili, nei bilanci, nelle relazioni ed in altri documenti

in ogni articolazione funzionale o unità organizzativa competente sono adottate misure idonee a garantire che le operazioni contabili siano effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza e siano tempestivamente segnalate eventuali situazioni anomale;

sono previste misure idonee a garantire che l'informazione comunicata ai soggetti gerarchicamente sovraordinati da parte dei responsabili dell'articolazione funzionale o dell'unità organizzativa competente sotto ordinata sia veritiera, corretta, accurata, tempestiva e documentata, anche con modalità informatiche;

sono previste misure idonee ad assicurare che, qualora siano formulate richieste, da chiunque provenienti, di atipica variazione quantitativa dei dati, rispetto a quelli già contabilizzati, chi ne sia a conoscenza informi, senza indugio, l'ORGANISMO;

sono previste misure idonee a garantire che, qualora siano formulate ingiustificate richieste di variazione dei *criteri* di rilevazione, registrazione e rappresentazione contabile, chi ne sia a conoscenza informi, senza indugio, l'ORGANISMO;

deve essere previsto l'obbligo per chi fornisce informazioni previste alle unità gerarchicamente sovraordinate di indicare i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, al fine di garantire la verificabilità delle stesse. Le copie dei documenti richiamati devono essere rese disponibili;

3.21. Acquisto, vendita o altre operazioni, in qualsiasi forma concluse, di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato e alla stipulazione di contratti derivati non negoziati su mercati regolamentati italiani ed europei

la gestione degli investimenti finanziari e dei rischi collegati è regolamentata sulla base di apposite prassi operative, le quali prevedono uno specifico iter autorizzativo;

3.22. Gestione degli adempimenti in materia fiscale

I seguenti principi di comportamento di carattere generale si applicano ai destinatari del presente MODELLO che, a qualunque titolo, direttamente o indirettamente, siano coinvolti nelle attività “sensibili” rispetto ai delitti tributari.

In via generale, a tali soggetti è richiesto di:

garantire la segregazione dei compiti tra le attività di determinazione e verifica della correttezza del calcolo delle imposte dirette e indirette;

garantire la piena e puntuale ricostruzione ex post e la tracciabilità delle operazioni concernenti la determinazione delle imposte sui redditi o sul valore aggiunto;

garantire la corretta tenuta di tutte le scritture contabili e dei documenti di cui è obbligatoria la conservazione nel rispetto degli adempimenti tributari;

in occasione di ispezioni ed accertamenti in materia fiscale, evitare atteggiamenti intenzionalmente volti ad occultare o sottrarre all’ispezione la documentazione richiesta, ovvero comportamenti idonei ad ostacolare la normale prosecuzione delle operazioni ispettive.

È inoltre previsto, a carico di tali soggetti, l’espreso divieto di:

presentare dichiarazioni relative alle imposte sui redditi o sul valore aggiunto contenenti elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti;

presentare dichiarazioni relative alle imposte sui redditi o sul valore aggiunto contenenti elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o

crediti e ritenute fittizi, 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;

nell'ambito di sistemi transfrontalieri, rappresentare elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, ovvero omettere la presentazione della dichiarazione sul valore aggiunto ovvero il pagamento delle somme dovute utilizzando in compensazione crediti inesistenti o non spettanti, al fine di evadere le imposte sul valore aggiunto;

emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto;

occultare o distruggere 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, al fine di evadere le imposte, ovvero di consentirne l'evasione a terzi;

alienare simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva, al fine di sottrarsi al pagamento delle imposte ovvero di interessi o sanzioni amministrative relativi a dette imposte;

indicare nella documentazione presentata ai fini della transazione fiscale elementi attivi per un ammontare inferiore quello reale o elementi passivi fittizi per un ammontare complessivo superiore;

registrare poste valutative di bilancio (ad es. fatture da emettere/da ricevere, valutazione cespiti, valutazione immobilizzazioni immateriali, ecc.) non conformi alla reale situazione patrimoniale, economica, finanziaria della Società ed ai principi contabili di riferimento.

La SOCIETÀ inoltre garantisce:

che il processo di determinazione delle imposte derivi da una rappresentazione del bilancio d'esercizio veritiera, secondo i principi contabili di riferimento;

che il personale adibito ai processi tax e alla predisposizione delle dichiarazioni fiscali sia adeguatamente formato in materia;

un'adeguata attività di monitoraggio degli aggiornamenti normativi in materia fiscale;

la compilazione e la trasmissione della dichiarazione dei redditi nel rispetto dei tempi e modi previsti dalla legge;

nel caso in cui alcune attività siano parzialmente esternalizzate a professionisti esterni, l'utilizzo di figure professionali di comprovata esperienza e con adeguata formazione in materia;

che l'archiviazione di tutta la documentazione rilevante, in formato cartaceo ovvero elettronico, sia effettuata nel rispetto delle previsioni normative e secondo standard atti a garantire la tracciabilità, la veridicità, l'immediata recuperabilità dei documenti.

Tra l'altro, sono attuati controlli operativi, nell'ambito dei processi amministrativo contabili e fiscali, ai fini di:

assicurare che le anagrafiche fornitori/clienti siano aggiornate e riflettano correttamente tutti gli elementi di esistenza / qualificazione anagrafica del fornitore;

nell'ambito dei processi di qualificazione del fornitore e di attivazione di rapporti commerciali con clienti e distributori, garantire che gli stessi siano correttamente identificati e valutati anche in termini di reputazione sul mercato, qualità delle prestazioni rese/attese, affidabilità operativa, patrimoniale, finanziaria, ecc.;

definire i criteri di approvazione degli ordini di acquisto;

eseguire approfondimenti sulla tipologia (soggetto Iva o meno) del fornitore al fine della corretta attribuzione dell'aliquota Iva e del relativo regime applicabile;

verificare la sede o residenza del fornitore/consulente e/o agente utilizzati nelle transazioni commerciali, al fine di individuare l'eventuale esistenza di un collegamento con Paesi considerati potenzialmente "a rischio" (ad es. Paesi riconosciuti quali "paradisi fiscali", Paesi a rischio terrorismo, ecc.) e di garantire la correttezza del trattamento fiscale delle operazioni e dei soggetti coinvolti.

assicurare che eventuali forniture non processate con ordine di acquisto o al di fuori delle procedure standard, siano adeguatamente verificate, in termini di prestazione resa, prima della registrazione della fattura passiva;

assicurare che i beni/servizi consegnati dai fornitori siano correttamente riscontrati con gli ordini di acquisto emessi o coi contratti relativi, anche in termini di tracciabilità della prestazione resa;

garantire che il pagamento di fatture passive sia autorizzato solo dopo avere eseguito i controlli di cui ai due punti precedenti;

riconciliare i conti fiscali e verificare le poste indetraibili/indeducibili, le variazioni in aumento /diminuzione, ecc.;

effettuare valutazioni analitiche in merito alle perdite pregresse e alle imposte anticipate e differite;

validare i prospetti contabili rilevanti prima dell'eventuale invio a professionisti esterni incaricati della revisione delle componenti di reddito non deducibili e detraibili, delle verifiche di compliance del calcolo delle imposte rispetto alla vigente normativa, ecc.

Nello svolgimento dell'attività di redazione del bilancio d'esercizio la SOCIETÀ assicura: la tenuta e custodia delle scritture contabili nel rispetto delle modalità e termini previsti dalla legge;

che gli effetti delle rilevazioni contabili con impatto fiscale vengano calcolati e registrati nel rispetto della normativa applicabile;

che le transazioni siano registrate in contabilità solo dopo opportuni controlli interni circa la loro rispondenza a documenti di supporto, e in termini di esistenza, inerenza e competenza delle operazioni sottostanti, anche nell'ambito dei rapporti con l'estero;

che gli effetti delle rilevazioni contabili con impatto fiscale siano calcolati e registrati nel rispetto della normativa applicabile.

Nella gestione degli adempimenti ed operazioni in materia Societaria:

la SOCIETÀ si ispira alle normative di riferimento (Codice Civile, norme tributarie e Leggi Speciali - es. DPR n. 633/1972 “Disciplina dell’IVA”, DPR n. 600/1973 “Accertamento Imposte sui redditi” -, Legge n. 383/2001 “Primi interventi per il rilancio dell'economia”, D.M. 23 gennaio 2004 “Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto, etc.), ai regolamenti nonché alle disposizioni a cui ha formalmente aderito (Codice Etico, Policies di gruppo, etc.), garantendo un’adeguata attività di monitoraggio degli aggiornamenti normativi;

la SOCIETÀ provvede all’individuazione delle Funzioni aziendali incaricate e legittimate alla tenuta e conservazione dei libri sociali nel rispetto delle modalità e termini previsti dalla legge;

la SOCIETÀ garantisce la puntuale archiviazione della documentazione obbligatoria prevista dalle normative di riferimento in modo da permettere la ricostruzione dei redditi e del volume di affari;

le Funzioni addette alla tenuta dei registri devono tempestivamente informare gli organi competenti in caso di eventi accidentali che possono deteriorare le scritture.

La SOCIETÀ assicura la tracciabilità nell’ambito della gestione dei rapporti Intercompany, attraverso:

l’ispirazione alle normative di riferimento, anche di natura tributaria, ai regolamenti nonché alle disposizioni a cui ha formalmente aderito (Codice Etico, Policies di Gruppo, ecc.).

un sistematico flusso documentale generato nell’ambito dei rapporti stessi atto a garantirne l’oggettiva esistenza (tra i servizi aziendali e tra le SOCIETÀ del Gruppo coinvolte);

la conservazione e archiviazione della documentazione amministrativo-contabile.

Nella gestione dei contenziosi e degli eventuali accordi transattivi con l’Autorità giudiziale, la SOCIETÀ:

deve presentare una documentazione veritiera ai fini della procedura di transazione fiscale, i cui elementi attivi/passivi devono corrispondere a quelli reali;

effettua specifici controlli al fine di assicurare il rispetto del divieto di alienare simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni mobili/immobili idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria.

deve garantire che tutte le operazioni societarie siano rispondenti alla realtà, verificandone i soggetti coinvolti e la documentazione a supporto;

la direzione aziendale rivede periodicamente i verbali delle verifiche fiscali per valutare la necessità di stanziamenti per eventuali sanzioni e/o versamenti aggiuntivi;

in caso di avvio di un procedimento di riscossione coattiva o di procedura di transazione fiscale, ne deve essere tempestivamente informato l'Organismo di Vigilanza.

3.23. Gestione degli adempimenti doganali

I seguenti principi di comportamento di carattere generale si applicano ai destinatari del presente MODELLO che, a qualunque titolo, direttamente o indirettamente, siano coinvolti nelle attività "sensibili" rispetto ai reati di contrabbando.

In via generale, a tali soggetti è richiesto di:

rispettare la normativa di riferimento in tema di importazione, esportazione e circolazione delle merci ed in particolare in riferimento al pagamento dei diritti di confine dovuti all'Amministrazione doganale (Agenzia delle dogane e dei Monopoli);

tenere condotte tali da garantire una lecita concorrenza nei confronti del commercio;

garantire la pratica doganale nelle operazioni con l'estero in maniera trasparente;

garantire la libera circolazione delle merci extra UE all'interno del territorio dell'Unione Europea attraverso il pagamento dei tributi doganali previsti dalle normative di riferimento.

È inoltre previsto, a carico di tali soggetti, l'espresso divieto di:

nelle operazioni di importazione, esportazione e circolazione delle merci extra UE, sottrarsi al totale o parziale pagamento dell'obbligazione doganale lesiva degli interessi dell'Unione alla puntuale e tempestiva riscossione delle risorse proprie;

sottrarre la merce al sistema di controllo della dogana istituito per l'accertamento e la riscossione dei diritti di confine, non dichiarandola alla stessa oppure occultandola o falsificando i documenti di trasporto e/o commerciali (es. attribuendo alla merce all'interno dei documenti doganali, un valore ridotto rispetto a quello che viene normalmente indicato per analogo prodotto proveniente dal medesimo paese di origine, o nell'ipotesi in cui all'interno dei documenti certificanti il trasporto venga indicato un quantitativo di merce inferiore a quello in esubero, accertato in sede di visita da parte del delegato al controllo, ecc.);

introdurre, scaricare, depositare o asportare merci estere in violazione delle prescrizioni, dei divieti e delle limitazioni stabiliti dalla normativa di riferimento;

costituire, in territori extra doganali, depositi non permessi di merci estere soggetti a diritti di confine, o costituzione di depositi in misura superiore a quella consentita;

usare impropriamente merci estere importate in franchigia e con riduzione dei diritti di confine, destinandole o utilizzandole in modo differente da quello per il quale la franchigia o la riduzione erano state concesse;

introdurre nello Stato di merci estere in sostituzione di merci nazionali o nazionalizzate spedite in cabotaggio od in circolazione;

ottenere un'indebita restituzione di diritti stabiliti per l'importazione delle materie prime impiegate nella fabbricazione di merci nazionali che si esportano attraverso l'utilizzo di mezzi fraudolenti;

nelle operazioni di importazione/esportazione temporanea o nelle operazioni di riesportazione/reimportazione, sottrarre merci al pagamento di diritti di confine attraverso la manipolazione artificiosa delle stesse ovvero attraverso l'utilizzo di mezzi fraudolenti;

omettere o ritardare la presentazione della dichiarazione doganale, ovvero, gestire impropriamente le formalità doganali attraverso l'indicazione di informazioni non veritiere circa la quantità, qualità o il valore delle merci.

3.24. Rispetto delle tutele della proprietà industriale e del diritto di autore

prima della commercializzazione dei prodotti (esportati o importati che siano, sia sviluppati dalla SOCIETÀ che ricevuti in licenza da terzi) o della loro fabbricazione in Stati che riconoscono titoli e diritti di proprietà industriale, è verificata l'eventuale sussistenza di - o se comunque possano essere violate - valide privative di terzi (fondamentalmente, nel nostro caso, brevetti d'invenzione, marchi e *know-how* non brevettato ma segreto, sostanziale e identificato);

la gestione delle predette verifiche è svolta in coordinamento con la Direzione Legale della SOCIETÀ sia per i brevetti che per i marchi;

le verifiche, svolte anche con il supporto di qualificati consulenti specializzati esterni, possono essere corredate da parere scritto della Direzione Legale e dell'eventuale consulente e devono essere trasmesse all'Amministratore Delegato per la decisione finale;

anche il deposito di domande di brevetto d'invenzione o di registrazione di marchio deve essere preceduto da apposite verifiche di anteriorità sia dello stato dell'arte in generale che, specificamente, dei titoli altrui esistenti nel Paese o Paesi di interesse, così da assicurare che siano rispettati i requisiti di novità e inventività per quanto riguarda i brevetti e di originalità e non confondibilità per quanto riguarda i marchi;

eventuali impugnazioni od opposizioni in sede amministrativa o giudiziale nei confronti di altrui brevetti o marchi sono pure precedute da accurate verifiche che confermino l'illegittimità o nullità, in tutto o in parte, di tali titoli e devono essere approvate dall'Amministratore Delegato con parere favorevole della Direzione Legale;

le domande di brevetto sono elaborate dalla Direzione R&D della SOCIETÀ; i marchi dai rispettivi settori commerciali o di *licensing*. Le domande e i marchi candidati, che possono essere corredate da adeguato parere della Funzione Legale in esito alle verifiche effettuate, sono trasmessi all'Amministratore Delegato per la decisione finale;

laddove, per esigenze di urgenza, la decisione finale dell'Amministratore Delegato non possa essere preceduta da adeguate verifiche, la possibilità di procedere al deposito della domanda di brevetto o del marchio è subordinata ad adeguata motivazione di tale deroga condivisa con la Direzione Legale;

per il *know-how* confidenziale non brevettato ricevuto da terzi sulla base di accordi di segretezza o di altro tipo, la comunicazione può essere effettuata all'interno solo sulla base di una necessità di conoscenza (principio *need to know*) delle persone qualificate che siano effettivamente coinvolte nella valutazione e/o uso di tale *know-how*;

la diffusione di pubblicazioni, scientifiche o di altro tipo, e degli estratti o copie di queste, può essere disposta dalla funzione aziendale interessata solo previa verifica, da parte della Funzione Legale, del rispetto delle normative vigenti in tema di diritto di autore.

3.25. Garanzia di natura, qualità, conformità dei prodotti commercializzati

sono previsti adeguati meccanismi di controllo per evitare che il prodotto consegnato all'acquirente sia diverso per natura, origine, provenienza, qualità o quantità rispetto a quello dichiarato o pattuito;

3.26. Gestione degli asset aziendali in materia di sicurezza e salute dei lavoratori

le attività ed i rapporti di manutenzione o ispezione degli asset aziendali necessari a garantire il rispetto della normativa su sicurezza e igiene sul lavoro sono disciplinate da un'apposita procedura;

3.27. Pianificazione del servizio di prevenzione e protezione della sicurezza e salute dei lavoratori

sono predisposti un *budget*, piani annuali e pluriennali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza;

3.28. Organizzazione della struttura con riferimento alle attività in tema di sicurezza e salute dei lavoratori

sono previsti un piano di prevenzione e protezione, le relative modalità di attuazione e il relativo sistema di periodico monitoraggio;

sono disciplinati i ruoli, le responsabilità e le modalità di gestione del servizio di prevenzione e protezione all'interno dell'organizzazione;

sono definiti, in coerenza con le disposizioni di legge vigenti in materia, i meccanismi relativi a:

- valutazione e controllo periodico dei requisiti di idoneità e professionalità del responsabile del servizio di prevenzione e protezione (c.d. RSPP) e degli addetti al servizio di prevenzione e protezione (c.d. SPP);
- definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;
- processo di nomina e relativa accettazione da parte del Medico Competente, con evidenziazione delle modalità e della tempistica in caso di avvicendamento nel ruolo;

3.29. Individuazione, valutazione e mitigazione dei rischi in materia di sicurezza e salute dei lavoratori

è definita una procedura relativa alla predisposizione del Documento di Valutazione dei Rischi (c.d. DVR) che preveda, fra l'altro, l'identificazione dei soggetti preposti, le modalità operative di redazione del DVR, le responsabilità per la verifica e l'approvazione dei contenuti dello stesso, le attività per il monitoraggio dell'attuazione e dell'efficacia delle azioni a tutela della salute e sicurezza al fine di riesaminare i rischi e provvedere all'aggiornamento dello stesso documento;

3.30. Attività di monitoraggio in materia di sicurezza e salute dei lavoratori

è predisposta una procedura relativa al monitoraggio sistemico e continuo dei dati/indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il sistema di prevenzione e protezione che preveda, tra l'altro:

- ruoli e responsabilità;

- la definizione e la formalizzazione di specifici indicatori di performance relativamente alle attività di gestione del Sistema di Prevenzione e Protezione che consentano di valutarne l'efficacia e l'efficienza;
- la disciplina delle attività di monitoraggio;
- l'analisi e l'implementazione delle eventuali azioni correttive per eventuali carenze nel sistema;

la procedura relativa al monitoraggio deve prevedere la tracciabilità degli incidenti occorsi, dei mancati incidenti e delle situazioni potenzialmente dannose, l'attività di rilevazione e registrazione degli stessi e la loro investigazione;

3.31. Attività di Audit in materia di sicurezza e salute dei lavoratori

sono individuate disposizioni organizzative relative al campo di applicazione, alla frequenza, alla metodologia, alle competenze, ai ruoli e alle responsabilità e i requisiti per la conduzione delle attività di *audit* e la registrazione e la comunicazione dei risultati sull'effettiva ed efficace applicazione delle soluzioni tecniche e organizzative atte alla gestione e al controllo di tutti gli aspetti operativi, che tengano conto delle prescrizioni legali e dei regolamenti aziendali;

sono previste e pianificate sistematiche verifiche dello stato di attuazione delle misure adottate atte a neutralizzare il rischio per la salute e sicurezza dei lavoratori; azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dalle suddette specifiche soluzioni tecniche e organizzative; la verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;

è definita una disposizione organizzativa che disciplini ruoli, responsabilità e modalità operative dello specifico *reporting* periodico, nei confronti dell'Amministratore delegato e dell'ORGANISMO, relativo alle attività svolte al fine di valutare l'efficacia e l'adeguatezza del sistema;

3.32. Gestione del sistema di prevenzione e protezione della sicurezza e salute dei lavoratori

sono definite procedure in merito alle fasi dell'attività di predisposizione e attuazione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori, prevedendo, in particolare:

- la trascrizione e l'archiviazione dei risultati degli accertamenti sanitari dei singoli lavoratori nelle Cartelle Sanitarie e di Rischio;
- la gestione, la distribuzione, il mantenimento in efficienza dei dispositivi di protezione individuale (c.d. DPI);
- le modalità operative per la nomina dei lavoratori incaricati dell'attuazione delle misure di prevenzione, di emergenza e di primo soccorso;
- le modalità operative per la gestione della segnaletica di sicurezza;
- le modalità operative per l'accesso dei lavoratori in aree a rischio per la salute e sicurezza;
- le modalità operative, i ruoli e le responsabilità in caso di eventuali situazioni di emergenza;
- le modalità operative per l'abbandono del posto di lavoro o zona pericolosa in cui persiste un pericolo grave e immediato;
- le misure organizzative per l'individuazione dei tempi e delle modalità per l'effettuazione della richiesta del rilascio o rinnovo del certificato di prevenzione incendi, nonché del rilascio del nullaosta provvisorio;

sono predisposte *check list* finalizzate all'adozione di misure operative atte ad evitare il verificarsi di incidenti, che prevedano, tra l'altro, l'elencazione dei compiti critici e dei processi a impatto sulla salute e sicurezza, dei DPI condivisi con il responsabile del servizio di prevenzione e protezione, dei prodotti e dei processi pericolosi, delle apparecchiature critiche;

è definito e collaudato (anche mediante prove di emergenza) un piano di emergenza ed una procedura di gestione delle emergenze atta a mitigare gli effetti sulla salute della popolazione e sull'ambiente esterno;

sono previste specifiche procedure relative alla problematica degli infortuni che prevedano:

- definizione di ruoli, responsabilità e modalità operative per la segnalazione e la gestione degli infortuni; l'esistenza di una *check list* mirata a definire le tipologie e la dinamica degli infortuni sul lavoro sulla base di quanto previsto dalla normativa vigente;

sono stabiliti ruoli e responsabilità per la definizione e l'attuazione di modalità organizzative atte a tutelare i lavoratori dai rischi connessi alle attività svolte, all'ambiente di lavoro, all'utilizzo di attrezzature e macchine e dai rischi connessi all'impiego di sostanze pericolose, agenti chimici, fisici, biologici, cancerogeni;

è previsto un dovere di valutazione del rischio di incendio, di predisposizione ed aggiornamento del registro antincendio, di predisposizione di un piano di emergenza;

3.33. Coinvolgimento del personale in materia di sicurezza e salute dei lavoratori

sono previste riunioni periodiche con la dirigenza, con il Medico Competente e i rappresentanti dei lavoratori;

è prevista la consultazione preventiva dei rappresentanti dei lavoratori in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;

3.34. Sistema di gestione della sicurezza (D. Lgs. 105/2015, c.d. Direttiva Seveso)

sono previste apposite procedure a presidio del sistema costituito da:

- documento di politica aziendale firmato dal legale rappresentante e distribuito a tutti i dipendenti;
- riesame del sistema a frequenza almeno annuale o in occasione di eventi particolari o significativi cambiamenti;
- documentazione del SGS;
- manuale procedure SGS;

- gestione delle modifiche di impianto e di processo gestione degli incidenti o quasi incidenti;
- *Auditors* interni e sistema di *self audit*;
- formazione del personale relativamente alla legge e al SGS in senso lato;
- piani di emergenza generale e di reparto;
- squadre di emergenza generale e di reparto;
- squadre di emergenza e primo soccorso;
- addestramento dei nuovi dipendenti all'emergenza;
- valutazione dei pericoli ed analisi dei rischi di primo livello;
- valutazione degli adempimenti di legge da espletare per ogni nuovo impianto/processo;
- documento di non aggravio di rischio per nuovi processi ed impianti;

Sono inoltre previste apposite procedure a presidio:

- dell'obbligo notifica nel caso superamento limiti di stoccaggio delle sostanze pericolose ex artt. 13 e 14 del D.lgs. 105/15;
- del controllo delle giacenze di sostanze pericolose per non superamento dei limiti della notifica;

3.35. Rispetto della normativa in materia di tutela dell'ambiente e adeguamento delle soluzioni tecniche

è redatta una "vendor list ambientale" in cui sono omologati tutti i fornitori o consulenti che la Società ha valutato idonei per la realizzazione dei presidi o per l'individuazione degli stessi;

3.36. Pianificazione dei presidi a tutela dell'ambiente in conformità alle prescrizioni normative

sono predisposti un *budget*, piani annuali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di tutela dell'ambiente;

ogni soluzione scelta deve essere adeguatamente motivata in merito alla prevalenza del criterio della migliore tutela ambientale rispetto al risparmio di tempi e di costi;

tracciabilità e separazione nelle fasi di tutto il procedimento di individuazione e realizzazione dei presidi (documentazione a supporto, verbalizzazione, intestazione e formalizzazione dei documenti, archiviazione degli stessi);

3.37. Attività di monitoraggio dei presidi a tutela dell'ambiente in conformità alle prescrizioni normative

è predisposta una procedura relativa al monitoraggio sistemico e continuo dei dati/indicatori che rappresentano le caratteristiche principali dei vari presidi a tutela dell'ambiente che preveda, tra l'altro:

- ruoli e responsabilità;
- periodicità e criteri di selezione;
- la definizione e la formalizzazione di specifici indicatori di *performance* relativamente ai presidi che consentano di valutarne l'efficacia e l'efficienza;
- la disciplina delle attività di monitoraggio;
- l'analisi e l'implementazione delle eventuali azioni correttive per eventuali carenze nel sistema;

la procedura relativa al monitoraggio deve prevedere la tracciabilità degli incidenti occorsi, dei mancati incidenti e delle situazioni potenzialmente dannose, l'attività di rilevazione e registrazione degli stessi, la loro investigazione, i provvedimenti in merito adottati, la loro tempestività ed efficacia nonché le relative comunicazioni agli enti competenti;

le procedure devono prevedere la verifica della corrispondenza delle dichiarazioni/certificazioni presentate con la documentazione tecnica di supporto;

3.38. Attività di Audit in materia di tutela dell'ambiente

sono effettuate dal Responsabile del magazzino sessioni di audit presso i Fornitori di Servizi Ambientali, sulla base di check-list specifiche, finalizzate ad accertare il grado di compliance alle prescrizioni legali e regolamenti in materia. Vengono redatti ed archiviati verbali relativi alle sessioni di audit effettuate;

3.39. Coinvolgimento e formazione del personale in materia di tutela dell'ambiente

sono previste riunioni periodiche con la dirigenza, con i lavoratori e i loro rappresentanti ai fini di una maggiore sensibilizzazione sui temi della tutela ambientale;

3.40. Individuazione di specifici presidi per aree di particolare rischio

GAS TOSSICI

Stoccaggio e impiego dei gas tossici

sono previste prassi operative:

- per la tenuta registri di carico e scarico, la gestione degli *stock* in funzione del massimo consentito;
- per la selezione di personale addetto fornito di patenti rilasciate dal Ministero dell'Interno e da rinnovarsi periodicamente;

INCENDI

Sicurezza degli impianti elettrici e sistema antincendio

sono previste prassi operative al fine di presidiare:

- la richiesta, in fase di ordine, del certificato di conformità dell'opera e di corretta installazione;
- l'archiviazione della documentazione originale;
- la consegna della certificazione ai VV.FF. in sede di rinnovo del CPI;
- i controlli periodici di ARPA o altri enti notificatori;

Prevenzione incendi

sono previste prassi operative al fine di presidiare:

- la richiesta del parere di conformità prevenzione incendi per nuovi impianti, la richiesta di sopralluogo ed aggiornamento CPI;
- la richiesta di rilascio del CPI di stabilimento corredata da perizia giurata e dichiarazione "nulla è mutato";
- il registro di prevenzione incendi e le verifiche periodiche delle attrezzature di spegnimento e dei sistemi di rilevazione incendi;

RIFIUTI

Gestione del catasto dei rifiuti e della denuncia annuale di produzione e smaltimenti

sono previste prassi operative al fine di presidiare:

- l'autorizzazione periodica per il deposito di rifiuti speciali/pericolosi solidi e liquidi;
- la tenuta dei registri di carico e scarico;
- la gestione dei processi di conferimento dei rifiuti a società autorizzate allo smaltimento;
- la compilazione formulari ecologici;
- l'omologa dei rifiuti;
- la spedizione e controllo dell'avvenuta consegna;
- la verifica dell'avvenuto smaltimento;
- la dichiarazione MUD annuale;
- l'identificazione e codifica CER dei nuovi rifiuti;
- l'archiviazione decennale della documentazione;
- sistema gestione e tracciabilità rifiuti

Tracciabilità dei rifiuti

sono previste apposite procedure per presidiare il periodico adeguamento alla normativa relativa alla tracciabilità dei rifiuti speciali pericolosi;

BONIFICHE E RIPRISTINO AMBIENTALE

Eventuale messa in sicurezza, bonifica e ripristino ambientale dei siti interessati

sono previste attività di monitoraggio a presidio della realizzazione:

- della caratterizzazione del sito;
- del progetto di messa in sicurezza dell'impianto di attuazione;
- del progetto provvisorio di bonifica ed attuazione;
- del progetto definitivo di bonifica ed attuazione;
- della verifica periodica dello stato del sito, trattamento dei reflui, monitoraggio analitico periodico e riesame dell'efficacia del trattamento;

ATTREZZATURE PARTICOLARI

Gestione attrezzature a pressione

sono previste prassi operative a presidio:

- dell'acquisto ed installazione di apparecchiature costruite solo da fornitori certificati che applicano la direttiva delle apparecchiature a pressione;
- della necessità di fornire al costruttore le informazioni di progresso ed i dati tecnici di progetto per il corretto dimensionamento della apparecchiatura;
- della necessità di ottenere certificato di conformità CE e manuale di uso e manutenzione disponibile per tutte le macchine ed archiviazione nel libretto INAIL della stessa macchina;

Trasporti su strada di merci pericolose (ADR/RID)

sono previste apposite procedure per presidiare:

- la verifica continua del corretto trasporto di merci pericolose;

- la verifica della corretta etichettatura delle merci pericolose secondo i criteri della legislazione europea;

Classification, labelling, packaging delle sostanze (CLP/REACH):

sono previste apposite procedure per presidiare:

- l'aggiornamento della classificazione delle sostanze;
- l'aggiornamento delle schede di sicurezza con la nuova classificazione a nuovo formato;
- l'emissione delle nuove etichettature.

3.41. Gestione strumenti informatici

Riservatezza ed accesso ai dati

Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione e conservazione, in modo tale da risultare accessibili esclusivamente a coloro i quali sono autorizzati a conoscerle, e, in generale, ogni specifico dato deve essere utilizzato esclusivamente da soggetti autorizzati (c.d. principio di riservatezza);

deve essere predisposto un sistema di protezione idoneo ad identificare ed autenticare univocamente gli utenti che intendono ottenere l'accesso ad un sistema elaborativo o trasmissivo;

deve essere realizzato un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichino attraverso la gestione e la verifica dei diritti d'accesso;

l'autenticazione deve essere effettuata prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati;

Integrità dei dati

Deve essere assicurato che ogni dato aziendale corrisponda a quello originariamente immesso nel sistema informatico o che risulti modificato in modo legittimo e che le

informazioni non possano essere manomesse o modificate da soggetti non autorizzati (c.d. principio di integrità);

Disponibilità dei dati

I dati aziendali devono essere sempre reperibili in conformità alle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica (c.d. principio di disponibilità);

Non ripudio

Devono essere applicate misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute (c.d. non ripudio);

Sicurezza informatica, verifiche della vulnerabilità

Devono essere esaustivamente identificate e classificate le risorse e le relative vulnerabilità ovvero le carenze di protezione con riferimento ad una determinata minaccia ed alle seguenti componenti: a) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti); b) *hardware*; c) *software*; d) documentazione; e) dati e informazioni; f) risorse umane;

devono essere compiutamente individuate le minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: a) errori e malfunzionamenti; b) frodi e furti; c) *software* dannoso; d) danneggiamenti fisici; e) sovraccarico del sistema; f) mancato rispetto della legislazione vigente;

in generale, deve essere puntualmente pianificata e periodicamente aggiornata una attività di sicurezza informatica con previsione di un sistema di protezione preventivo;

deve essere predisposta ed attuata una *policy* aziendale che stabilisca le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi ed un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive;

devono essere preventivati i potenziali danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della probabilità di accadimento e delle possibili

contromisure in base ad un'analisi costi-benefici degli investimenti per la predisposizione delle stesse;

deve essere definito un ampio piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;

deve essere documentato ed espressamente accettato il rischio residuo.

Sicurezza informatica, verifiche del corretto uso degli strumenti

Sono effettuate verifiche periodiche a campione sul corretto utilizzo degli strumenti informatici e telematici da parte di soggetti interni ed esterni all'ente;

i controlli effettuati devono essere documentati e le relative risultanze ed evidenze adeguatamente conservate;

Sicurezza informatica, continuità nei servizi informatici

deve essere definito un sistema di emergenza, ovvero devono essere predisposte tutte le procedure tecnico-organizzative per poter affrontare stati di emergenza e garantire la continuità delle operazioni attraverso meccanismi di superamento di situazioni anomale;

sono previsti ed attuati processi e meccanismi che garantiscano la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti di protezione del trasferimento dati, al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi ed alle componenti di *networking*;

Sicurezza informatica - analisi degli eventi informatici

deve essere effettuata una compiuta attività di analisi degli eventi registrati volta a rilevare ed a segnalare eventi anomali che, discostandosi dagli *standard*, soglie e prassi stabilite, possono essere indicativi di eventuali minacce;

Sicurezza informatica - registrazione degli eventi informatici

deve essere predisposto un sistema di tracciamento e monitoraggio degli eventi ed interventi di messa in sicurezza della rete;

Dati - copie di sicurezza

deve essere previsto il salvataggio di copia di *backup* dei dati a frequenze prestabilite;

Dati - verifica della qualità

devono essere istituiti presidi di carattere tecnologico volti alla verifica preventiva ed al monitoraggio continuo sulla qualità dei dati e la performance dei prodotti HW-SW;

Sicurezza fisica - sale server

deve essere assicurata la sicurezza fisica dei siti ove risiedono i sistemi di IT;

deve essere organizzato un sistema di gestione delle credenziali fisiche (*badge*, *pin*, codici di accesso, *token authenticator*, valori biometrici);

Procedure - istruzioni operative - gestione degli account

deve essere regolamentata la creazione, la modifica e la cancellazione di *account* e profili;

è prevista una *password* o codici di valutazione per l'accesso ad ogni terminale che devono essere conosciute esclusivamente dal personale preposto e modificate secondo cadenze prestabilite;

devono essere predisposte procedure formali per l'assegnazione di privilegi speciali (ad es. amministratori di sistema, *super user*);

Inventario Logico-fisico - hardware e software

deve essere predisposto un inventario *dell'hardware* e del *software* in uso agli utenti che deve essere costantemente aggiornato;

è predisposta ed attuata una politica aziendale e di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche ed informazioni);

Sicurezza Informatica - Access Log

deve essere effettuata una *review* periodica dei *log* dagli amministratori di sistema in ambiente di produzione;

deve essere impedito agli operatori di sistema accedere a sistemi o dati diversi da quelli sui quali sono stati chiamati a operare;

deve essere effettuato costantemente il tracciamento degli accessi degli utenti alla rete aziendale;

devono essere effettuati controlli sugli accessi degli applicativi effettuati dagli utenti;

Sicurezza Informatica - Accesso agli ambienti di produzione

deve essere realizzata una corretta separazione tra gli ambienti di sviluppo, *test* e produzione ed in particolare sia previsto il divieto per il personale addetto allo sviluppo di applicativi di avere accesso all'ambiente di produzione;

Sicurezza Informatica - crittografia

è elaborata una politica per l'uso di controlli crittografici per la protezione delle informazioni;

è regolamentato il processo di generazione, distribuzione ed archiviazione delle chiavi;

è regolamentata la gestione delle chiavi a sostegno dell'uso delle tecniche crittografiche da parte della SOCIETÀ;

Sicurezza Informatica - utilizzo della firma digitale

è regolamentata la digitalizzazione con firma digitale dei documenti con riferimento al soggetto responsabile, ai livelli autorizzativi, all'utilizzo dei sistemi di certificazione, all'eventuale utilizzo ed invio dei documenti con modalità di *storage*;

Dati - riutilizzo dei supporti di memorizzazione

sono previsti strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza);

Attività e normativa della Privacy

sono adottate misure minime di sicurezza per il trattamento di dati personali effettuati con strumenti elettronici (sistemi di autenticazione, di autorizzazione, antivirus, *backup*);

sono realizzate attività di sicurezza a supporto della redazione del DPS (analisi dei rischi periodica, almeno annuale) sui trattamenti dei dati personali effettuati ed attività di *audit* volte ad individuare aree di scopertura con relativa pianificazione delle misure di sicurezza da adottare;

Procedure e istruzioni operative - Policy della sicurezza per il personale interno

devono essere definite politiche di sicurezza delle informazioni — gestione ed uso delle *password*, modalità di effettuazione dei *log-in* e *log-out*, uso della posta elettronica, modalità di utilizzo dei supporti rimovibili, l'uso dei sistemi di protezione (*antivirus, antispam, antiphishing, antispay*);

Sicurezza informatica - sensibilizzazione e formazione del personale interno

è attuata una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali;

sono redatti, diffusi e conservati documenti normativi, tecnici, di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte;

Fornitori di servizi/prodotti informatici - gestione dei rapporti

sono periodicamente verificati i rapporti con i fornitori di servizi informatici e siano introdotte, nei relativi contratti, adeguate clausole di tutela;

Fornitori di servizi/prodotti informatici - controlli e servizi outsourcing

sono predisposti con periodicità *IT assessment* in particolare quando si tratti di servizi gestiti in *outsourcing*.