Modello di Organizzazione, Gestione e Controllo

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

Documento approvato

con delibera del Consiglio di Amministrazione del 4 marzo 2024

INDICE

Introduzione

1. PREMESSA

La Società **Eliwell Controls S.r.l.** società di diritto italiano, iscritta al Registro Imprese di Treviso con codice fiscale n° 00987080256 è parte del Gruppo commercialmente noto come Schneider Electric, la cui capogruppo è quotata alla borsa di Parigi. Il Gruppo ha strutturato una politica di compliance e di sostenibilità, nell'ambito della quale è stata elaborata la Carta della Fiducia.
Tale documento definisce i valori etici del Gruppo, ai quali devono attenersi le singole società e tutti i soggetti (interni ed esterni) che operano nell'ambito del Gruppo stesso, nonché i loro dipendenti.

Eliwell opera nel settore elettronico, si occupa della progettazione, sviluppo, realizzazione, produzione e distribuzione di apparecchiature elettroniche, elettromeccaniche, elettriche e dei relativi componenti. In particolare, Eliwell progetta apparecchi per il controllo e la regolazione automatica della temperatura per impianti nel settore HVACR.

L'obiettivo del presente documento consiste nel rendere coerente i principi adottati dal Gruppo di cui la Società è parte all'interno della Carta della Fiducia con le disposizioni riportate dalla normativa italiana sulla responsabilità amministrativa degli enti prevista dal Decreto Legislativo 8 giugno 2001, n. 231 (di seguito "D.Lgs. 231/2001").
Attraverso l'adozione di un Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D. Lgs.231/2001 (di seguito anche "Modello 231", "Modello Organizzativo" o "Modello"), l'intento della Società è quello di:
- adeguarsi alla normativa sulla responsabilità amministrativa degli enti, analizzando i potenziali rischi di condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 e valorizzando e integrando i relativi presidi di controllo, atti a prevenire la realizzazione di tali condotte;
- promuovere una cultura aziendale orientata all'etica, alla correttezza e alla trasparenza delle attività;
- determinare, in tutti coloro che operano per conto della Società nell'ambito delle attività sensibili, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in conseguenze disciplinari e/o contrattuali oltre che nelle sanzioni penali e amministrative comminabili nei loro stessi confronti ai sensi della normativa di riferimento;
- ribadire che tali forme di comportamento illecito sono fortemente condannate all'interno della Società, in quanto le stesse sono contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la Società intende attenersi nell'esercizio dell'attività aziendale;
- consentire alla Società, grazie a un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione di reati e sanzionare i comportamenti contrari alla legge e alle regole aziendali.

Il Modello Organizzativo adottato dalla Società rappresenta un insieme coerente di principi, procedure e disposizioni che incidono sul funzionamento interno della Società e sulle modalità con le quali la stessa si rapporta con l'esterno.
Il presente documento è stato adottato dalla Società con delibera del Consiglio di Amministrazione in data 4 marzo 2024**.**

2. STRUTTURA DEL DOCUMENTO

La struttura del Modello si compone di:
- *Parte Generale* che descrive i contenuti del Decreto, la funzione e i principi generali di funzionamento del Modello, nonché i meccanismi di concreta attuazione dello stesso;
- *Parte Speciale*, che descrive, per ciascuna delle attività e processi soggetti a potenziale "rischio 231", le fattispecie di reato rilevanti, i principi comportamentali da rispettare, nonché i presidi di controllo da porre in essere per la prevenzione dei rischi.

Il Modello si compone inoltre dei seguenti Allegati:

- *Chart of Approval*, il documento che contiene tutte deleghe e i processi per l'approvazione delle decisioni dell'organizzazione della Società, allo scopo di mantenere dei controlli adeguati ed un approccio coerente attraverso l'organizzazione globale (Allegato 1);
- *Carta della Fiducia di Schneider Electric o Trust Charter* (di seguito definito anche "Codice di Condotta" o "Codice"), che definisce i valori ed i principi etici generali a cui gli organi societari e i suoi componenti, nonché i dipendenti, i collaboratori ed i consulenti della Società, si devono ispirare nella conduzione delle proprie attività, al fine di impedire il verificarsi di comportamenti illeciti o non allineati agli standard aziendali. L'importanza che la Carta della Fiducia riveste per la Società e la sua efficacia cogente sono comprovate dal richiamo alle sanzioni previste in caso di violazione del Codice stesso. (Allegato 2);
- "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 (Allegato 3);
- "*Reati tributari e attività connesse*" (Allegato 4);
- "*Report flussi informativi ODV*" (Allegato 5).

Parte Generale

1. IL QUADRO NORMATIVO DI RIFERIMENTO

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

Il D.Lgs. 231/2001, emanato in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 300, disciplina la "*responsabilità degli enti per gli illeciti amministrativi dipendenti da reato".* Il D.Lgs. 231/2001 trova la sua genesi in alcune convenzioni internazionali e comunitarie ratificate dall'Italia, che impongono di prevedere forme di responsabilità degli enti collettivi per talune fattispecie di reato.
Secondo la disciplina introdotta dal D.Lgs. 231/2001 un ente può essere ritenuto "responsabile" per alcuni reati commessi o tentati, nell'interesse o a vantaggio della società stessa, da:
- soggetti apicali, ossia coloro i quali rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché coloro che esercitano, anche di fatto, la gestione e il controllo delle stesse;
- soggetti sottoposti alla direzione o alla vigilanza di soggetti apicali.

Per quanto attiene alla nozione di "*interesse*", lo stesso si concretizza ogniqualvolta la condotta illecita sia posta in essere con l'esclusivo intento di conseguire un beneficio alla società, indipendentemente dalla circostanza che tale obiettivo sia stato conseguito.
Del pari, la responsabilità incombe sulla società ogniqualvolta l'autore dell'illecito, pur non avendo agito al fine di beneficiare l'ente, abbia comunque fatto conseguire un "vantaggio", di tipo economico o meno, alla persona giuridica.
Infine, è opportuno porre in evidenza il fatto che la responsabilità amministrativa delle società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e si affianca a quest'ultima.

1.2. Le sanzioni amministrative

Nell'eventualità in cui sussista la responsabilità ai sensi del D.Lgs. 231/2001, in conseguenza della commissione o tentata commissione dei reati presupposto, la normativa prevede la possibilità di comminare a carico della Società le seguenti sanzioni:

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

1.3. La condizione esimente dei modelli di organizzazione, gestione e controllo

Aspetto caratteristico del D.Lgs. 231/2001 è l'attribuzione di un valore "esimente" ai modelli di organizzazione, gestione e controllo adottati dagli enti.
Perché operi il carattere esimente del Modello, l'ente è tenuto a **provare** che:

- l'organo dirigente ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire i reati presupposto previsti dal Decreto;

- il compito di vigilare sul funzionamento e l'osservanza del Modello, e di curare il suo aggiornamento, è stato affidato ad un "organismo" dotato di autonomi poteri di iniziativa e controllo, l'organismo di vigilanza;
- il reato rilevante ai sensi del Decreto è stato commesso eludendo fraudolentemente il Modello Organizzativo correttamente predisposto dalla società;
- il reato è stato commesso senza che vi fosse omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Nel caso, invece, di un reato commesso da parte dei soggetti sottoposti all'altrui direzione o vigilanza, l'ente risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza l'ente è tenuto.
La responsabilità amministrativa della società è in ogni caso esclusa, per espressa previsione legislativa (art. 5, comma 2, D.Lgs. 231/2001), se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi.

Il presente Modello è stato redatto tenendo conto delle indicazioni espresse dalle linee guida elaborate da Confindustria e approvate dal Ministero della Giustizia.

2. L'ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

2.1. La redazione del Modello di organizzazione, gestione e controllo

Il processo di redazione della prima versione del Modello si è sviluppato attraverso le fasi progettuali di seguito descritte:

1. Individuazione delle attività e dei processi nel cui ambito potrebbero potenzialmente configurarsi le condizioni, le occasioni e/o i mezzi per la commissione dei reati previsti dal Decreto (c.d. ***"attività sensibili"***), nonché delle strutture aziendali coinvolte nello svolgimento di tali attività.

2. Analisi delle attività e dei processi sensibili e rilevazione dei meccanismi organizzativi e di controllo in essere o da adeguare. Il sistema di controllo è stato esaminato prendendo in considerazione i seguenti presidi *standard* di prevenzione presenti a livello di Gruppo:
   - esistenza di procedure formalizzate;
   - tracciabilità e verificabilità *ex post* delle transazioni tramite adeguati supporti documentali/informativi;
   - esistenza di un sistema di poteri e di livelli autorizzativi formalizzati e coerenti con le responsabilità organizzative assegnate;
   - rispetto del principio di segregazione dei compiti;

3. Al termine delle attività sopra descritte, lo sviluppo del Modello Organizzativo è stato articolato secondo le indicazioni contenute nelle Linee Guida emanate da Confindustria attraverso:

   a) la sua approvazione da parte del Consiglio di Amministrazione;
   b) la nomina dell'Organismo di Vigilanza preposto alla verifica di effettiva attuazione e osservanza del Modello;
   c) la definizione di un sistema disciplinare avverso alle eventuali violazioni del Modello;
   d) la diffusione dei contenuti del Modello attraverso attività di formazione e informazione dei Destinatari.

Successivamente a tale attività di redazione, il Modello viene costantemente aggiornato e adattato dai responsabili delle aree, dall'OdV, dall'Internal Audit e dall'Internal Control che eseguono una costante opera di revisione dei processi che sono stati identificati quali a rischio 231, di formazione dei soggetti incaricati di operare in tali processi e dei destinatari del modello tramite attività di Risk Assesment quali la mappatura di eventuali nuovi processi nel cui ambito potrebbero potenzialmente configurarsi le condizioni, le occasioni e/o i mezzi per la commissione dei reati previsti dal Decreto, l'adozione e la revisione delle politiche aziendali

sia da parte della Società che da parte del Gruppo di cui fa parte, nonché delle campagne annuali dei Kics (Key Internal Controls) come meglio definiti nel proseguo del Modello.

Tenendo conto delle attività continue di Risk Assesment eseguita dalla Società, si è ritenuto di incentrare maggiormente l'attenzione sui rischi di commissione dei seguenti reati:
- **reati commessi nei rapporti con la Pubblica Amministrazione** (artt. 24 e 25);
- **delitti informatici e trattamento illecito di dati** (art. 24-*bis*);
- **delitti di criminalità organizzata** (art. 24-*ter*);
- **falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** (art. 25-*bis*);
- **delitti contro l'industria e il commercio** (art. 25-*bis.1*);
- **reati societari** (art. 25-*ter*) ivi inclusa la corruzione tra privati ex art. 2365 codice civile;
- **reati di omicidio colposo o lesioni gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** (art. 25-*septies*);
- **ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (art. 25- *octies*);
- **delitti in materia di violazione del diritto d'autore** (art. 25-*novies*)[1];
- **induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 25-*decies*);
- **reati ambientali** (art. 25-*undecies*);
- **impiego di cittadini di Paesi terzi il cui soggiorno è irregolare** (art. 25-*duodecies*);
- **reati tributari** (art. 25-*quinquiesdecies*).

Relativamente agli altri reati e illeciti previsti dal Decreto, si è ritenuto che le specifiche attività svolte dalla Società non presentino profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa. Nondimeno, si ritiene che la Carta della Fiducia definisca precise norme comportamentali idonee anche alla prevenzione di questi eventuali altri reati.

Le "**attività sensibili**" individuate ai sensi del D.Lgs. 231/2001 sono le seguenti:

Attività sensibili	Parte Speciale
1. Gestione delle relazioni con la Pubblica Amministrazione e gli Enti certificatori: a. gestione dei rapporti con la Pubblica Amministrazione in occasione di visite ispettive; b. gestione dei rapporti con la Pubblica Amministrazione per l'ottenimento di autorizzazioni e licenze; c. gestione dei rapporti con la Pubblica Amministrazione per la gestione ed esecuzione di adempimenti; d. gestione dei rapporti con la Pubblica Amministrazione per l'ottenimento di finanziamenti/contributi pubblici e. gestione dei rapporti con gli enti certificatori; f. gestione del contenzioso.	Parte Speciale A

[1] vedi L. 93/2023 recante "*Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica*". La Legge, introducendo la lettera h-bis) al comma 1 dell'art 171-ter, L. 633/41, estende le fattispecie rilevanti ai sensi dell'art 25-novies del dlgs. 231/2001.

2. Gestione delle attività amministrative, contabili e societarie, in particolare: a. gestione della contabilità e predisposizione del bilancio di esercizio; b. gestione degli affari fiscali; c. gestione dei rapporti con gli organi di controllo (collegio sindacale e società di revisione); d. gestione delle operazioni societarie straordinarie.	Parte Speciale B
3. Gestione delle vendite di beni e servizi: a. gestione delle vendite infragruppo; b. gestione delle vendite extra gruppo;	Parte Speciale C
4. Gestione del personale: a. selezione, assunzione del personale e percorsi di carriera; b. gestione amministrativa del personale; c. gestione dei rapporti con le rappresentanze sindacali.	Parte Speciale D
5. Acquisto di beni e servizi: a. gestione degli acquisti diretti; b. gestione degli acquisti indiretti.	Parte Speciale E
6. Gestione dello sviluppo prodotto.	Parte Speciale F
7. Gestione degli omaggi, liberalità, sponsorizzazioni.	Parte Speciale G
8. Gestione della tesoreria e dei rimborsi spese: a. gestione della cassa e dei rimborsi spese; b. gestione delle operazioni bancarie con gli istituti di credito	Parte Speciale H
9. Gestione dei sistemi informativi.	Parte Speciale I
10. Gestione degli adempimenti in materia di salute e sicurezza sul lavoro e ambientale: a. gestione degli adempimenti in materia di salute e sicurezza sul lavoro; b. gestione degli adempimenti in materia ambientale.	Parte Speciale L
11. Gestione dei rapporti con gli agenti	Parte Speciale M

Nello svolgimento delle singole attività sensibili sopra elencate, i soggetti via via coinvolti devono inderogabilmente:
- rispettare il principio della **segregazione dei compiti** tra chi esegue, chi controlla e chi autorizza;
- rispettare la **normativa aziendale** (es. procedure e policy aziendali);
- rispettare il **sistema dei poteri** in vigore, in linea con le responsabilità organizzative assegnate;
- garantire la **tracciabilità** e verificabilità *ex post* volta ad assicurare l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati;
- rispettare i **principi di comportamento e presidi di controllo specifici**, previsti dalle Parti Speciali del Modello e dalla Carta della Fiducia della Società.

3. L'ORGANISMO DI VIGILANZA

3.1. L'Organismo di Vigilanza

L'Organismo di Vigilanza, un organismo dotato di autonomi poteri di iniziativa e controllo, ha il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

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

- autonomia e indipendenza: rispetto ad ogni forma d'interferenza o di condizionamento da parte di qualunque esponente della società e, in particolare, dell'organo amministrativo;
- professionalità: capacità tecniche dell'OdV di assolvere alle proprie funzioni rispetto alla vigilanza del Modello, nonché nelle necessarie qualità per garantire la dinamicità del Modello medesimo, attraverso proposte di aggiornamento da indirizzare al Vertice aziendale;
- continuità di azione: verifica continua sul rispetto del Modello, sull'effettività e sull'efficacia dello stesso, promuovendone il continuo aggiornamento e rappresentando un referente costante per ogni soggetto che presti attività lavorativa per la Società.

Il D.Lgs. 231/2001 non fornisce indicazioni specifiche circa la composizione dell'Organismo di Vigilanza.
In assenza di tali indicazioni, la Società ha optato per una soluzione che, tenuto conto delle finalità perseguite dalla legge e dagli indirizzi ricavabili dalla giurisprudenza pubblicata, tale organismo sia in grado di assicurare, in relazione alle proprie dimensioni e alla propria complessità organizzativa, l'effettività dei controlli per il quale è stato preposto.
Conseguentemente, la Società ha deciso per una composizione collegiale del proprio Organismo di Vigilanza, composto da tre membri di cui due interni e uno esterno, la cui nomina deve essere deliberata dal Consiglio di Amministrazione.

3.2. Principi generali in tema di istituzione, nomina e sostituzione dell'Organismo di Vigilanza

L'Organismo di Vigilanza della Società è istituito con delibera del Consiglio di Amministrazione e resta in carica per un periodo di tre anni, è possibile riconfermare l'OdV al termine del suo mandato.
Al termine del mandato, nel caso in cui l'Odv non venga riconfermato, esso continua a svolgere *ad interim* le proprie funzioni fino a nuova nomina dell'Organismo, che deve essere effettuata con prima delibera utile del Consiglio di Amministrazione.
Se, nel corso della carica, l'Organismo di Vigilanza, oppure un suo componente, cessa il proprio incarico, il Consiglio di Amministrazione provvede alla sostituzione con propria delibera.
Inoltre, il compenso dell'Organismo di Vigilanza è stabilito dal Consiglio di Amministrazione.
La nomina dei componenti dell'Organismo di Vigilanza è condizionata alla presenza di alcuni requisiti soggettivi di eleggibilità. In particolare, all'atto del conferimento dell'incarico, i soggetti designati a ricoprire la carica di componente dell'Organismo di Vigilanza devono rilasciare una dichiarazione nella quale attestino l'assenza di motivi di ineleggibilità, quali a titolo esemplificativo:

- conflitti di interesse, anche potenziali, con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'Organismo di Vigilanza, quali a titolo meramente esemplificativo:
    - intrattenere significativi rapporti d'affari con la Società, salvo il rapporto di lavoro subordinato;
    - intrattenere significativi rapporti d'affari con il Presidente o altro soggetto munito di poteri;
    - avere rapporti con o far parte del nucleo familiare del Presidente o di altro soggetto munito di poteri, dovendosi intendere per nucleo familiare quello costituito dal coniuge, non separato legalmente, dai parenti ed affini entro il terzo grado;
    - risultare titolari direttamente (o indirettamente) di partecipazioni nel capitale della Società di entità tale da permettere di esercitare una notevole influenza sulla Società;
- funzioni di amministrazione di imprese sottoposte a fallimento, liquidazione coatta amministrativa o altre procedure concorsuali nei tre esercizi precedenti alla nomina quale membro dell'Organismo di

Vigilanza, ovvero all'instaurazione del rapporto di consulenza / collaborazione con lo stesso Organismo;

- stato di interdizione temporanea o di sospensione dai pubblici uffici, ovvero dagli uffici direttivi delle persone giuridiche e delle imprese;
- esistenza di una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile;
- sentenza di condanna, in Italia o all'estero, ancorché non ancora passata in giudicato e anche se con pena condizionalmente sospesa, o con sentenza di applicazione della pena su richiesta delle parti ai sensi dell'art. 444 c.p.p. (cosiddetto "patteggiamento"), salvi gli effetti della riabilitazione, per i delitti richiamati dal D.Lgs. 231/2001 o delitti comunque incidenti sulla moralità professionale;
- sentenza di condanna, ancorché non ancora passata in giudicato e anche se con pena condizionalmente sospesa, o con sentenza di applicazione della pena su richiesta delle parti ai sensi dell'art. 444 c.p.p. (cosiddetto "patteggiamento"), salvi gli effetti della riabilitazione:

  - a pena detentiva per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267;
  - a pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
  - a pena detentiva per un tempo non inferiore ad un anno per un reato contro la Pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;
  - per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore ad un anno;
  - per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato dal D.Lgs. 61/2002.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi a carico di un soggetto nominato nel corso del mandato, questi decadrà automaticamente dalla carica.
Nel caso di presenza di dipendenti della Società tra i membri dell'Organismo di Vigilanza, la cessazione del relativo rapporto di lavoro comporta anche la decadenza da tale carica.
L'Organismo di Vigilanza potrà giovarsi, sotto la sua diretta sorveglianza e responsabilità, nello svolgimento dei compiti affidatigli, della collaborazione di tutte le strutture della Società, ovvero di consulenti esterni, avvalendosi delle rispettive competenze e professionalità.
A tal fine, il Consiglio di Amministrazione assegna un *budget* di spesa all'Organismo di Vigilanza, tenendo conto delle richieste di quest'ultimo: l'assegnazione di un *budget* di spesa permette all'Organismo di Vigilanza di operare in autonomia e con gli strumenti opportuni per un efficace espletamento dei compiti assegnatigli dal presente Modello, secondo quanto previsto dal D.Lgs. 231/2001. Tuttavia, in caso di necessità, l'Organismo di Vigilanza potrà richiedere al Consiglio di Amministrazione di disporre anche di cifre superiori, dandone adeguata rendicontazione successiva.

Al fine di garantire la necessaria stabilità all'Organismo di Vigilanza, la revoca dei propri poteri e l'attribuzione degli stessi ad altro soggetto può avvenire soltanto per giusta causa, anche legata a interventi di ristrutturazione organizzativa della Società, mediante un'apposita delibera del Consiglio di Amministrazione.
Per "giusta causa" ai fini della revoca dei poteri connessi con l'incarico di un componente dell'Organismo di Vigilanza potrà intendersi, a titolo meramente esemplificativo:
- una sentenza di condanna definitiva della Società ai sensi del Decreto o una sentenza di patteggiamento passata in giudicato, ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;

- una sentenza di condanna o di patteggiamento emessa nei confronti dell'Organismo di Vigilanza per aver commesso uno dei reati o illeciti amministrativi previsti dal Decreto (o reati/illeciti amministrativi della stessa indole);
- la violazione degli obblighi di riservatezza a cui l'OdV è tenuto;
- la mancata partecipazione a più di due riunioni consecutive senza giustificato motivo;
- una grave negligenza nell'adempimento dei propri compiti quale, ad esempio, l'omessa redazione della relazione informativa annuale al Consiglio di Amministrazione sull'attività svolta;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'Organismo di Vigilanza.

In casi di particolare gravità, il Consiglio di Amministrazione potrà comunque disporre, sentito il parere del Collegio Sindacale, la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un OdV *ad interim*.

3.3. Funzioni e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono conferiti i poteri di iniziativa e di controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del D.Lgs. 231/2001.
In particolare, l'OdV ha il compito di vigilare:
- sulla reale adeguatezza ed effettività del Modello rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il D.Lgs. 231/2001, tenendo conto anche delle dimensioni e della complessità organizzativa e operativa della Società;
- sulla permanenza nel tempo dei requisiti di adeguatezza ed effettività del Modello;
- sull'osservanza delle prescrizioni del Modello da parte dei Destinatari, rilevando eventuali violazioni e proponendo i relativi interventi correttivi e/o sanzionatori agli organi aziendali competenti;
- sull'aggiornamento del Modello nel caso in cui si riscontrassero esigenze di adeguamento in relazione alle mutate condizioni aziendali o normative, proponendo le eventuali azioni di adeguamento agli organi aziendali competenti e verificandone l'implementazione.

Per l'espletamento e l'esercizio delle proprie funzioni, all'OdV sono attribuite le seguenti facoltà e poteri:
- accedere a tutte le strutture della Società e a tutta la documentazione aziendale rilevante ai fini di verificare l'adeguatezza e il rispetto del Modello;
- effettuare verifiche a campione mirate su specifiche attività/operazioni a rischio e sul rispetto dei presidi di controllo e di comportamento adottati e richiamati dal Modello e dalle procedure aziendali;
- promuovere l'aggiornamento della mappatura dei rischi in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal D.Lgs. 231/2001;
- coordinarsi con i Responsabili aziendali di riferimento per valutare l'adeguatezza del corpo normativo interno adottato e definire eventuali proposte di adeguamento e miglioramento (regole interne, procedure, modalità operative e di controllo) verificandone, successivamente, l'attuazione;
- monitorare le iniziative di informazione e formazione finalizzate alla diffusione della conoscenza e della comprensione del Modello in ambito aziendale;
- richiedere ai Responsabili aziendali, in particolare a coloro che operano in aree aziendali a potenziale rischio-reato, le informazioni ritenute rilevanti, al fine di verificare l'adeguatezza e l'effettività del Modello;
- raccogliere eventuali segnalazioni provenienti da qualunque Destinatario del Modello in merito a: i) eventuali criticità delle misure previste dal Modello; ii) violazioni dello stesso; iii) qualsiasi situazione che possa esporre la Società a rischio di reato;
- segnalare periodicamente ai Responsabili interessati eventuali violazioni di presidi di controllo richiamati dal Modello e/o dalle procedure aziendali o le carenze rilevate in occasione delle verifiche svolte, affinché questi possano adottare i necessari interventi di adeguamento coinvolgendo, ove necessario, il Consiglio di Amministrazione;

- vigilare sull'applicazione coerente delle sanzioni previste dalle normative interne nei casi di violazione del Modello, fermo restando la competenza dell'organo dirigente per l'applicazione dei provvedimenti sanzionatori;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i Destinatari del Modello.

Oltre a ciò, l'Organismo di Vigilanza è tenuto al vincolo di riservatezza rispetto a tutte le informazioni di cui viene a conoscenza a causa dello svolgimento del proprio incarico: per questa motivazione, ogni informazione in suo possesso deve essere trattata in conformità con la vigente legislazione in materia di protezione dei dati personali. Inoltre, la divulgazione di tali informazioni potrà essere effettuata solo ai soggetti e con le modalità previste dal presente Modello.

3.4. Obblighi di informazione nei confronti dell'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere tempestivamente informato dai Destinatari del Modello, mediante apposite segnalazioni, in merito ad atti, comportamenti od eventi che possano determinare una violazione del Modello o che, più in generale, siano rilevanti ai fini del D.Lgs. 231/2001.
In particolare, tutti i Destinatari del presente Modello hanno l'obbligo di segnalare tempestivamente all'OdV le seguenti informazioni (c.d. "segnalazioni"):
- la commissione, il tentativo di commissione o il ragionevole pericolo di commissione dei reati previsti dal Decreto;
- eventuali presunte violazioni delle modalità comportamentali e operative definite nella Carta della Fiducia, nel Modello e/o nel corpo normativo e procedurale aziendale, di cui siano direttamente o indirettamente venuti a conoscenza;
- di qualsiasi atto, fatto, evento od omissione rilevato od osservato nell'esercizio delle responsabilità e dei compiti assegnati, con profilo di criticità rispetto alle norme del Decreto;
- osservazioni sull'adeguatezza del sistema di controllo;
- qualsiasi eccezione comportamentale o qualsiasi evento inusuale indicando le ragioni delle difformità e dando atto del diverso processo seguito.

Ai sensi dell'art. 6, comma 2-*bis*, D.Lgs. 231/2001, il Modello deve prevedere appositi canali che consentano di segnalare eventuali condotte illecite rilevanti ai sensi del Decreto stesso, ovvero violazioni del Modello di cui i Destinatari siano venuti a conoscenza in ragione delle funzioni svolte.
Sotto questo profilo, tutti i Destinatari possono servirsi degli indirizzi (anche di posta elettronica) che vengono messi a disposizione dalla Società, al fine di inviare le segnalazioni in forma scritta, e non anonima, tramite:
- lettera in busta chiusa, da spedire o consegnare presso l'indirizzo della Società;
- o indirizzo di posta elettronica dedicato.
L'accesso a tale indirizzo, e l'utilizzo dello stesso, sono consentiti ai soli componenti dell'Organismo di Vigilanza, in quanto dotati di apposite credenziali di accesso loro esclusivamente riservate.
L'Organismo di Vigilanza valuta le segnalazioni ricevute ed i casi in cui è necessario che si attivi per ulteriori verifiche ed eventuali azioni: per tale motivazione, la segnalazione di condotte integranti taluno dei reati presupposto indicati nel D.Lgs. 231/2001, e/o di violazioni del Modello, deve essere quanto più completa e circostanziata possibile, preso atto che l'OdV non ha l'obbligo di verificare in maniera puntuale e sistematica tutti i fenomeni rappresentati e non è, pertanto, tenuto ad intervenire a fronte di qualsivoglia segnalazione, essendo rimessa alla discrezionalità e responsabilità dello stesso OdV la valutazione degli specifici casi nei quali sia opportuno attivare verifiche e/o approfondimenti di maggiore dettaglio.
Le segnalazioni rivelatesi fondate costituiscono elemento positivo di valutazione del segnalante nei processi interni di verifica dei risultati conseguiti e delle potenzialità espresse dai quali dipendono l'attribuzione dei ruoli e delle responsabilità all'interno della Società e gli avanzamenti di carriera.

Per contro, il mancato rispetto delle tutele assicurate agli autori delle segnalazioni e, rispettivamente, la presentazione con dolo o colpa grave di segnalazioni che si rivelino false costituiscono illecito disciplinare sanzionabile in conformità a quanto in proposito previsto nel successivo capitolo 5.
Oltre alle segnalazioni di cui sopra, i Responsabili aziendali di volta in volta interessati, con l'intervento del legale rappresentante, devono obbligatoriamente trasmettere all'Organismo di Vigilanza le informazioni concernenti (c.d. "informazioni generali"):

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini o di procedimenti penali, anche nei confronti di ignoti, relativi a fatti d'interesse e/o che possano coinvolgere la Società (relativi al D.Lgs. 231/2001 e non);
- i provvedimenti e/o notizie aventi ad oggetto l'esistenza di procedimenti amministrativi o civili di rilievo relativi a richieste o iniziative di Autorità pubbliche;
- ogni atto o citazione a testimoniare che veda coinvolti soggetti della Società o che collaborano con essa;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento penali o civili nei loro confronti (non solo in relazione ai reati di cui al D.Lgs. 231/2001);
- le informazioni relative alle eventuali visite ispettive condotte da funzionari della Pubblica Amministrazione e comunicati da tutte le strutture aziendali;
- le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le comunicazioni inerenti a modifiche organizzative e societarie intervenute nel proprio ambito di attività;
- anomalie o criticità riscontrate dai Responsabili nello svolgimento delle attività sensibili per l'applicazione del D.Lgs. 231/2001.

L'Organismo di Vigilanza predispone e, ove necessario, aggiorna un "Documento Flussi Informativi" nel quale sono sinteticamente e complessivamente individuate le diverse comunicazioni al medesimo dovute e la relativa periodicità (ad esempio semestrale).
Al fine di garantire la miglior efficienza dei flussi informativi, tale documento viene prima consegnato ai Responsabili della gestione, in modo da fornire loro una rappresentazione chiara e puntuale degli adempimenti loro richiesti, e successivamente, con l'intervento del legale rappresentante della società, indirizzato all'OdV per il suo esame.
Le informazioni generali e le informazioni specifiche devono essere inviate all'OdV in forma scritta utilizzando l'indirizzo di posta elettronica dedicato.
Ogni informazione o segnalazione prevista è conservata dall'Organismo di Vigilanza in un apposito archivio riservato (informatico o cartaceo).

3.4.1. Il Whistleblowing

Nel paragrafo precedente si è fatto riferimento all'obbligo, riconosciuto in capo ai Destinatari del Modello 231, di informare l'OdV di alcuni comportamenti scorretti.
In questo caso, è opportuno citare il D.Lgs. 24/2023, recante "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*", il quale ha recepito nel nostro ordinamento la normativa comunitaria in ambito di *whistleblowing*.
Il *whistleblowing*, disciplina la condotta di quelle persone che segnalano irregolarità, o addirittura illeciti penali, all'interno del proprio ambito lavorativo.
Centrali in tale ottica sono:

1. da un lato, il flusso informativo verso l'OdV (ed eventualmente non solo a quest'ultimo): quindi, la comunicazione, da parte di un soggetto dell'organizzazione aziendale, di azioni illegali, immorali o illegittime poste in essere di cui viene a conoscenza;
2. dall'altro lato, la relativa tutela, che si concretizza nell'interesse del *whistleblower* di ricevere adeguata protezione sia da parte dell'ordinamento sia da parte della Società.

Dunque, si evince che il fenomeno del *whistleblowing* è strettamente collegato con il tema dell'informazione e della sua gestione in azienda attraverso appositi canali e flussi informativi e, inoltre, trova collocazione anche nell'ambito di un'organizzazione aziendale che possa assicurare comportamenti conformi ad un'etica condivisa in ambito lavorativo, definendo le regole che ne presidiano il perseguimento.
In perfetta sintonia con i principi etici ai quali la Società intende ispirarsi nella gestione dell'impresa, è stata adottata una precisa politica dal Gruppo al quale la Società appartiene, la Politica del Gruppo sulla segnalazione di irregolarità. Tale politica assicura la più assoluta riservatezza in merito all'identità degli autori delle segnalazioni, fatti salvi esclusivamente gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in mala fede: in questo caso, tale politica, tutela i segnalanti (cd. *whistleblower)* contro qualsiasi forma di ritorsione, discriminazione o penalizzazione di sorta per motivi direttamente od indirettamente riconducibili alla presentazione della segnalazione stessa.

Il canale di segnalazione adottato dal Gruppo, la Trust Line, utilizzato anche dalla Società, rispetta i principi e le garanzie previste all'interno della normativa nazionale e comunitaria in materia di *whistleblowing*.
Sussistono ulteriori canali di segnalazione messi a disposizione dalla Società e sono riepilogati nel paragrafo 8 della Parte Generale del Modello.

3.5. Reporting dell'Organismo di Vigilanza verso gli organi societari

Al fine di garantire la piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza è tenuto a riferire direttamente al Consiglio di Amministrazione della Società, trasmettendo allo stesso, e per conoscenza al Collegio Sindacale:

- con cadenza annuale**,** una relazione informativa relativa all'attività svolta;
- al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione per quanto di competenza.

L'Organismo di Vigilanza ha comunque la facoltà di richiedere la propria audizione al Consiglio di Amministrazione o al Collegio Sindacale, qualora ne ravvisi la necessità.
Allo stesso modo, il Consiglio di Amministrazione e il Collegio Sindacale hanno facoltà di convocare l'Organismo di Vigilanza qualora lo ritengano opportuno.
Nell'ambito del *reporting* annuale vengono affrontati i seguenti aspetti:

- controlli e verifiche svolti dall'Organismo di Vigilanza ed esito degli stessi;
- eventuali criticità emerse;
- stato di avanzamento di eventuali interventi correttivi e migliorativi del Modello;
- eventuali innovazioni legislative o modifiche organizzative che richiedano aggiornamenti nell'identificazione dei rischi o variazioni del Modello;
- eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito di violazioni del Modello;
- eventuali segnalazioni ricevute da soggetti interni ed esterni nel corso del periodo in ordine a presunte violazioni al Modello o alla Carta della Fiducia;
- il piano di attività previsto per l'anno successivo;
- altre informazioni ritenute significative.

L'OdV redige apposito verbale degli incontri con gli organi societari e cura l'archiviazione della eventuale relativa documentazione.

4. DIFFUSIONE DEL MODELLO

4.1. Destinatari

Le regole e le disposizioni contenute nel Modello e nei suoi Allegati si applicano e devono essere rispettate da coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo della Società, dai dipendenti, nonché da coloro i quali, pur non appartenendo alla Società, operano su mandato della medesima. Dunque, sono Destinatari del presente Modello:
- gli organi sociali (compresi i membri del Consiglio di Amministrazione e del Collegio Sindacale) nonché i titolari di qualifiche formali (di direzione, gestione e controllo della Società o di una sua unità organizzativa) riconducibili alla definizione di "soggetti apicali" contenuta all'art. 6 del D.Lgs. 231/2001;
- i soggetti che esercitano tali funzioni (di direzione, gestione e controllo) anche solo di fatto;
- tutto il personale della Società, in forza di qualsiasi tipo di rapporto contrattuale;
- chiunque agisca in nome e per conto della Società sotto la sua direzione e vigilanza.

Con riferimento, invece, ai collaboratori esterni, consulenti, intermediari, fornitori, partner d'affari e altre controparti contrattuali in genere, la Società richiede il rispetto delle prescrizioni dettate dal Decreto e dei principi etici adottati dalla Società, tramite la sottoscrizione di specifiche clausole contrattuali.

4.1.1. Formazione ed informazione

L'adeguata formazione e la costante informazione dei Destinatari in ordine ai principi ed alle prescrizioni contenute nel Modello e nei suoi Allegati rappresentano fattori di grande importanza per la corretta ed efficace attuazione dello stesso.
Tutti i Destinatari del Modello sono tenuti ad avere piena conoscenza degli obiettivi di correttezza e di trasparenza che si intendono perseguire con il Modello e delle modalità attraverso le quali la Società ha inteso perseguirli, approntando un adeguato sistema di procedure e controlli.
La comunicazione e la formazione sui principi e i contenuti del Modello sono garantite dall'Organismo di Vigilanza che identifica, di concerto con la Società, la migliore modalità di fruizione di tali servizi.
L'attività di comunicazione e formazione (ivi compreso il piano di formazione) è supervisionata dall'Organismo di Vigilanza che potrà proporre eventuali integrazioni ritenute utili.

4.2. La comunicazione del Modello 231

Al momento dell'assunzione, le Risorse Umane promuovono la conoscenza del Modello e della Carta della Fiducia. In particolare, ai nuovi assunti deve essere consegnata un'informativa con riferimento all'applicazione della normativa di cui al D.Lgs. 231/2001 nell'ambito della Società e del Gruppo.
In questo modo, i soggetti Destinatari si impegnano, nello svolgimento dei compiti afferenti alle aree rilevanti ai fini del Decreto e in ogni altra attività che possa realizzarsi nell'interesse o a vantaggio della Società, al rispetto dei principi, regole e procedure in esso contenuti.
Inoltre, ogni dipendente sarà tenuto a dichiarare, mediante specifica clausola inserita nel contratto di assunzione, di essere a conoscenza e rispettare la normativa di cui al D.Lgs. 231/2001 e di accettare espressamente i contenuti della Carta della Fiducia e del Modello adottato dalla Società.

4.3. Attività di formazione per i dipendenti

Al fine di agevolare la comprensione della normativa di cui al Decreto e del Modello, i dipendenti, con modalità diversificate secondo il loro ruolo e grado di coinvolgimento nelle attività individuate come sensibili ai sensi del D.Lgs. 231/2001 all'interno del Modello, sono tenuti a partecipare alle specifiche attività formative promosse dalla Società attraverso *training* e corsi in modalità e-learning.

La Società garantisce l'organizzazione delle attività formative specifiche rivolte ai soggetti apicali e agli altri dipendenti coinvolti nelle attività sensibili, con frequenza e contenuti idonei a garantire la conoscenza del Decreto e la diffusione del Modello e della Carta della Fiducia.
La partecipazione ai programmi di formazione è obbligatoria rispetto a tutti i destinatari della formazione stessa e deve essere documentata. Inoltre, sono previsti controlli di frequenza e verifiche dell'apprendimento.
Per quanto concerne, invece, i partner d'affari, i consulenti e collaboratori esterni, essi vengono informati, all'atto dell'avvio della collaborazione, dell'adozione, da parte della Società, del Modello e della Carta della Fiducia e dell'esigenza che il loro comportamento sia conforme alle prescrizioni di cui al D.Lgs. 231/2001.

5. SISTEMA DISCIPLINARE E SANZIONATORIO

5.1. Funzione del sistema disciplinare

La definizione di un adeguato sistema disciplinare, con sanzioni proporzionate alla gravità della violazione delle regole di cui al presente Modello da parte dei Destinatari, costituisce un presupposto essenziale per l'efficacia del Modello stesso.
Le sanzioni previste saranno applicate a ogni violazione delle disposizioni contenute nel Modello a prescindere dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'Autorità Giudiziaria, nel caso in cui il comportamento da censurare integri gli estremi di una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.
In ogni caso, la sanzione prescinde dalla commissione del reato e si attesta come reazione della Società al mancato rispetto di procedure o regole comportamentali richiamate dal Modello.

5.2. Misure nei confronti di lavoratori dipendenti non dirigenti

Le violazioni delle disposizioni e delle regole comportamentali previste dal Modello, e dai suoi Allegati, da parte dei dipendenti della Società costituiscono inadempimento contrattuale.
Tali violazioni possono comportare l'adozione di sanzioni disciplinari, nei limiti stabiliti dal Contratto Collettivo Nazionale Lavoro (CCNL) applicabile e nel pieno rispetto delle tutele previste dall'art. 7 della legge 20 maggio 1970 n. 300. In questo caso, sono previste le seguenti sanzioni disciplinari:

I. richiamo verbale;
II. ammonizione scritta;
III. multa non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare;
IV. sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;
V. licenziamento per mancanze *ex* art. 10 del CCNL: licenziamento con preavviso, licenziamento senza preavviso.

La tipologia e l'entità della sanzione è definita tenendo conto della gravità e/o recidività della violazione e del grado di colpa, più precisamente:

- intenzionalità del comportamento;
- presenza di circostanze aggravanti o attenuanti;
- rilevanza degli obblighi violati;
- entità del danno derivante alla Società;
- ruolo, livello di responsabilità gerarchica e autonomia del dipendente;
- eventuale condivisione di responsabilità con altri soggetti che abbiano concorso a determinare la mancanza;
- eventuali simili precedenti disciplinari.

A titolo esemplificativo, in caso di violazione delle regole previste dal Modello o da questo richiamate e in caso di commissione (anche sotto forma di tentativo) di qualsiasi illecito penale per cui è applicabile il D.Lgs. 231/2001, si applicano i provvedimenti sotto riportati.
Incorre nei provvedimenti di richiamo verbale, ammonizione scritta, multa o sospensione, il dipendente che violi le procedure interne previste o richiamate dal presente Modello - ad esempio non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere i controlli di competenza o adotti, nell'espletamento di attività sensibili, un comportamento non conforme alle prescrizioni del Modello stesso. La sanzione sarà commisurata alla gravità dell'infrazione e alla reiterazione della stessa.
Costituiscono comunque grave trasgressione, ove non si configuri un comportamento sanzionabile con uno dei provvedimenti di cui ai punti successivi, i seguenti comportamenti:

- l'inadempimento degli obblighi di "segnalazione" e di "informazione" nei confronti dell'Organismo di Vigilanza;
- la non giustificata o sistematica mancata partecipazione alle iniziative di formazione in tema 231, promosse dalla Società;
- il mancato rispetto delle regole di condotta previste dal Codice Etico;
- il mancato rispetto delle procedure e di altri presidi di controllo previsti per le attività sensibili nella Parte Speciale del presente Modello;
- in tema di *whistleblowing* l'effettuazione con dolo o colpa grave di segnalazioni che si rivelano infondate.

Incorre nel provvedimento di licenziamento senza preavviso il dipendente che adotti, nell'espletamento delle attività sensibili, un comportamento palesemente in violazione delle prescrizioni del Modello o del Codice Etico, tale da determinare la concreta applicazione a carico della Società di misure previste dal D.Lgs. 231/2001.
Ad ogni notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. Una volta accertata la violazione, sarà comminata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa e all'eventuale recidiva.
Resta inteso che saranno rispettate le procedure, le disposizioni e le garanzie previste dall'articolo 7 dello Statuto dei Lavoratori, in materia di provvedimenti disciplinari.
L'accertamento delle infrazioni (eventualmente su segnalazione dell'Organismo di Vigilanza), la gestione dei provvedimenti disciplinari e l'irrogazione delle sanzioni stesse sono di competenza del Datore di Lavoro con il supporto del *management* di riferimento.
Ogni atto relativo al procedimento disciplinare dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

5.3. Misure nei confronti dei dirigenti

Con riferimento ai dirigenti, valgono le vigenti norme di legge e/o di contrattazione collettiva.
Le misure disciplinari nei confronti dei dirigenti sono, oltre alla revoca della procura o delle procure eventualmente conferite:
- la censura scritta, nell'ipotesi di violazione non grave del Modello;
- il licenziamento senza preavviso, nell'ipotesi di grave violazione del Modello che leda irreparabilmente il rapporto di fiducia con la Società in modo tale da non consentire la prosecuzione, nemmeno provvisoria, del rapporto di lavoro.

A meramente titolo esemplificativo, costituiscono infrazioni:
- la commissione, anche sotto forma di tentativo, di un reato per cui è applicabile il D.Lgs. 231/2001 nell'espletamento delle proprie funzioni;
- l'inosservanza delle regole prescritte dal Modello o dal Codice Etico;
- la mancata vigilanza sui sottoposti circa il rispetto del Modello e delle regole da esso richiamate;

- l'inadempimento degli obblighi di "segnalazione" e di "informazione" nei confronti dell'Organismo di Vigilanza;
- la tolleranza od omessa segnalazione di irregolarità commessa da altri prestatori di lavoro o *partner* della Società;
- in tema di *whistleblowing,* la violazione delle misure di tutela del segnalante.

In ogni caso, se la violazione del Modello fa venire meno il rapporto di fiducia, la sanzione è individuata nella risoluzione del rapporto di lavoro.
Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

5.4. Misure nei confronti degli Amministratori

L'Organismo di Vigilanza, nel caso in cui raccolga la notizia della violazione delle disposizioni e delle regole di comportamento del Modello o del Codice Etico da parte di membri del Consiglio di Amministrazione, dovrà tempestivamente informare dell'accaduto l'Assemblea dei Soci e l'intero Consiglio di Amministrazione che, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potrà assumere gli opportuni provvedimenti previsti dalla Legge, sentito il parere del Collegio Sindacale.
L'Assemblea dei Soci su proposta del Consiglio di Amministrazione, sentito il Collegio Sindacale, tenuto conto della gravità della violazione e delle circostanze in cui è stata commessa, adotterà, in conformità ai poteri previsti dalla legge e/o dallo statuto, le misure sanzionatorie qui di seguito indicate e ferma restando la facoltà per la Società di esperire le azioni giudiziarie civili e/o penali indipendentemente ed a prescindere dall'applicazione di dette misure:
- revoca della delega;
- revoca dell'incarico.

Nel caso di violazioni poste in essere da un soggetto facente parte del vertice aziendale che rivesta altresì la qualifica di dirigente si applicheranno le sanzioni disciplinari di cui al paragrafo 5.3 che precede.
Si specifica, a titolo esemplificativo, che costituisce violazione dei doveri degli amministratori:
- la commissione nell'espletamento delle proprie funzioni, anche sotto forma di tentativo, di un reato per cui è applicabile il D.Lgs. 231/2001;
- l'inosservanza delle regole prescritte dal Modello o dal Codice Etico;
- la mancata vigilanza sui prestatori di lavoro o *partner* della Società circa il rispetto del Modello e delle regole da esso richiamate;
- l'inadempimento degli obblighi di "segnalazione" nei confronti dell'Organismo di Vigilanza;
- la tolleranza od omessa segnalazione di irregolarità commessa da altri prestatori di lavoro o *partner* della Società;
- in tema di *whistleblowing,* la violazione delle misure di tutela del segnalante.

Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni ed il monitoraggio di sua competenza.

5.5. Misure nei confronti dei Sindaci

Anche in caso di comportamenti da parte di uno o più Sindaci che violino il Modello o il Codice Etico, l'Organismo di Vigilanza sarà tenuto ad informare il Collegio Sindacale ed il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti.
L'Assemblea dei Soci su proposta del Consiglio di Amministrazione, sentito il Collegio Sindacale, tenuto conto della gravità della violazione e delle circostanze in cui è stata commessa revocherà l'incarico per giusta causa, in conformità ai poteri previsti dalla legge e/o dallo statuto, ferma restando la facoltà per la Società di esperire le azioni giudiziarie civili e/o penali indipendentemente ed a prescindere dall'applicazione di detta misura.
A titolo meramente esemplificativo, costituisce violazione del Modello:

- l'omissione della supervisione e/o della vigilanza sui sottoposti circa la corretta applicazione delle regole comportamentali e procedurali del Modello;
- la mancata comunicazione all'Organismo di Vigilanza e/o al Consiglio di Amministrazione e/o al Collegio Sindacale delle violazioni del Modello poste in essere da dipendenti e/o vertici aziendali di cui si abbia conoscenza certa e diretta.

Ogni atto relativo al procedimento sanzionatorio dovrà essere comunicato all'Organismo di Vigilanza per le valutazioni e il monitoraggio di sua competenza.

5.6. Misure nei confronti di partner d'affari, consulenti e collaboratori esterni

L'adozione – da parte di *partner* d'affari, fornitori, agenti, intermediari, consulenti e collaboratori esterni, comunque denominati, o altri soggetti aventi rapporti contrattuali con la Società – di comportamenti in contrasto con il D.Lgs. 231/2001 e con i principi ed i valori contenuti nella Carta della Fiducia sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.
L'adozione reiterata di comportamenti in contrasto con il D.Lgs. 231/2001 o la violazione grave o reiterata dei principi contenuti nella Carta della Fiducia sarà considerata inadempimento degli obblighi contrattuali e potrà dar luogo alla risoluzione del contratto da parte della Società.

6. AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO

Il Consiglio di Amministrazione delibera in merito all'aggiornamento del Modello e al suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza, ad esempio, di:
- modifiche dell'assetto organizzativo della Società e/o delle modalità di svolgimento delle attività d'impresa;
- modifiche normative;
- risultanze dei controlli;
- significative violazioni delle prescrizioni del Modello.

Nel caso in cui si rendano necessarie modifiche di natura esclusivamente formale, quali chiarimenti o precisazioni del testo, i Responsabili aziendali possono provvedervi in maniera autonoma, dopo aver sentito il parere dell'OdV, previa autorizzazione del Presidente o dal Direttore Generale, il quale ne riferisce senza indugio al Consiglio di Amministrazione.
In ogni caso, eventuali accadimenti che rendano necessaria la modifica o l'aggiornamento del Modello devono essere segnalati in forma scritta dall'OdV al Consiglio di Amministrazione, affinché lo stesso possa effettuare le delibere di propria competenza.

7. PRESIDI DI CONTROLLO DEL MODELLO

La *Chart of Approval* (*CoA*) e i *Kics* (*Key Internal Controls*) sono presidi di controllo che si fondano sulle procedure aziendali.

7.1. Chart of Approval

La Carta delle Approvazioni (*CoA, Chart of Approval*) è il documento che disciplina i livelli autorizzativi interni suddivisi per macroaree aziendali, il cui obiettivo consiste nel normare e schematizzare i ruoli richiamati al fine di prendere le decisioni riguardanti l'organizzazione di Schneider Electric.
Le decisioni, che vengono approvate seguendo il procedimento stabilito all'interno della *Chart of Approval,* si concretizzano in un atto giuridico, che viene sottoscritto dal procuratore della Società (in possesso di valida procura) e che vincolerà una Società del Gruppo nei confronti di soggetti terzi.
Coloro che approvano la richiesta (i cd. Approvatori) vengono designati per titoli e non per nomi.

7.2. La campagna annuale di autovalutazione: i Kics (Key Internal Controls)

È il processo di *self-assessment* attraverso il quale i responsabili di processo assegnati verificano l'applicazione dei processi aziendali gestiti per mezzo di regole e procedure che l'azienda impone ai propri dipendenti. Annualmente la Società pianifica una campagna di autovalutazione (i cd. *Kics* "*Key Internal Controls"*), che costituisce parte integrante del Modello di controllo. Tali *Kics* vengono definiti nel loro contenuto da esperti in materia appartenenti alle varie funzioni aziendali, con l'obiettivo di:

- prevenire rischi e frodi;
- proteggere i beni;
- salvaguardare le organizzazioni, aiutare i proprietari di processi e i manager operativi nell'affrontare o mitigare i rischi stessi.

Nel caso in cui a seguito della campagna Kics vengono identificate delle non conformità rispetto ai processi aziendali, esse devono essere corrette entro un tempo definito tramite dei piani di azione specifici.

7.3. Procedure aziendali

Le Società facenti parte del Gruppo Schneider hanno l'obiettivo, per il tramite delle procedure aziendali, di:

- migliorare la qualità dei processi interni attraverso una corretta opera di formalizzazione, diffusione e informazione in merito a regole e prassi aziendali;
- ridurre il rischio civile e penale per il singolo dipendente, sia esso collaboratore che apicale;
- ridurre i rischi civili e penali per la Società.

Attraverso le procedure aziendali, ogni Società facente parte del Gruppo formula degli schemi di controllo interno nei quali sono esplicitati i protocolli specifici di prevenzione per ciascuna delle attività a rischio identificate. All'interno di ogni schema di controllo, sono individuati i controlli/protocolli specifici adottati dalla Società per la determinata attività a rischio e volti a prevenire la commissione dei reati *ex* D.Lgs. 231/2001.

Tutte le procedure aziendali, sia della Società che del Gruppo, sono disponibili all'interno del portale Spice+ sia nella pagina Global per le politiche del Gruppo che sulla pagina Italia per le politiche della Società.

Inoltre, nella successiva Parte Speciale, il presente documento individua le attività denominate sensibili a causa del rischio insito di commissione dei reati della specie di quelli elencati al Capitolo 2.

8. APPENDICE CANALI DI SEGNALAZIONE DELLE IRREGOLARITÀ

Le irregolarità rispetto alle politiche aziendali e del D.Lgs. 231/2001 possono essere effettuate tramite i seguenti canali di comunicazione:

- il portale di segnalazione Trust Line disponibile al seguente link: https://secure.ethicspoint.eu/domain/media/en/gui/100211/index.html;
- tramite lettera in busta chiusa, da spedire o consegnare presso l'indirizzo della Società ed indirizzata all'Organismo di Vigilanza;
- tramite mail all'indirizzo di posta elettronica dedicato odv.eliwell@se.com dell'Organismo di Vigilanza.

Parte Speciale

Documento approvato

con delibera del Consiglio di Amministrazione del 4 marzo 2024

1. INTRODUZIONE

La presente Parte Speciale del Modello ha la finalità di definire i principi di comportamento e i presidi di controllo che i Destinatari (come definiti al par. 4.1. della Parte Generale), coinvolti nell'ambito delle "attività sensibili", devono osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali. Al suo interno sono analizzate tutte le attività che a seguito di un audit interno sono state ritenute sensibili ai sensi del D.Lgs. 231/2001

Parte Speciale A

Gestione delle relazioni con la Pubblica Amministrazione (PA) e gli Enti certificatori

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito dei processi relativi alla gestione delle relazioni con la Pubblica Amministrazione[2] e gli enti certificatori sono:

- gestione dei rapporti con la Pubblica Amministrazione:
  - in occasione di visite ispettive;
  - ai fini dell'ottenimento di autorizzazioni / licenze;
  - in occasione della gestione ed esecuzione di adempimenti;
- gestione dei rapporti con gli Enti certificatori;
- gestione del contenzioso.

2. GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE IN OCCASIONE DI VISITE ISPETTIVE

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;

[2] Per Pubblica Amministrazione si intendono: le istituzioni pubbliche, i pubblici ufficiali e gli incaricati di pubblico servizio.
Le **istituzioni pubbliche** sono le amministrazioni dello Stato (quali l'Amministrazione Finanziaria, le Autorità garanti e di Vigilanza, le Autorità Giudiziarie); le aziende e le amministrazioni dello Stato ad ordinamento autonomo; le Regioni, le Province e i Comuni, le comunità montane, nonché i loro consorzi e associazioni; le istituzioni universitarie; le Camere di Commercio, Industria, Artigianato e Agricoltura; gli enti pubblici non economici nazionali, regionali e locali; le amministrazioni, le aziende e gli enti del Servizio Sanitario Nazionale. La funzione pubblica viene rivestita anche dalla Commissione delle Comunità Europee, dal Parlamento Europeo, dalla Corte di Giustizia e dalla Corte dei Conti delle Comunità Europee.
I **pubblici ufficiali** sono i pubblici dipendenti o privati, che possono o devono formare e manifestare la volontà della P.A., ovvero esercitare poteri autoritativi o certificativi nell'ambito di una potestà di diritto pubblico.
Gli **incaricati di pubblico servizio** sono coloro che, a qualunque titolo, prestano un pubblico servizio senza essere dotati di poteri tipici della pubblica funzione, quali quelli autoritativi e certificativi.

- art. 322. c.p. - Istigazione alla corruzione;
- art. 322-*bis* c.p. - Induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri;
- art. 640 c.p. - Truffa;

- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 2638 c.c. - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

2.2. Principi di comportamento[3]

I Destinatari devono:

- intrattenere rapporti corretti, trasparenti, imparziali e collaborativi con i funzionari della Pubblica Amministrazione e le Autorità Pubbliche di Vigilanza a cui la Società è soggetta;

- segnalare, senza ritardo, al proprio responsabile gerarchico e all'Organismo di Vigilanza eventuali tentativi di richieste indebite da parte di funzionari della Pubblica Amministrazione, rivolti, ad esempio, ad ottenere favori, elargizioni illecite di denaro od altre utilità, anche nei confronti di terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la Pubblica Amministrazione;

- fornire ai propri collaboratori (interni ed esterni) adeguate direttive sulle modalità di condotta da adottare nei contatti formali e informali con soggetti della Pubblica Amministrazione;

- garantire che a rappresentare la Società siano i soggetti autorizzati nel rispetto del sistema di procure e deleghe in essere e che sia tenuta traccia delle ispezioni ricevute e delle eventuali sanzioni comminate;

- prestare completa e immediata collaborazione ai funzionari della Pubblica Amministrazione, fornendo puntualmente ed esaustivamente la documentazione e le informazioni richieste sia nell'ambito di visite ispettive sia nell'ordinario svolgimento di attività di vigilanza da parte di Autorità pubbliche;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- corrispondere od offrire, direttamente o indirettamente, anche sotto forme diverse di aiuti o contribuzioni (ad esempio sponsorizzazioni e liberalità), pagamenti o benefici materiali a pubblici ufficiali o incaricati di pubblico servizio o a persone a questi vicini, per influenzare il loro comportamento ed assicurare vantaggi di qualunque tipo alla Società;

- effettuare promesse o indebite elargizioni di omaggi o altra utilità a pubblici funzionari o incaricati di pubblico servizio o persone a questi vicini, con la finalità di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;

- ricorrere a forme di contribuzione che, sotto la veste di affidamento di incarichi professionali, consulenze, pubblicità o altro, abbiano il fine di influenzare l'attività dei pubblici funzionari nell'espletamento dei loro doveri;

- cedere a raccomandazioni o pressioni provenienti da pubblici funzionari o incaricati di pubblico servizio;

- ricercare e/o instaurare rapporti personali di favore ovvero condizionare impropriamente, in modo diretto o indiretto, le decisioni della Pubblica Amministrazione e/o lo svolgimento di un corretto rapporto con la

[3] I principi di comportamento qui riportati valgono anche per le altre attività sensibili concernenti i rapporti con la P.A. e gli Enti certificatori.

stessa, al fine di ottenere vantaggi indebiti o indurre, facilitare o remunerare una decisione, il compimento di un atto d'ufficio o contrario ai doveri d'ufficio da parte di esponenti della Pubblica Amministrazione;

- tenere condotte ingannevoli nei confronti della Pubblica Amministrazione tali da indurla in errori di valutazione;

- omettere le informazioni dovute nelle comunicazioni alle Autorità Pubbliche di Vigilanza e, in genere, tenere comportamenti ostruzionistici quali, a titolo puramente indicativo, opporre rifiuti pretestuosi, ritardare l'invio delle comunicazioni o la messa a disposizione della documentazione richiesta;

- ostacolare in qualunque modo le Autorità Pubbliche di Vigilanza nell'esercizio delle funzioni loro demandate dalla legge.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle relazioni con la Pubblica Amministrazione in occasione di visite ispettive:

- In caso di visite ispettive, i funzionari pubblici/incaricati di pubblico servizio devono essere identificati al loro arrivo e conseguentemente registrati.

- Le visite ispettive sono gestite dal personale delle Direzioni / Funzioni aziendali competenti per materia, sotto la supervisione dei Responsabili delle stesse.

- Durante le ispezioni devono partecipare almeno due rappresentanti aziendali di cui almeno uno formalmente delegato.

- Il soggetto formalmente delegato, prima di sottoscrivere il verbale rilasciato dal funzionario pubblico, è responsabile di leggere attentamente il contenuto dello stesso al fine di verificare che le informazioni ivi riportate siano corrette. Diversamente, devono essere fatte presenti le proprie considerazioni all'ispettore intervenuto, il quale è tenuto a provvedere alla rettifica o all'annotazione della dichiarazione sul verbale stesso.

- Il rappresentante aziendale responsabile della gestione della visita ispettiva deve garantire la tracciabilità della documentazione richiesta ed effettivamente consegnata / trasmessa ai funzionari pubblici in sede di visita ispettiva.

- I verbali dell'ispezione predisposti dalla Pubblica Autorità devono essere verificati e archiviati dal rappresentante aziendale responsabile della gestione della visita ispettiva.

- Ove non venga rilasciato apposito verbale da parte dell'Autorità competente, i soggetti interni idoneamente individuati, a cui è affidata la gestione della visita ispettiva, devono redigere al termine della stessa un verbale interno da trasmettersi all'Organismo di Vigilanza.

- Tutta la documentazione rilevante, ivi inclusi l'originale dei verbali relativi alle visite ispettive, deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

- In occasione delle visite ispettive deve essere predisposto ed aggiornato un apposito registro elettronico che tenga traccia delle visite e che permetta di individuare le generalità degli ispettori, l'ente di appartenenza ed il motivo della visita.

3. GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE AI FINI DELL'OTTENIMENTO DI AUTORIZZAZIONI / LICENZE

3.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
  - art. 322-*bis* c.p. - Induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri;
  - art. 640 c.p. - Truffa.

3.2. Principi di comportamento

I Destinatari devono:

- assicurare che la documentazione inviata o condivisa con la Pubblica Amministrazione, predisposta sia internamente che con il supporto eventuale di collaboratori / consulenti, sia completa, veritiera e corretta e le informazioni e/o dati ivi contenuti attinenti siano corretti ed esaustivi;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

Inoltre, è espressamente vietato:

- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società.

3.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle relazioni con la Pubblica Amministrazione ai fini dell'ottenimento di autorizzazioni / licenze:

- I rapporti con i funzionari della Pubblica Amministrazione per l'ottenimento di autorizzazioni e licenze sono intrattenuti da personale della Società cui sono conferite adeguate procure o deleghe formali o da consulenti esterni opportunamente delegati all'interno delle lettere di incarico per la prestazione del servizio.

- Il personale della Direzione / Funzione aziendale competente deve predisporre la pratica di richiesta alla Pubblica Amministrazione e la relativa documentazione a supporto.

- Il Responsabile della Direzione / Funzione aziendale competente, o persona da questi delegata, deve effettuare una verifica di completezza e correttezza della documentazione da inviare/trasmettere alla Pubblica Amministrazione.

- Qualora in fase di presentazione delle richiesta, o successivamente alla stessa, siano svolti incontri con esponenti della Pubblica Amministrazione, deve essere garantita la rendicontazione degli stessi, avendo cura di specificare il nominativo dei rappresentanti aziendali partecipanti, dei rappresentanti della Pubblica

Amministrazione presenti e del relativo ente di appartenenza, dell'oggetto dell'incontro, degli esiti dello stesso, di eventuali criticità emerse e di ogni altra informazione rilevante.

- La documentazione da inviare / trasmettere alla Pubblica Amministrazione deve essere sottoscritta sulla base del sistema di deleghe e procure in vigore.

- Tutta la documentazione rilevante deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

4. GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE IN OCCASIONE DELLA GESTIONE ED ESECUZIONE DI ADEMPIMENTI

4.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), in particolare:
  - art. 318 c.p. – Corruzione per l'esercizio della funzione;
  - art. 319 c.p. – Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. – Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. – Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. – Pene per il corruttore;
  - art. 322. C.p. – Istigazione alla corruzione;
  - art. 322-*bis* c.p. – Induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri;
  - art. 640 c.p. – Truffa;
  - art. 640-*ter* c.p. – Frode informatica.
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 2638 c.c. – Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n.74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 8 D.Lgs. n.74/2000 – Emissione di fatture o altri documenti per operazioni inesistenti;
  - art. 11 D.Lgs. n. 74/2000 – Sottrazione fraudolenta al pagamento di imposte

4.2. Principi di comportamento

I Destinatari devono:

- assicurare che i rapporti intrattenuti con i pubblici ufficiali siano gestiti esclusivamente dai soggetti muniti di idonei poteri;

- espletare diligentemente e tempestivamente tutti gli adempimenti richiesti dalla normativa / regolamentazione pubblica applicabile nell'ambito della propria attività;

- assicurare che gli adempimenti nei confronti della Pubblica Amministrazione siano effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete e veritiere evitando, e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto di interesse;

- trasmettere tutte le comunicazioni previste dalla legge e dai regolamenti alle Autorità di Vigilanza, o qualsiasi altra comunicazione richiesta per altri motivi, con la massima tempestività e nel modo più completo e accurato possibile;

- assicurare lo svolgimento di un processo periodico di monitoraggio finalizzato a intercettare l'eventuale insorgere di novità in materia tributaria;

- garantire il monitoraggio delle scadenze fiscali, sulla base delle scadenze di legge previste;

- provvedere tempestivamente, secondo i termini di legge, all'effettuazione delle dichiarazioni e pagamenti di natura fiscale alle Autorità competenti;

- garantire la tracciabilità del processo relativo alla trasmissione delle dichiarazioni fiscali alle Autorità competenti, da effettuarsi nel rispetto delle norme di legge e regolamenti, in virtù degli obiettivi di trasparenza e corretta informazione;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- esporre dati, notizie, informazioni false nelle comunicazioni alle Autorità Pubbliche di Vigilanza o occultare fatti che avrebbero dovuto essere comunicati;

- accedere senza autorizzazione ai sistemi informativi della Pubblica Amministrazione, intervenire su dati ed informazioni in essi contenuti per procurare un indebito vantaggio alla Società o a terzi;

- laddove gli adempimenti vengano effettuati utilizzando il sistema informatico/telematico della Pubblica Amministrazione, alterare lo stesso ed i dati inseriti, ovvero utilizzare in modo improprio o illecito i dati trattati, procurando un danno alla stessa Pubblica Amministrazione;

- indicare, al fine di evadere le imposte sui redditi o sul valore aggiunto, nelle dichiarazioni relative a dette imposte, elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o inesistenti o crediti e ritenute fittizi;

- predisporre e inviare dichiarazioni fiscali alle Autorità competenti, contenenti dati falsi, artefatti, incompleti o comunque non rispondenti al vero;

- omettere dichiarazioni / comunicazioni di natura fiscale, dovute per legge, al fine di evadere le imposte.

4.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle relazioni con la Pubblica Amministrazione in occasione della gestione ed esecuzione di adempimenti:

- Il personale della Direzione / Funzione aziendale competente, deve predisporre, in occasione della trasmissione di domande, istanze, comunicazioni, atti, dichiarazioni, rendiconti o altra documentazione richiesta dalla Pubblica Amministrazione, la pratica e la relativa documentazione a supporto.

- Il Responsabile della Funzione aziendale competente, o persona da questi delegata, deve effettuare una verifica di completezza e correttezza della documentazione da inviare / trasmettere alla Pubblica Amministrazione.

- La documentazione da inviare / trasmettere alla Pubblica Amministrazione deve essere sottoscritta sulla base del sistema di deleghe e procure in vigore.

- Nel caso in cui i rapporti con la Pubblica Amministrazione siano intrattenuti e gestiti da collaboratori e/o consulenti / partner esterni, l'oggetto di tale servizio è regolamentato in forza di apposito contratto / lettera d'incarico, redatto per iscritto e riportante il compenso pattuito e il contenuto della prestazione nonché, ove necessario, formale mandato ad operare in nome e per conto della Società.

- Qualora in fase di gestione degli adempimenti si svolgano incontri, anche di natura istituzionale, con esponenti della Pubblica Amministrazione, deve essere prevista la partecipazione di almeno due esponenti aziendali formalmente delegati.

- Deve essere garantita la tracciabilità e rendicontazione dei predetti incontri, avendo cura di specificare il nominativo dei rappresentanti aziendali partecipanti, dei rappresentanti della Pubblica Amministrazione presenti e del relativo ente di appartenenza, dell'oggetto dell'incontro, degli esiti dello stesso, di eventuali criticità emerse e di ogni altra informazione rilevante.

- Tutta la documentazione rilevante deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

Con specifico riferimento alla gestione degli adempimenti di natura fiscale, si evidenzia che:

- il pagamento dell'IVA tramite F24 viene fatto esclusivamente per le PA Split Payment;

- Il consulente fiscale esterno predispone, sulla base dei dati e delle informazioni trasmesse (bilancio di verifica) dalla Funzione Finance il Modello dichiarativo F24, che trasmette, mediante apposita piattaforma telematica, entro i termini di legge, all'Amministrazione Finanziaria;

- Il consulente fiscale esterno, a seguito dell'avvenuta trasmissione, invia alla Società una copia dei Modelli dichiarativi in versione definitiva e la ricevuta di avvenuta ricezione da parte dell'Amministrazione Finanziaria;

- I modelli dichiarativi devono essere sottoscritti nel rispetto delle procure vigenti;

- il Tax Manager di gruppo redige, unitamente alla funzione Finance ed al consulente fiscale esterno, le dichiarazioni dei redditi e provvede ad istruire il pagamento delle relative imposte;

- il consulente fiscale esterno trasmette, nei termini di legge, i modelli fiscali relativi alle dichiarazioni dei redditi dell'esercizio.

5. GESTIONE DEI RAPPORTI CON GLI ENTI CERTIFICATORI

5.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:

- art. 2635 c.c. – Corruzione tra privati;

5.2. Principi di comportamento

Per l'attività sensibile in oggetto si rimanda ai principi di comportamento stabiliti nell'ambito della gestione dei rapporti con la P.A.[4].

5.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione dei rapporti con gli Enti certificatori finalizzati all'ottenimento / rinnovo delle certificazioni di prodotto:

- Gli Enti certificatori sono selezionati sulla base di almeno due offerte tecnico/economiche quando applicabile.

- I rapporti con gli Enti certificatori sono regolati da appositi contratti autorizzati e sottoscritti da soggetti dotati di idonei poteri in linea con il sistema di deleghe e procure in vigore.

- Le visite annuali degli Enti certificatori, volte al mantenimento della certificazione, sono definite dall'ente stesso e comunicate formalmente alla Società. La comunicazione della visita contiene il dettaglio delle aree e delle tempistiche oggetto di ispezione.

- Il personale che si interfaccia con l'Ente certificatore deve essere formalmente delegato da personale dotato di idonei poteri.

- In caso di visita deve essere garantita la presenza di almeno due persone della società.

- Prima del formale avvio della visita, l'ente certificatore, di concerto con il Quality Manager e i responsabili di funzione individuati (a seconda delle aree oggetto di ispezione), organizza un incontro nel quale vengono esplicitati gli obiettivi dell'intervento.

- Al termine della visita viene svolto un incontro riepilogativo in occasione del quale vengono riportate le risultanze dell'incontro e condivisi eventuali action plan.

- Il report di visita dell'ente certificatore viene siglato congiuntamente dall'Ente stesso e dal Quality Manager.

- Il Quality Manager provvede a diffondere, via mail, il report di visita ai responsabili di funzione coinvolti.

6. GESTIONE DEL CONTENZIOSO

6.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dall'art. 25 del D.Lgs. 231/2001), in particolare:
  - art. 319-*ter* c.p. – Corruzione in atti giudiziari;
  - art. 321 c.p. – Pene per il corruttore;
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:

[4] Vedi § 2.2. e ss della Parte Speciale A.

- art. 2621 c.c. – False comunicazioni sociali;
- art. 2621-*bis* c.c. – Fatti di lieve entità;
- art. 2635 c.c. – Corruzione tra privati;

- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, art. 377-*bis* c.p. (richiamato dall'art. 25-*decies* del D.Lgs. 231/2001).

6.2. Principi di comportamento

I Destinatari devono:

- assicurare che i rapporti intrattenuti con l'Autorità Giudiziaria avvengano nell'assoluto rispetto delle leggi e normative vigenti. Inoltre, tali rapporti devono rispettare i principi di lealtà e correttezza ed essere improntati alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del ruolo istituzionale, dando puntuale e sollecita esecuzione alle prescrizioni e agli adempimenti richiesti;

- garantire la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte;

- sottoporre ai soggetti muniti di idonei poteri, in base al sistema di procure e deleghe in essere, la documentazione al fine di verificarla ed approvarla prima dell'inoltro all'Autorità Giudiziaria;

- rendere sempre all'Autorità Giudiziaria dichiarazioni veritiere, complete, corrette e rappresentative dei fatti;

- esprimere liberamente le proprie rappresentazioni dei fatti, se indagati o imputati in procedimenti penali;

- avvertire tempestivamente il proprio responsabile gerarchico di ogni minaccia, pressione, offerta o promessa di denaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da utilizzare in procedimenti penali;

- avvertire tempestivamente il Vertice aziendale di ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o ad essa attinente;

- garantire la corretta archiviazione di tutta la documentazione prodotta e consegnata al fine di garantire la tracciabilità delle varie fasi del processo;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- effettuare promesse o indebite elargizioni di denaro o altra utilità (ad esempio, assunzioni, conferimenti di incarichi di natura professionale, commerciale o tecnica) a pubblici funzionari o incaricati di pubblico servizio o persone a questi vicini con la finalità di promuovere o favorire interessi della Società;

- erogare omaggi o altre utilità a pubblici funzionari o incaricati di pubblico servizio oppure cedere a raccomandazioni o pressioni provenienti da essi con le stesse finalità vietate al punto precedente;

- esibire documenti falsi o alterati;

- condizionare o indurre, in qualsiasi forma e con qualsiasi modalità, la volontà dei soggetti chiamati a rispondere all'Autorità Giudiziaria al fine di non rendere dichiarazioni o dichiarare fatti non rispondenti al vero;

- promettere o offrire denaro, omaggi o altra utilità a soggetti coinvolti in procedimenti civili, penali o amministrativi o a persone a questi vicini;

- tenere una condotta ingannevole che possa indurre l'Autorità Giudiziaria in errore di valutazione della documentazione presentata.

6.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione del contenzioso. In generale bisogna distinguere tra il contenzioso legale in senso stretto (es. claims relativi al prodotto) ed il contenzioso relativo al recupero crediti:

- nel primo caso, la funzione Legal di Gruppo è la principale responsabile della gestione dei contenziosi aziendali. Ove necessario, in base alla complessità delle controversie, la funzione Legal si può avvalere del supporto di consulenti legali esterni;

- nel secondo caso, è il Credit Manager a valutare la necessità di ricorrere alle vie legali per il recupero del credito. Per tali controversie la Società si avvale di un consulente legale esterno.

- Contenzioso in senso stretto

- La funzione Legal di gruppo provvede ad attivare ed istruire tutte le attività necessarie alla risoluzione dei contenziosi.

- L'avvio di cause, arbitrati o simili procedimenti che prevedono risarcimenti o spese legali deve essere autorizzato da personale dotato di adeguati poteri in base al sistema di deleghe e procure in vigore.

- La selezione e gestione di eventuali nuovi consulenti esterni e legali che supportano la Società nello svolgimento delle attività rientranti in questo ambito, è disciplinata dall'attività sensibile "Gestione degli acquisti indiretti" cui si rimanda.

- La funzione Legal di gruppo, svolte le attività istruttorie del caso, sulla base degli elementi in proprio possesso, elabora con il supporto del/dei legale/i esterni la strategia da adottare, la quale viene valutata dal CFO.

- La documentazione inviata all'Autorità Giudiziaria *(e.g. mezzi probatori, atti di causa, scritti difensivi, ecc.)*, debitamente verificata in termini di correttezza e accuratezza, deve essere sottoscritta da soggetti muniti di adeguati poteri in base al sistema di deleghe e procure in vigore.

- I rapporti con le Autorità pubbliche in occasione di contenziosi devono essere gestiti da soggetti dotati di adeguate deleghe / procure.

- Eventuali accordi transattivi devono essere autorizzati da soggetti dotati di adeguati poteri sulla base del sistema di deleghe e procure in vigore.

- Tutta la documentazione rilevante deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

- Contenzioso derivante dal recupero crediti

  - *Recupero mediante decreto ingiuntivo*

- Il Credit Manager, a fronte di una situazione di insolvenza, procede con l'invio ai clienti di lettere di sollecito.

- Le lettere di sollecito devono essere predisposte seguendo lo standard, predisposto dalla Funzione Legal di gruppo.

- Se a seguito delle lettere di sollecito la situazione di insolvenza persiste, il Credit Manager ricorre, mediante il supporto del legale, al decreto ingiuntivo.

- Tutta la documentazione rilevante deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

- *Recupero mediante procedure concorsuali*

- A fronte di procedure concorsuali (a titolo esemplificativo fallimenti, amministrazioni straordinarie) che investono clienti della società, il Credit Manager, ottenuta la notizia della procedura da parte del curatore fallimentare, deve provvedere alla compilazione della documentazione necessaria per l'ottenimento del credito.

- La documentazione per l'ottenimento del credito deve essere predisposta seguendo lo standard predisposto dalla Funzione Legal.

- La documentazione deve essere firmata da persone dotate di idonei poteri.

- Tutta la documentazione rilevante deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

Parte Speciale B

Gestione delle attività amministrative, contabili e societarie

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito dei processi relativi alla gestione delle attività amministrative, contabili e societarie sono:

- gestione della contabilità e predisposizione del bilancio di esercizio;

- gestione degli affari fiscali;

- gestione dei rapporti con il collegio sindacale, i soci e la società di revisione;

- gestione delle operazioni societarie straordinarie (ad esempio fusioni, conferimenti, operazioni sul capitale o sulle partecipazioni).

2. GESTIONE DELLA CONTABILITA' E PREDISPOSIZIONE DEL BILANCIO DI ESERCIZIO

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 2621 c.c. - False comunicazioni sociali;
  - art. 2627 c.c. - Illegale ripartizione degli utili e delle riserve;
  - art. 2632 c.c. - Formazione fittizia del capitale;
  - art. 2629 c.c. - Operazioni in pregiudizio dei creditori;
  - art. 2626 c.c. - Indebita restituzione dei conferimenti;
  - art. 2628 c.c. - Illecite operazioni sulle azioni o quote societarie.

- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n.74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 8 D.Lgs. n.74/2000 – Emissione di fatture o altri documenti per operazioni inesistenti;
  - art. 10 D.Lgs. n.74/2000 – Occultamento o distruzione di documenti contabili;
  - art. 11 D.Lgs. n. 74/2000 - Sottrazione fraudolenta al pagamento di imposte.

2.2. Principi di comportamento

I Destinatari devono:

- rispettare le regole e i principi contenuti nel Codice Civile, nei principi contabili e nelle altre disposizioni normative e regolamentari applicabili;

- osservare le regole di corretta, completa e trasparente registrazione contabile, secondo i criteri indicati dalla Legge e dai principi contabili adottati;

- garantire la tempestività, l'accuratezza e il rispetto del principio di competenza nell'effettuazione delle registrazioni contabili;

- assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima e coerente con la documentazione di riferimento;

- rispettare i criteri di ragionevolezza e prudenza nella valutazione e registrazione delle poste contabili, anche valutative/estimative, tenendo traccia dei parametri di valutazione e dei criteri che hanno guidato la determinazione del valore;

- assicurare che ogni operazione infragruppo avvenga secondo criteri di correttezza ed in ossequio ai contratti di servizio in essere;

- garantire la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte nel processo di chiusura contabile e di predisposizione del bilancio;

- tenere un comportamento corretto e trasparente in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente <u>vietato:</u>

- rappresentare in contabilità - o trasmettere per l'elaborazione e la rappresentazione in bilancio relazioni e prospetti o altre comunicazioni sociali – dati falsi, lacunosi o comunque non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della Società;

- registrare in contabilità operazioni a valori non corretti rispetto alla documentazione di riferimento, oppure a fronte di transazioni inesistenti in tutto o in parte, o senza un'adeguata documentazione di supporto che ne consenta una corretta rilevazione contabile e successivamente una ricostruzione accurata;

- omettere dati ed informazioni previsti dalla normativa vigente o dalle procedure e prassi interne sulla situazione economica, patrimoniale e finanziaria della Società;

- porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio mediante utilizzo di fatture per operazioni inesistenti emesse da terzi), ovvero finalizzate alla creazione di "fondi neri" o di "contabilità parallele";

- alterare o distruggere documenti ed informazioni finanziarie e contabili disponibili in formato cartaceo e/o elettronico.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito delle attività di gestione della contabilità e predisposizione del bilancio di esercizio:

- Gestione del sistema contabile e del piano dei conti

- Le registrazioni contabili, rilevanti ai fini del bilancio civilistico, devono essere effettuate esclusivamente attraverso l'applicativo dedicato, che garantisce la tracciabilità delle operazioni e l'esecuzione automatica di controlli contabili preimpostati.

- L'accesso all'applicativo contabile locale deve essere consentito esclusivamente agli utenti autorizzati tramite User ID e Password personali, assegnati dal Responsabile IT (mediante tool di ticketing) su richiesta della funzione Finance.

- L'accesso all'applicativo contabile per il *reporting package* deve essere consentito esclusivamente agli utenti autorizzati tramite User ID e Password personali, assegnati dalla Capogruppo su richiesta della Funzione Finance.

- Periodicamente deve essere svolta una verifica circa la corretta attribuzione tra profili e utenze ai fini del rispetto dei principi della *Segregation of Duties* (SoD).

- Le modifiche al piano dei conti civilistico devono essere preventivamente autorizzate dal Responsabile Finance e tracciate.

- La funzione Finance monitora che il piano dei conti di reporting package, predefinito e predisposto dalla Capogruppo, sia allineato con quanto riportato nell'ERP contabile locale.

- Tenuta della contabilità

- Deve essere garantita la segregazione delle funzioni tra i soggetti che effettuano le transazioni e i soggetti che le rilevano contabilmente.

- Le registrazioni contabili devono essere effettuate nel rispetto dei principi contabili adottati, a fronte di un'adeguata documentazione di supporto, archiviata a cura della Funzione Finance.

- Tutti i rapporti intercompany devono essere regolati attraverso politiche di *transfer price*.

- Ai fini della predisposizione del bilancio di esercizio deve essere garantita la tracciabilità dei dati/informazioni trasmessi dalle singole aree aziendali alla Funzione Finance, anche se di Gruppo.

- Chiusure contabili e predisposizione del reporting package

- Ai fini del reporting package è prevista una chiusura contabile mensile. Per rispettare le scadenze prefissate, le funzioni coinvolte nella chiusura contabile devono svolgere le attività rispettando le tempistiche individuate da un'apposita *checklist.*

- Le scritture contabili manuali, per la determinazione di fondi e stanziamenti, devono essere autorizzate dall'Amministratore Delegato.

- Con riferimento alle chiusure contabili mensili, la Funzione Finance, prima del formale invio del reporting package alla Capogruppo, svolge un'analisi finalizzata ad evidenziare gli scostamenti più rilevanti tra la situazione *as is* - *forecast* e tra la situazione *as is* e quella dell'anno precedente.

- Tali scostamenti vengono condivisi dalla Funzione Finance con l'Amministratore Delegato.

- Le motivazioni in merito ai principali scostamenti devono essere tracciate e ripercorribili.

  - Predisposizione del bilancio civilistico

  - Ai fini dell'approvazione del bilancio civilistico deve essere svolta almeno una riunione, che abbia ad oggetto il progetto di bilancio, tra l'Amministratore Delegato, la società di revisione che esercita il controllo legale dei conti e la funzione Finance di gruppo.

3. GESTIONE DEGLI AFFARI FISCALI

3.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 2621 c.c. - False comunicazioni sociali
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n.74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 8 D.Lgs. n. 74/2000 – Emissione di fatture o altri documenti per operazioni inesistenti;
  - art. 10 D.Lgs. n.74/2000 – Occultamento o distruzione di documenti contabili;
  - art. 11 D.Lgs. n. 74/2000 - Sottrazione fraudolenta al pagamento di imposte

3.2. Principi di comportamento e Presidi di controllo

Si rimanda ai paragrafi 2.3. e 2.4. della presente Parte Speciale, in quanto i Destinatari sono tenuti a rispettare i principi di comportamento e a garantire i presidi di controllo che vengono già definiti nell'ambito dell'attività di contabilità e predisposizione del bilancio d'esercizio.

3.3. I Reati Tributari

3.3.1. Principi di comportamento

Premesso che il principio generale a cui si ispirano le misure organizzative adottate dalla Società per assicurare una corretta, efficiente ed efficace gestione delle attività aziendali e, *inter alia*, prevenire la commissione dei Reati, può essere individuato nel rispetto dei requisiti di separazione, chiarezza, formalizzazione e comunicazione dei ruoli aziendali per quanto attiene, in particolare, l'attribuzione della responsabilità e della decisionalità in materia di assetti organizzativi e attività operative nonché della rappresentanza della Società, in tema di prevenzione dei citati reati tributari, più specificatamente i Destinatari devono:

- assicurare un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e dei principi contabili utilizzati, in tutte le attività finalizzate alla formazione del bilancio e delle dichiarazioni fiscali della Società ovvero della Capogruppo, in caso di adesione al consolidato fiscale nazionale;

- registrare correttamente ogni operazione attiva e passiva, verificando che sia debitamente autorizzata, verificabile, legittima, coerente e congrua;

- osservare tutte le norme poste dalla legge a disciplina dei rapporti giuridici ed economici tra società appartenenti allo stesso Gruppo, in particolare verificando che i contratti con la Capogruppo o con società collegate siano stipulati a fronte di effettive esigenze reciproche e rispondano alle normali regole di mercato;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- registrare o concorrere a registrare fatture od altri documenti relativi a forniture o prestazioni non effettivamente ricevute, in tutto od in parte, dalla Società;

- registrare o concorrere a registrare fatture od altri documenti emessi da un soggetto diverso da quello che ha fornito beni o prestazioni alla Società;

- emettere o concorrere ad emettere fatture od altri documenti relativi a forniture o prestazioni che la Società, in tutto od in parte, non ha effettivamente erogato;

- emettere o concorrere ad emettere fatture od altri documenti relativi a forniture o prestazioni che la Società ha erogato in favore di un soggetto diverso da quello indicato nei documenti stessi;

- effettuare o concorrere ad effettuare, in qualsiasi forma, pagamenti che non trovino causa in una fornitura di beni o prestazione di servizi effettivamente erogata in favore della Società e debitamente supportata da idonea documentazione commerciale, contabile e fiscale;

- alterare, occultare o distruggere documenti o scritture a rilevanza contabile o fiscale;

- compiere operazioni simulate di vendita del patrimonio della Società ovvero altri atti fraudolenti su propri od altrui beni;

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, considerati individualmente o nel loro complesso, integrino, direttamente o indirettamente, le fattispecie di reato di cui alla presente Parte Speciale.

3.3.2. Presidi di controllo

Ai fini dell'attuazione dei principi generali di comportamento elencati nel precedente paragrafo, i Destinatari devono rispettare i protocolli di controllo qui di seguito descritti, e le pertinenti procedure interne, posti a presidio del rischio-reato sopra identificato:

- Rapporti con Consulenti, Agenti, Partner e Fornitori

- i compensi riconosciuti in favore di consulenti, agenti, partner e fornitori sono stabiliti in forma scritta, con adeguata evidenza delle motivazioni che ne hanno influenzato la determinazione anche in termini di proporzionalità del compenso in relazione al tipo di incarico o di prestazione o di fornitura e al mercato di riferimento e sono autorizzati secondo i limiti di delega assegnata al richiedente;

- i pagamenti a favore di consulenti, agenti, partner e fornitori sono sempre supportati da idonea fattura, con l'evidenza del rapporto contrattuale sottostante e degli accordi intercorsi con le controparti e sulla

base dell'effettiva e valida ricezione dei beni o servizi concordati, confermata in forma scritta dalla funzione richiedente;

- il Responsabile Affari Legali di Gruppo (limitatamente ai documenti contrattuali) e, a seconda dei casi, il Responsabile della Funzione beneficiaria della consulenza o della fornitura assicurano l'ordinata e corretta archiviazione di tutta la documentazione relativa ai rapporti di consulenza/fornitura/partnership/agenzia di loro rispettiva competenza;

- il CAO (Chief Accounting Officer), attraverso la sua struttura, assicura l'ordinata e corretta archiviazione di tutta la documentazione contabile e fiscale relativa ai rapporti con consulenti, agenti, partner e fornitori.

- Rapporti con i clienti

- i rapporti con i clienti sono regolati da contratti/ordini redatti in forma scritta riportanti con chiarezza quantomeno l'oggetto, la durata, il prezzo, le modalità di pagamento e gli eventuali sconti/premi pattuiti. Il Responsabile Commerciale assicura l'ordinata raccolta ed archiviazione di tutti i contratti/ordini gestiti;

- i premi legati ai quantitativi acquistati e/o al fatturato raggiunto sono regolati da appositi contratti in forma scritta, redatti dalla Funzione Commerciale con il supporto del Responsabile Affari Legali di Gruppo, che ne assicura l'ordinata raccolta ed archiviazione.

- Formazione del bilancio e predisposizione di comunicazioni ai soci e/o ai terzi relative alla situazione economica, patrimoniale e finanziaria della Società

- a cura del CAO (Chief Accounting Officer), sono implementate e formalizzate istruzioni che definiscono con chiarezza per il personale coinvolto in attività di predisposizione del bilancio, i principi contabili da adottare per la definizione delle poste del bilancio e le modalità operative per la loro contabilizzazione. Tali indicazioni sono aggiornate dagli uffici competenti alla luce delle novità della normativa fiscale e civilistica e diffuse ai destinatari sopra indicati;

- a cura del CAO (Chief Accounting Officer) sono definite istruzioni operative rivolte alle Funzioni della Società che indicano i dati e le notizie che queste devono fornire ai servizi coinvolti nel processo di redazione del bilancio in relazione alle chiusure annuali ed infrannuali, nonché le relative modalità e tempistiche;

- i Responsabili delle singole Funzioni e, per quanto di competenza, il CAO (Chief Accounting Officer), assicurano che tutte e scritture di rettifica effettuate siano supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati e, analiticamente, lo sviluppo dei relativi calcoli;

- i Responsabili delle Funzioni deputate ai controlli periodici in ambiti a rilevanza contabile assicurano l'ordinata raccolta ed archiviazione della documentazione relativa alle verifiche effettuate;

- il CAO (Chief Accounting Officer), attraverso la sua struttura, assicura l'ordinata raccolta ed archiviazione di tutta la documentazione di supporto alla stesura del bilancio.

- Pagamenti

- l'Amministratore Delegato assicura, anche per il tramite di soggetti a ciò delegati, che le operazioni finanziarie siano effettuate in forza dei poteri di firma previsti dalle procure, a seguito di adeguata autorizzazione al pagamento come previsto dalle deleghe organizzative interne;

- nessun pagamento può essere effettuato in contanti, se non previa autorizzazione scritta dei soggetti ai quali detto potere è stato conferito e nel rispetto delle pertinenti procedure interne.

- Omaggi, sponsorizzazioni, spese di rappresentanza e erogazioni liberali[5]

- in linea generale gli omaggi destinati a privati consistono in beni di modico valore coerenti con l'attività della Società (ad esempio penne, agende, ecc.) e la loro distribuzione deve essere, per quanto possibile, pianificata ed avvenire in concomitanza con le campagne omaggi aziendali.

- Gestione dei rapporti con società del Gruppo

- i rapporti infragruppo, con specifico riferimento alle operazioni commerciali e di prestazioni di servizi concluse con altre società del Gruppo, devono essere supportati da adeguata documentazione sia contrattuale sia giustificativa della transazione commerciale e/o della prestazione di servizi, garantendone la correttezza e l'idoneità anche dal punto di vista tributario;

- la corretta contabilizzazione della spesa inerente ad un rapporto intragruppo è espressamente regolata e disciplinata da una specifica procedura interna denominata Gestione Pagamenti Intragruppo (che pertanto in questa sede si intende integralmente richiamata) che ha lo scopo di regolamentare i flussi autorizzativi legati ai pagamenti intragruppo e che prevede le seguenti regole operative che coinvolgono, a vario titolo per le rispettive competenze, le funzioni finanza, legale e SME:

  - preventiva verifica che la società emittente la fattura sia quella partner, come da apposito riepilogo annuale (forecast) predisposto dalla Società (a cui segue una comparazione a consuntivo);
  - verifica, da parte della funzione legale, della vigenza di apposito contratto che disciplini il rapporto intragruppo, anche dal punto di vista del costo sostenuto e/o dell'addebito ricevuto (*cost allocation key*);
  - verifica, da parte del *Subject Matter Expert* di riferimento, della coerenza tra prestazione ricevuta ed importo addebitato;
  - esame di eventuali giustificazioni in caso di discordanze/differenze/anomalie tra prestazione ricevuta e costo addebitato, eventualmente richiedendo – se necessario – una riduzione del costo addebitato;
  - verifica fiscale della coerenza, della competenza e dell'inerenza dell'addebito da parte del Responsabile fiscale della Società, con particolare riguardo al corretto comportamento fiscale in tema di deducibilità totale/parziale/indeducibilità del costo;
  - necessità, da parte del CAO (*Chief Accounting Officer*) dell'approvazione della registrazione in contabilità della fattura passiva e della relativa autorizzazione al pagamento da parte, congiuntamente tra loro, del CAO (*Chief Accounting Officer*) e del CFO (*Chief Financial Officer*) Italia.

- l'Ufficio Legale di Gruppo (limitatamente alla documentazione contrattuale) ed il CAO (*Chief Accounting Officer*) assicurano l'ordinata raccolta ed archiviazione di tutta la documentazione relativa ai rapporti intrattenuti con le altre società del Gruppo.

- Flussi informativi verso l'OdV

[5] Vedi Parte Speciale G del presente Modello per ulteriori chiarimenti in merito ai beni destinati a omaggi.

È opportuno fornire all'Organismo di Vigilanza gli strumenti necessari al fine di esercitare le sue attività di monitoraggio e di verifica puntuale dell'efficace esecuzione dei protocolli di controllo previsti dalla presente Parte Speciale. In allegato, il modello di riferimento adottato per tale scopo.

4. GESTIONE DEI RAPPORTI CON GLI ORGANI DI CONTROLLO (COLLEGIO SINDACALE E SOCIETA' DI REVISIONE)

4.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:

  - art. 2625 c.c. - Impedito controllo;
  - art. 2635 c.c. - Corruzione tra privati.

4.2. Principi di comportamento

I Destinatari devono:

- mantenere, nei confronti dell'attività di controllo attribuita agli organi sociali e ai soci, un comportamento corretto, trasparente e collaborativo tale da permettere agli stessi l'espletamento della loro attività istituzionale;

- fornire ai sindaci libero e tempestivo accesso ai dati ed alle informazioni richieste;

- fornire ai sindaci informazioni accurate, complete, fedeli e veritiere.

- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- porre in essere comportamenti che ostacolino lo svolgimento delle attività di controllo da parte del Collegio Sindacale, dei Soci e della Società di Revisione, mediante l'occultamento di documenti ed informazioni richiesti, ovvero fornendo documenti ed informazioni incompleti, non chiari o fuorvianti.

- corrispondere od offrire, direttamente o indirettamente, anche sotto forme diverse di aiuti o contribuzioni, pagamenti o benefici materiali alla controparte o a persone a questi vicine, per influenzare il loro comportamento ed assicurare vantaggi di qualunque tipo alla Società;

- dare seguito a richieste indebite di denaro o altri benefici provenienti da qualunque persona. In tali casi, il dipendente deve informare tempestivamente il proprio superiore e sospendere ogni rapporto d'affari con il richiedente.

4.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito dei rapporti con gli organi di controllo:

- I rapporti con il Collegio Sindacale devono essere intrattenuti da personale formalmente individuato che condivide formalmente con i sindaci i risultati delle loro verifiche.

- Tutta la documentazione consegnata ai sindaci e ai revisori deve essere preliminarmente verificata, in termini di completezza e correttezza, dal Responsabile Finance.

- Le comunicazioni rilevanti nei confronti dei sindaci e dei revisori devono avvenire in via formale (tramite e-mail) ed essere tracciabili. È necessario tenere traccia della documentazione consegnata (ad esempio, inviandogliela via e-mail e/o richiedendo una conferma e-mail dell'avvenuta ricezione).

- Tutte le verifiche svolte dai sindaci sono formalizzate nel verbale del Collegio Sindacale e le evidenze ufficiali sono archiviate a cura del Collegio stesso.

- Agli incontri di closing con la Società di Revisione devono partecipare, se possibile, almeno due esponenti aziendali espressamente autorizzati.

- Gli esiti degli incontri e delle verifiche effettuate dalla Società di Revisione devono essere adeguatamente formalizzati.

- Le attività e le decisioni concordate con gli organi societari, Collegio Sindacale e Società di Revisione, devono essere oggetto di una reportistica periodica al vertice aziendale.

5. GESTIONE DELLE OPERAZIONI SOCIETARIE STRAORDINARIE

5.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), in particolare:
  - art. 318 c.p. - Corruzione nelle sue diverse fattispecie;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
- i delitti contro la criminalità organizzata (richiamati dall'art. 24-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 416 c.p. – Associazione per delinquere
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 2621 c.c. - False comunicazioni sociali;
  - art. 2632 c.c. - Formazione fittizia del capitale;
  - art. 2629 c.c. - Operazioni in pregiudizio dei creditori;
  - art. 2635 c.c. - Corruzione tra privati.

5.2. Principi di comportamento

I Destinatari devono:

- assicurare che ogni tipo di operazione societario ordinaria o straordinaria sia condotta dalla Società nel pieno rispetto delle norme di legge o dei regolamenti applicabili;

- tenere un comportamento corretto, trasparente e collaborativo in tutte le attività finalizzate alla predisposizione di prospetti ed altre comunicazioni sociali finalizzati ad una operazione societaria, al fine di fornire ai soci ed ai terzi un'informativa veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società e dell'operazione stessa;

- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

- dare notizia, da parte di ogni amministratore, agli altri amministratori e al Collegio Sindacale di situazioni di conflitto d'interessi relative a una determinata operazione, precisandone la natura, i termini, l'origine e la portata ed astenersi dal partecipare alla relativa deliberazione;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale previsti dalla legge;

- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;

- ripartire riserve nei casi in cui ciò non sia consentito dalla legge;

- acquistare o sottoscrivere azioni della Società e/o delle sue controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;

- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;

- aumentare fittiziamente il capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;

- effettuare operazioni straordinarie in violazione delle disposizioni di legge a tutela dei creditori.

5.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle operazioni straordinarie.

- Preventivamente ad ogni operazione straordinaria deve essere effettuata:

  - una valutazione preliminare dell'operazione volta a verificarne l'opportunità, la fattibilità e la coerenza strategica;
  - un'analisi sull'identità della controparte;
  - una *due diligence*, eventualmente con il supporto di una società esterna specializzata.

- Nei contratti/lettere d'incarico stipulati con consulenti e/o collaboratori che possano supportare la Società nella gestione di operazioni societarie straordinarie deve essere inserita un'apposita clausola che preveda:

- un'espressa dichiarazione da parte del consulente e/o collaboratore di essere a conoscenza e rispettare la normativa di cui al D.Lgs. 231/2001, di non essere mai stato implicato in procedimenti giudiziari relativi a reati nello stesso contemplato e di impegnarsi al rispetto della Carta della Fiducia;
- le conseguenze per il consulente e/o collaboratore in caso di violazione di quanto dichiarato.

- Tutta la documentazione relativa alle operazioni straordinarie (tra cui, la presentazione dell'operazione, i risultati della *due diligence*, i prospetti relativi alle situazioni economico-patrimoniali) deve essere archiviata a cura della Funzione Finance.

Parte Speciale C

Gestione delle vendite di beni e servizi

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 riguardano la gestione delle vendite di beni e servizi. Nello specifico:

- gestione delle vendite intra gruppo;
- gestione delle vendite extra gruppo.

2. GESTIONE DELLA VENDITA DI BENI E SERVIZI

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
  - art. 640 c.p. - Truffa;
- i delitti di criminalità organizzata (richiamati dall'art. 24-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 416 c.p. - Associazione per delinquere;
  - art. 407, comma 2, lettera a), numero 5), c.p.p. - Illegale fabbricazione, introduzione nello stato, messa in vendita di armi da guerra o tipo guerra o parti di esse;
- i delitti contro l'industria e il commercio (richiamati dall'art. 25-*bis*.1 del D.Lgs. 231/2001), e in particolare:
  - art. 513 c.p. - Turbata libertà dell'industria o del commercio;
  - art. 515 c.p. - Frode nell'esercizio del commercio;
  - art. 517 c.p. - Vendita di prodotti industriali con segni mendaci;
  - art. 517-*ter* c.p. - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale;
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:
  - art. 2635 c.c. - Corruzione tra privati;
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n.74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 8 D.Lgs. n.74/2000 – Emissione di fatture o altri documenti per operazioni inesistenti;
  - art. 10 D.Lgs. n.74/2000 – Occultamento o distruzione di documenti contabili;
  - art. 11 D.Lgs. n. 74/2000 - Sottrazione fraudolenta al pagamento di imposte

2.2. Principi di comportamento

I Destinatari devono[6]:

- rispettare le leggi antitrust e di tutela della concorrenza;
- improntare il proprio comportamento a criteri di onestà, cortesia, trasparenza e collaborazione, fornendo informazioni adeguate e complete, evitando di incorrere in pratiche elusive o corruttive o a minacce e violenze finalizzate a influenzare il comportamento delle controparti commerciali;
- assicurare che la scelta dei Clienti avvenga a cura delle funzioni competenti, affinché siano effettuate transazioni con controparti contrattuali che possano garantire integrità, onestà ed affidabilità nella gestione dei rapporti commerciali, nonché solidità patrimoniale e finanziaria;
- assicurare che ogni operazione di vendita sia correttamente autorizzata, verificabile, legittima, coerente e congrua;
- assicurare che la definizione e applicazione dei prezzi, nonché la gestione della scontistica, sia effettuata secondo principi di correttezza, concorrenzialità e trasparenza;
- utilizzare, nei contatti formali e informali intrattenuti con le controparti commerciali, una condotta diligente e professionale in modo da fornire informazioni chiare, accurate e veritiere;
- garantire che durante l'esecuzione delle attività commerciali, anche tentate, non siano consegnati prodotti diversi da quelli richiesti / desiderati dalla controparte, ovvero che quest'ultimi non siano per origine, provenienza, qualità o quantità diversi da quanto dichiarato;
- comunicare, senza ritardo, al proprio responsabile gerarchico eventuali comportamenti posti in essere dalle controparti volti a ottenere favori, elargizioni illecite di denaro od altre utilità, anche nei confronti dei terzi, nonché qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con il Cliente o potenziale Cliente;
- compiere con diligenza tutti gli accertamenti sulle controparti commerciali relativi a:
  - i legami di qualsiasi natura con organizzazioni terroristiche o eversive dell'ordine democratico;
  - gli effettivi destinatari delle forniture e all'affidabilità del Cliente (ad esempio in termini di rispetto della normativa antiriciclaggio, di terrorismo internazionale, etc.) sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile ed indipendente;
- assicurare che la documentazione inviata o condivisa con la Pubblica Amministrazione, predisposta sia internamente che con il supporto eventuale di collaboratori/consulenti, sia completa, veritiera e corretta e le informazioni e/o dati ivi contenuti attinenti siano corretti ed esaustivi;
- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- porre in essere operazioni sospette sotto il profilo della correttezza e della trasparenza;
- dare o ricevere pagamenti indebiti e simili;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni di acquisto dei Clienti;
- divulgare materiale comunicativo destinato ai Clienti che non sia stato approvato / emesso dalle funzioni preposte nel rispetto del sistema di deleghe e procure vigente;

[6] Anche per l'attività sensibile concernente la gestione della vendita di beni o servizi si richiamano i principi di comportamento stabiliti per i rapporti con la P.A. (vedi § 2.2. e ss della Parte Speciale A).

- consegnare all'acquirente merce configurante l'ipotesi di *aliud pro alio*;
- offrire atti di cortesia commerciale (ad esempio omaggi e sconti) a soggetti terzi tali da poter ingenerare, nell'altra parte ovvero in un terzo estraneo ed imparziale, l'impressione che essi siano finalizzati ad acquisire o concedere indebiti vantaggi, ovvero tali da ingenerare comunque l'impressione di illegalità o immoralità;
- ottenere un vantaggio sleale su chiunque attraverso pratiche commerciali illecite;
- compiere atti di concorrenza sleale, e in particolare:
  - diffondere notizie e apprezzamenti sui prodotti e sull'attività di un concorrente, idonei a determinarne il discredito, o appropriarsi di pregi dei prodotti o dell'impresa di un concorrente;
  - porre in essere atti fraudolenti idonei a produrre uno sviamento della clientela altrui e un danno per le imprese concorrenti della Società;
  - realizzare qualsiasi forma di attività intimidatoria o vessatoria nei confronti di concorrenti;
  - avvalersi direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale ed idoneo a danneggiare l'altrui azienda;
  - detenere per la vendita, porre in vendita o mettere comunque in circolazione oggetti o altri beni realizzati usurpando o violando titoli di proprietà industriale;
  - porre in vendita o mettere altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi, o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità del prodotto ovvero tali da ingenerare la possibilità di confusione con prodotti similari da parte dei Clienti;
- intrattenere qualsiasi tipo di rapporto (contrattuale, finanziario, etc.) con persone o organizzazioni indicate nelle principali Black List internazionali;
- porre in essere condotte che, mediante violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, siano volte ad impedire o turbare gare pubbliche o licitazioni private per conto di pubbliche amministrazioni, ovvero ad allontanarne gli offerenti;
- porre in essere condotte che, mediante violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, siano volte a turbare il procedimento amministrativo diretto a stabilire il contenuto del bando di gare o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della Pubblica Amministrazione;
- non adempiere, anche mediante frodi, gli obblighi che derivino da un contratto di fornitura concluso con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità, facendo mancare, in tutto o in parte, cose od opere, che siano necessarie a uno stabilimento pubblico o ad un pubblico servizio.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle vendite di beni e servizi:

- <u>Gestione delle vendite infragruppo</u>

- Il prezzo di vendita per le vendite infragruppo deve rispettare la *Transfer Price Policy*.

- I contratti di service, tra la Società e le società del Gruppo, devono prevedere le modalità ed i parametri per la determinazione del prezzo e della congruità dello stesso rispetto ai riferimenti di mercato, tenuto conto dell'oggetto del contratto, e dei servizi oggetto della prestazione.

- <u>Gestione delle vendite extra gruppo</u>

- L'apertura dell'anagrafica clienti è di competenza dell'Ufficio Vendite/Commerciale, che provvede alla compilazione del modulo "*Anagrafica Cliente*" inserendo le informazioni generali del cliente (dati anagrafici, partita iva, contatti, termini di pagamento, *incoterms*, valuta, area manager di riferimento, il *customer service* di riferimento, regione di appartenenza, gruppo di clienti) e lo invia per conoscenza alla Funzione Finance.

- In fase di codifica, l'Ufficio Vendite/Commerciale, a seconda del Paese di appartenenza del cliente, svolge verifiche con l'ausilio della funzione *Trade Compliance*.

- I rapporti commerciali con i clienti devono essere formalizzati in appositi contratti. In mancanza di questi sono da considerarsi vincolanti l'offerta commerciale, la conferma d'ordine e le condizioni generali di vendita.

- Qualsiasi modifica alle condizioni generali di vendita deve essere preventivamente validata dalla Funzione Legal.

- I contratti di vendita devono riportare:

  - clausole contrattuali standardizzate in relazione alla natura e alla tipologia di contratto, ivi incluse previsioni contrattuali finalizzate all'osservanza di principi di controllo/regole etiche nella gestione delle attività commerciali;

  - un'espressa dichiarazione della controparte di essere a conoscenza e rispettare la normativa di cui al D.Lgs. 231/2001 e di impegnarsi al rispetto della Carta della Fiducia adottata dalla Società;

  - la possibilità di risolvere il contratto in caso di violazione di quanto dichiarato.

- I listini prezzi definiti per prodotto sono caricati a sistema previa formale condivisione con la Direzione Vendite e l'Amministratore Delegato.

- La definizione dei prezzi deve basarsi su criteri e modalità che ne garantiscano l'allineamento ai riferimenti di mercato.

- La scontistica deve essere definita dall'Ufficio Commerciale. Eventuali extra sconti devono essere autorizzati dal Sales Director.

- Periodicamente devono essere sottoposti a monitoraggio (a titolo esemplificativo mediante un report *ad hoc*) eventuali modifiche ai prezzi dei prodotti che evidenziano marginalità potenzialmente sospette.

- Gli ordini dei clienti si devono ricevere per iscritto, salvo casi particolari (a titolo esemplificativo per clienti noti e/o per ordini ripetitivi) al verificarsi dei quali sono ammissibili ordini telefonici.

- L'Ufficio Vendite è tenuto a verificare gli ordini (nome prodotto, prezzo, condizioni di pagamento, date di consegna, istruzioni di consegna), ad inserirli a sistema ed a emettere la conferma d'ordine.

- In fase di spedizione della merce è compito dell'Ufficio Spedizioni allegare la *packing list*, i documenti fiscali ed altri eventuali documenti/dichiarazioni/attestati di conformità.

- L'Ufficio Spedizioni è responsabile di accertare che imballaggi, etichette e documenti di spedizione siano quelli riportati nell'ordine di acquisto del cliente.

- L'Ufficio Spedizioni deve verificare che il trasportatore sigli il documento di trasporto che accompagna le merci.

Parte Speciale D

Gestione del personale

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito dei processi relativi alla gestione del personale sono:

- selezione e assunzione del personale;

- gestione amministrativa del personale;

- gestione dei rapporti con le rappresentanze sindacali.

2. SELEZIONE, ASSUNZIONE DEL PERSONALE E PERCORSI DI CARRIERA

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
  - art. 640 c.p. – Truffa

2.2. Principi di comportamento

I Destinatari devono:

- rispettare le normative a tutela dei lavoratori e in materia di immigrazione vigenti (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, ecc.);

- operare nel rispetto del criterio di meritocrazia in relazione alle reali esigenze della Società;

- effettuare attività di selezione e assunzione per accertate necessità aziendali ed atte a garantire che la scelta dei candidati sia effettuata sulla base delle valutazioni di idoneità tecnica e attitudinale. L'attività deve avvenire nel rigoroso rispetto delle procedure aziendali ed essere ispirata a criteri di trasparenza, nella valutazione dei requisiti di competenza e professionalità, di capacità e potenzialità individuale;

- garantire la tracciabilità delle procedure di selezione e assunzione e la corretta archiviazione della documentazione attestante il loro corretto svolgimento;

- assicurare che l'assunzione del personale avvenga sulla base di regolari contratti di lavoro, non essendo ammessa alcuna forma di rapporto lavorativo non conforme o comunque elusiva delle disposizioni normative vigenti;

- verificare preventivamente le informazioni disponibili sui candidati al fine di instaurare rapporti unicamente con soggetti che godano di buona reputazione, che siano impegnati solo in attività lecite e la cui cultura etica sia comparabile a quella della Società;

- provvedere affinché gli adempimenti obbligatori previsti in caso di assunzione del personale siano predisposti con la massima diligenza e professionalità, in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere e i rapporti con i Funzionari Pubblici siano improntati alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del ruolo istituzionale;

- garantire che eventuali variazioni retributive siano concesse sulla base di criteri meritocratici e/o di anzianità;

- curare che siano assicurate all'interno della Società condizioni di lavoro rispettose della dignità personale, delle pari opportunità e un ambiente di lavoro adeguato;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- operare secondo logiche di favoritismo;

- promettere o concedere promesse di assunzione / avanzamenti di carriera / aumenti retributivi / benefit / bonus a risorse vicine o gradite a funzionari pubblici o a qualsiasi soggetto terzo privato con cui la Società si relaziona quando questo non sia conforme alle reali esigenze dell'azienda e non rispetti il principio della meritocrazia;

- assumere personale, anche per contratti temporanei, senza il rispetto delle normative vigenti in materia (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, etc.);

- assumere o impiegare lavoratori minorenni o lavoratori stranieri privi di permessi di soggiorno, ovvero il cui permesso sia scaduto - e per il quale non si sia richiesto il rinnovo - revocato o annullato;

- assumere o promettere l'assunzione ad impiegati della Pubblica Amministrazione o a qualsiasi soggetto terzo privato (o loro parenti, affini, amici, ecc.) che abbiano partecipato personalmente e attivamente a una trattativa d'affari ovvero ad impiegati della Pubblica Amministrazione (o loro parenti, affini, amici, ecc.) che abbiano partecipato, anche individualmente, a processi autorizzativi della P.A. o ad atti ispettivi, nei confronti della Società;

- esporre nella documentazione inviata o condivisa con la Pubblica Amministrazione fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle attività relative alla selezione e assunzione del personale:

- Ricerca, selezione e assunzione del personale

- In caso di fabbisogno di personale il Responsabile di Linea invia, all'Amministratore Delegato e all'HR Business Partner, una richiesta di personale attraverso un Sistema Informativo e l'approvazione della stessa è necessaria per avviare il processo di selezione.

- In caso di valutazione positiva della richiesta di personale, l'HR Business Partner, congiuntamente all'Amministratore Delegato ed al Responsabile di Linea, analizzano i contenuti della posizione ricercata e le principali competenze richieste e definiscono una *job description*.

- L'HR Business Partner, con il supporto del Dipartimento di Talent Acquisition della capo gruppo in Italia, la Schneider Electric SpA, avvia l'iter di ricerca interno alla Società e/o al Gruppo. Nel caso in cui non sia possibile identificare una potenziale promozione interna, è prevista l'attivazione di una fase di ricerca esterna ove necessario anche con il supporto di società di *head hunting*, per la raccolta di candidature.

- L'HR Business Partner, con il supporto del Dipartimento di Talent Acquisition della capo gruppo in Italia, effettua una prima scrematura dei curricula raccolti, devono essere almeno due, inviando una richiesta di colloquio ai candidati giudicati in linea con la posizione aperta.

- L'HR Business Partner, con il supporto del Dipartimento di Talent Acquisition della capo gruppo in Italia, effettua un primo colloquio conoscitivo con il candidato e gli sottopone il questionario informativo e i documenti rilevanti in materia di privacy.

- Successivamente, il Responsabile di Linea, congiuntamente all'Amministratore Delegato ed all'HR Business Partner, effettua un secondo colloquio di natura tecnica con il candidato.

- Le risultanze dei colloqui sono tracciate all'interno di un'apposita scheda di valutazione nella quale sono riportate le considerazioni e valutazioni effettuate in merito al candidato.

- Terminata la fase di selezione, ove si ritenga di aver individuato un candidato che risponda al profilo ricercato, l'Amministratore Delegato, congiuntamente con l'HR Business Partner, predispone una proposta economica, coerente con i minimi tabellari e i livelli di mercato di riferimento, e le condizioni di assunzione.

- Al fine di procedere a nuove assunzioni di personale, devono essere svolte verifiche pre-assuntive finalizzate a prevenire l'insorgere di situazioni pregiudizievoli che espongano la Società al rischio di commissione di reati presupposto in tema di responsabilità amministrativa d'impresa; ed in particolare deve essere:

  - verificato, nel caso in cui il processo di selezione e assunzione riguardi lavoratori stranieri, che il candidato sia in possesso di documenti di soggiorno validi.

- All'interno dei contratti di assunzione deve essere prevista una specifica clausola in forza della quale il neoassunto dichiara di essere a conoscenza e rispettare la normativa di cui al D.Lgs. 231/2001 e di impegnarsi al rispetto della carta della Fiducia e del Modello adottato dalla Società.

- L'Amministratore Delegato, congiuntamente con l'HR Business Partner, deve verificare la bozza di contratto di assunzione predisposta dal personale competente sulla base degli standard in essere e, in ogni caso, i contratti di assunzione devono essere sottoposti all'approvazione di soggetto dotato di idonei poteri sulla base del sistema di deleghe e procure in vigore.

- l'ufficio dell'amministrazione del personale della capo gruppo In Italia (HR Services) invia al futuro dipendente la checklist dei documenti da produrre in fase di assunzione, a titolo esemplificativo la autocertificazione del titolo di studio, il certificato attestante lo stato di famiglia e di residenza, il codice fiscale, la carta d'identità, il codice iban, l'eventuale iscrizione alle liste di mobilità, il permesso di soggiorno.

- Per ciascun neoassunto, l'Amministratore Delegato, di concerto con il Responsabile di Linea, definisce un piano di inserimento che specifica gli obiettivi del lavoro, i comportamenti attesi, le indicazioni operative necessarie per lo svolgimento delle mansioni ed il piano formativo.

- In relazione al personale appartenente a categorie protette, l'ufficio dell'amministrazione del personale della capo gruppo in Italia (HR Services), deve verificare eventuali scoperti monitorando il rispetto dei requisiti e soglie di legge al fine di determinare eventuali fabbisogni.

- In relazione ai rapporti di lavoro con dipendenti e collaboratori provenienti da Paesi extra CEE devono essere inseriti in apposito scadenziario i dettagli anagrafici e la durata del permesso di soggiorno.

- L'ufficio dell'amministrazione del personale della capo gruppo in Italia (HR Services), deve monitorare periodicamente, mediante specifico scadenziario, la regolarità dei permessi di soggiorno / carta di soggiorno dei lavoratori stranieri in forza presso la Società.

- In caso di scadenza il personale richiede alla risorsa, con adeguato anticipo, di provvedere al rinnovo dei permessi, salvo impossibilità a proseguire nel rapporto di lavoro.

- In relazione ai contratti di somministrazione di lavoro, d'opera o di appalto la Direzione Risorse Umane deve verificare il rispetto delle norme di legge in materia.

- Tutta la documentazione rilevante (i.e. CV, moduli interviste, contratti di assunzione, etc.) nell'ambito del processo di selezione e assunzione (anche per ciò che concerne il personale appartenente a categorie protette) deve essere debitamente archiviata presso la Direzione Risorse Umane della capo gruppo.

- <u>Valutazione delle prestazioni del personale</u>

- Annualmente, per ogni dipendente, viene definito, dall'Amministratore Delegato, congiuntamente con il Responsabile di linea e l'HR Business Partner, il piano di performance e di sviluppo delle competenze.

- Gli obiettivi attesi ed il piano di sviluppo devono essere debitamente formalizzati e tracciabili (a titolo esemplificativo mediante TalentLink).

- Il raggiungimento degli obiettivi viene valutato dall'Amministratore Delegato, congiuntamente con il Responsabile di Linea nel rispetto di principi di meritocrazia, integrità e professionalità.

- Il riconoscimento degli incentivi, che si sostanzia nel riconoscimento di una parte variabile della retribuzione, è subordinato al raggiungimento degli obiettivi definiti all'interno dello Short Term Incentive Plan.

- Gli aumenti salariali dei dipendenti sono normati da apposite Linee Guida, contenenti per ciascun livello contrattuale del CCNL applicato il livello minino e massimo di aumento (espresso in termini di percentuale rispetto alla RAL media).

3. GESTIONE AMMINISTRATIVA DEL PERSONALE

3.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
  - art. 640 c.p. - Truffa;
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:
  - art. 2621 c.c. - False comunicazioni sociali;
  - art. 2635 c.c. - Corruzione tra privati.

3.2. Principi di comportamento

I Destinatari devono:

- provvedere affinché gli adempimenti obbligatori previsti in relazione alla gestione amministrativa del personale, siano predisposti con la massima diligenza e professionalità, in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere e i rapporti con i Funzionari Pubblici siano improntati alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del ruolo istituzionale;
- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- inserire, nell'anagrafica del personale, dipendenti fittizi allo scopo di creare disponibilità extracontabili o per ottenere agevolazioni di qualsivoglia natura;

- esporre nella documentazione inviata o condivisa con la Pubblica Amministrazione fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società.

3.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione amministrativa del personale:

- L'inserimento / modifica dell'anagrafica dipendenti nel relativo sistema informativo (Talent Link interfacciato con Infinity Zucchetti) è affidata alla Direzione Risorse Umane della capo gruppo, dotata di adeguato "profilo" di accesso.

- In fase di creazione/modifiche dell'anagrafica dipendenti la Direzione Risorse Umane della capo gruppo provvede a verificare la corretta trasposizione dei dati tra gli applicativi rilevanti: Talent Link (data base amministrativo), Infinity Zucchetti (sistema paghe e presenze).

- Il personale competente della Direzione Risorse Umane della capo gruppo effettua, con cadenza periodica, una sistematica revisione dell'anagrafica dipendenti ai fini della corretta gestione amministrativa del personale.

- La rilevazione delle presenze del personale dipendente è effettuata mediante sistema di timbratura, normato dal CCNL applicato e/o inserimento manuale delle presenze nel sistema Infinity Zucchetti (ad es. nel caso di lavoro agile).

- Il personale competente della Direzione Risorse Umane della capo gruppo scarica mensilmente le timbrature dal sistema (Infinity Zucchetti) ed effettua una prima verifica dei dati contenuti nel file di rilevazione presenze al fine di intercettare eventuali anomalie nel cartellino dei dipendenti.

- Mensilmente, in occasione dell'elaborazione dei cedolini, il personale autorizzato della Direzione Risorse Umane della capo gruppo verifica la risultanza dell'elaborazione dei cedolini fatta dal sistema Infinity Zucchetti.

- L'HR Service Manager Italy della capo gruppo o personale da questi delegato, provvede all'elaborazione dei cedolini relativi agli stipendi e dei Modelli F24 per il versamento dei contributi e delle ritenute fiscali.

- L'HR Service Manager Italy della capo gruppo prima della formale liquidazione degli stipendi verifica, per tutti i dipendenti, che le retribuzioni fisse da riportare all'interno del cedolino di competenza, siano in linea con quelle del mese precedente. In caso di scostamenti significativi è svolta una verifica interna per validare l'ammontare.

- Il pagamento degli stipendi e dei Modelli F24 deve essere autorizzato da soggetti dotati di idonei poteri sulla base del sistema di deleghe e procure in vigore.

- Il personale competente della Funzione Finance provvede a imputare in contabilità i dati relativi al costo del personale e ad effettuare i controlli di quadratura.

- Tutta la documentazione relativa al personale deve essere debitamente archiviata, all'interno della cartella del dipendente e/o in appositi database elettronici curati dalla Direzione Risorse Umane della capo gruppo.

- Tutta la documentazione rilevante deve essere debitamente archiviata presso la Direzione / Funzione aziendale competente.

4. GESTIONE DEI RAPPORTI CON LE RAPPRESENTANZE SINDACALI

4.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:

  - art. 2635 c.c. - Corruzione tra privati.

4.2. Principi di comportamento

I Destinatari devono:

- intrattenere rapporti corretti, trasparenti, imparziali e collaborativi con i rappresentanti delle organizzazioni sindacali;

- astenersi dall'influenzare impropriamente l'attività dei rappresentanti delle organizzazioni sindacali in occasione delle contrattazioni con esse intraprese e nello svolgimento di qualsiasi altra attività che preveda un loro coinvolgimento;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- corrispondere o offrire, direttamente o indirettamente, anche sotto forme diverse di aiuti o contribuzioni (ad esempio sponsorizzazioni e liberalità), pagamenti o benefici materiali a rappresentanti delle organizzazioni sindacali o a persone a questi vicini, per influenzare il loro comportamento ed assicurare vantaggi di qualunque tipo alla Società.

4.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito dei rapporti con le rappresentanze sindacali, preso atto che gli stessi sono applicati dalla Direzione Risorse Umane della capo gruppo, a cui si fa espresso rinvio in tema dei seguenti principi:

- I rapporti sindacali devono essere gestiti in linea con quanto previsto dal sistema di deleghe e procure in vigore.

- Agli incontri con i rappresentanti sindacali devono partecipare almeno due persone.

- Le riunioni con le rappresentanze sindacali devono essere documentate in appositi verbali divulgati tra i partecipanti.

- Gli accordi sindacali devono essere firmati da soggetti dotati di idonei poteri, in linea con il sistema di deleghe e procure vigente.

- Tutta la documentazione rilevante deve essere archiviata presso la presso la Direzione / Funzione aziendale competente.

Parte Speciale E

Gestione degli acquisti di beni e servizi

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito dei processi relativi alla gestione degli acquisti, riguardano sia quelli diretti sia quelli indiretti.

2. GESTIONE DEGLI ACQUISTI

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i delitti contro la criminalità organizzata (richiamati dall'art. 24-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 416 c.p. – Associazione per delinquere
- i reati contro la Pubblica Amministrazione (richiamati dall'art. 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
- i delitti contro l'industria e il commercio (richiamati dall'art. 25-*bis*.1 del D.Lgs. 231/2001), e in particolare:
  - art. 517-*ter* c.p. - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale;
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), ed in particolare:
  - art. 2621 c.c. False comunicazioni sociali;
  - art. 2635 c.c. Corruzione tra privati;
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 10 D.Lgs. n. 74/2000 – Occultamento o distruzione di documenti contabili;

2.2. Principi di comportamento

I Destinatari devono:

- ispirarsi al principio per cui la scelta dei fornitori, siano essi persone fisiche o giuridiche, avvenga a cura delle funzioni aziendali competenti e sia effettuata sulla base di requisiti di qualità, professionalità, affidabilità ed economicità;

- evitare nella conduzione di qualsiasi trattativa situazioni nelle quali i soggetti coinvolti siano o possano apparire in conflitto di interesse;

- instaurare rapporti unicamente con soggetti che godano di una reputazione rispettabile, che siano impegnati solo in attività lecite e la cui cultura etica aziendale sia comparabile a quella della Società. A tale fine, i Destinatari coinvolti nella gestione dei rapporti con i fornitori sono tenuti a verificare preventivamente le informazioni disponibili sui soggetti stessi;

- assicurare la trasparenza degli accordi ed evitare la sottoscrizione di patti o accordi segreti contrari alla legge;

- rispettare principi di trasparenza, motivazione e non discriminazione nella scelta della controparte contrattuale;

- scegliere, ove possibile, tra una rosa di potenziali fornitori, quello che garantisca il miglior rapporto tra qualità e convenienza;

- accertarsi dell'identità della controparte, sia essa persona fisica o giuridica, e dei soggetti per conto dei quali essa eventualmente agisce e verificare l'eticità e la solidità patrimoniale e finanziaria della controparte contrattuale;

- garantire che eventuali incarichi affidati a soggetti terzi per operare in rappresentanza e/o nell'interesse della Società siano sempre assegnati in forma scritta richiedendo eventualmente, anche tramite specifiche clausole contrattuali, alle controparti il rispetto dei principi comportamentali previsti dalla Carta della Fiducia;

- verificare l'effettivo adempimento della prestazione oggetto del rapporto contrattuale e degli eventuali stati di avanzamento prima del pagamento del prezzo concordato;

- effettuare, ove possibile, controlli specifici in presenza di offerte di fornitura di beni a prezzi significativamente inferiori a quelli di mercato, volti ad appurare l'effettiva provenienza della merce;

- consentire la tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte;

- liquidare i compensi in modo trasparente, sempre documentabile e ricostruibile *ex post;*

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente <u>vietato:</u>

- effettuare acquisti che non trovino riscontro in una specifica e motivabile esigenza della Società;

- assegnare incarichi a controparti "vicine" o "gradite" a soggetti pubblici o a qualsiasi soggetto terzo privato con cui la Società si relaziona in assenza dei necessari requisiti di qualità e convenienza dell'operazione;

- instaurare rapporti o porre in essere operazioni con soggetti terzi qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione dei reati di associazione per delinquere, ricettazione, riciclaggio o impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;

- corrispondere, promettere od offrire, direttamente o indirettamente, pagamenti impropri o altre utilità non dovute a rappresentanti di fornitori / potenziali fornitori, o a persone a questi vicini, con la finalità di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;

- approvare contratti / lettere d'incarico / ordini di acquisto a fronte di approvvigionamenti in tutto o in parte fittizi e/o non necessari e/o a prezzi non allineati a quelli di mercato, allo scopo di impiegare, trasferire, sostituire o occultare disponibilità finanziarie di provenienza illecita;

- effettuare pagamenti in favore di controparti che operino per conto della Società, in assenza di adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e delle prestazioni effettuate;

- riconoscere rimborsi spese in favore di controparti contrattuali che non trovino adeguata giustificazione in relazione al tipo di incarico svolto;

- frazionare artificiosamente un'operazione / transazione di acquisto al fine di eludere le normative applicabili;

- accettare fatture a fronte di operazioni inesistenti;

- creare fondi patrimoniali extra-contabili a fronte di operazioni contrattualizzate a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;

- avvalersi di fornitori coinvolti in attività di sfruttamento del lavoro minorile, procacciamento illegale della forza lavoro attraverso il traffico di migranti e/o la tratta degli schiavi o in qualsiasi altra attività che possa violare gli obblighi di legge in tema di lavoro, condizioni igienico sanitarie e di sicurezza, diritti sindacali o di associazione e rappresentanza;

- farsi rappresentare da soggetti terzi quando si possano creare situazioni di conflitto d'interesse.

2.3. Presidi di controllo

Con riguardo ai presidi di controllo, che devono essere posti in essere nell'ambito della gestione degli acquisti di beni e di servizi, è opportuno prendere visione delle procedure aziendali e dei livelli autorizzativi disciplinati all'interno della *Chart of Approval*.

Parte Speciale F

Gestione del marketing prodotto

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito dei processi relativi alla gestione degli acquisti sono la gestione dello sviluppo prodotto.

2. GESTIONE DELLO SVILUPPO PRODOTTO

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- reati di falsità in monete, in carte di pubblico credito, in valori bollati e in strumenti o segni di riconoscimento (richiamati dall'art. 25-*bis* del D.Lgs 231/2001), in particolare:
  - art. 473 c.p. - Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali;
- i delitti contro l'industria e il commercio (richiamati dall'art. 25-*bis*.1 del D.Lgs. 231/2001), e in particolare:
  - art. 473 c.p. - Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali;
  - art. 517-*ter* c.p. - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale.

2.2. Principi di comportamento

I Destinatari devono:

- garantire la *compliance* dei prodotti commercializzati dalla Società alle normative di legge applicabili;

- garantire la coerenza delle attività di gestione dell'*Intellectual Property* rispetto alle disposizioni di legge vigenti in materia, la corretta definizione dei ruoli e delle responsabilità in relazione allo sviluppo e gestione del prodotto, nonché il corretto utilizzo di ideazioni ed elaborazioni di cui la Società ha diritto all'uso;

- utilizzare esclusivamente ideazioni o elaborazioni creative (quali, a solo titolo esemplificativo, i disegni industriali dei prodotti, etc.) di cui la Società ha esclusiva proprietà o diritto all'uso in forza di compensi pattuiti con terzi;

- utilizzare marchi di esclusiva proprietà e/o il cui utilizzo rientra nella disponibilità della Società attraverso un legittimo titolo all'uso;

- adottare adeguate misure di manleva per qualsiasi rivendicazione, azione legale e richiesta di risarcimento eventualmente avanzata da terzi, dovuta alla violazione di brevetti o di richieste di brevetto, di marchi o di modelli depositati e di diritti di proprietà industriale e intellettuale relativi a prodotti/servizi acquistati da terzi;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- contraffare, alterare o usare marchi o segni distintivi, nonché brevetti, disegni o modelli industriali, nazionali o esteri, di prodotti o servizi, con riferimento ai quali, con ordinaria e qualificata diligenza, si possa conoscere l'esistenza di altrui titoli di proprietà industriale;

- progettare oggetti o altri beni usurpando o violando titoli di proprietà industriale, potendo conoscerne l'esistenza con ordinaria e qualificata diligenza;

- usare nomi o segni distintivi idonei a produrre confusione con nomi o segni distintivi legittimamente usati da altri, o imitare servilmente i prodotti di un concorrente, o compiere con qualsiasi altro mezzo, atti idonei a creare confusione con i prodotti e con l'attività di un concorrente;

- contraffare, alterare, ovvero fare uso di beni di qualsiasi genere aventi marchi o titoli industriali contraffatti al fine di rendere un danno alle ditte produttrici;

- porre in essere qualsiasi atto dispositivo e/o di utilizzazione, in qualsiasi forma o modalità, di opere dell'ingegno di cui la Società non detenga esclusiva proprietà e/o legittimo titolo all'uso;

- intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuto o sospettato lo svolgimento di attività illecite con riferimento alle fattispecie di reato di cui all'art. 25-*bis* in materia di marchi, brevetti e segni distintivi;

- nel caso in cui, in ragione del proprio stato o attività professionale, si sia venuti a conoscenza di notizie destinate a rimanere segrete relativamente a scoperte o invenzioni scientifiche o applicazioni industriali di terze parti, utilizzare tali notizie al fine di ottenere un indebito vantaggio per la Società.

2.3. Presidi di controllo

Con riferimento ai presidi di controllo, che devono essere posti in essere nell'ambito della gestione dello sviluppo prodotto, è opportuno prendere visione delle procedure aziendali e dei livelli autorizzativi disciplinati all'interno della *Chart of Approval*.

Inoltre, con riguardo ai contratti conclusi con i professionisti e con i fornitori, questi devono prevedere specifiche clausole contenenti l'impegno della controparte:

- di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni, modelli od opere tutelate dal diritto d'autore oggetto di cessione ovvero di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
- che i diritti di utilizzo e/o di sfruttamento delle privative industriali e/o intellettuali, oggetto di cessione o di concessione in uso, non violano alcun diritto di proprietà industriale/ intellettuale in capo a terzi;
- a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio dovesse derivarle per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

Parte Speciale G

Gestione degli omaggi, delle liberalità e delle sponsorizzazioni

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 riguardano la gestione degli omaggi, delle liberalità e delle sponsorizzazioni.

2. GESTIONE DEGLI OMAGGI, DELLE LIBERALITA' [7] E DELLE SPONSORIZZAZIONI [8]

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i reati contro la Pubblica Amministrazione (richiamati dall'art. 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:
  - art. 2621 c.c. – False comunicazioni sociali;
  - art. 2635 c.c. – Corruzione tra privati;
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 10 D.Lgs. n. 74/2000 – Occultamento o distruzione di documenti contabili.

2.2. Principi di comportamento

I Destinatari devono:

- garantire che tutte le liberalità/sponsorizzazioni siano debitamente autorizzate nel rispetto del sistema di procure in vigore e secondo le soglie di valore definite, tracciate e verificabili;

- effettuare erogazioni sotto forma di liberalità unicamente per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Società;

[7] Per liberalità si intendono erogazioni liberali in denaro / donazioni di beni materiali a terzi non strettamente legati ad un ritorno di immagine o ad altra utilità per la Società.

[8] Per sponsorizzazioni si intendono, ad esempio, accordi che prevedano pubblicità in cambio dell'impegno a finanziare un ente o un evento.

- nel selezionare le iniziative da sostenere, operare con estrema attenzione al fine di evitare ogni possibile situazione di conflitto di interesse;

- assicurarsi che il valore, la natura e lo scopo di liberalità/sponsorizzazioni siano considerati legali ed eticamente corretti, tali da non compromettere l'immagine della Società ovvero non siano interpretati come un mezzo per ottenere trattamenti di favore per la stessa;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- promettere o offrire liberalità/sponsorizzazioni, anche sotto pressione psicologica o coercizione, anche se indirettamente, per tramite di interposta persona, a soggetti appartenenti alla Pubblica Amministrazione o controparti private o a soggetti da questi segnalati con la finalità, anche implicita, di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;

- elargire liberalità/sponsorizzazioni che possano essere interpretate come eccedenti le normali pratiche commerciali o di cortesia;

- erogare liberalità/sponsorizzazioni qualora vi sia il fondato sospetto che ciò possa esporre la Società al rischio di commissione di uno dei reati disciplinati dal D.Lgs. 231/2001;

- accettare, anche in occasioni di festività, per sé o per altri, omaggi o altre utilità, ad eccezione dei regali d'uso di modico valore e/o ascrivibili a normali corretti rapporti di cortesia, tali da **non** compromettere l'integrità o la reputazione di una delle parti né da poter essere interpretati, da un osservatore imparziale, come finalizzati ad acquisire vantaggi indebiti e/o in modo improprio.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle liberalità e sponsorizzazioni:

- la concessione di liberalità e sponsorizzazioni è regolata dai livelli autorizzativi individuati dalla *Chart of Approval (CoA)*.

- deve essere garantita la tracciabilità delle liberalità e delle sponsorizzazioni concesse attraverso la compilazione di apposito registro che dettagli, fra le altre:

  - quantità, descrizione e valore degli articoli;
  - persona concedente la liberalità/sponsorizzazione;
  - dati identificativi del destinatario (nome e cognome).

- il predetto registro è monitorato al fine di identificare eventuali anomalie (a titolo di esempio, più liberalità verso lo stesso soggetto*)* e conseguentemente porre in essere le relative azioni correttive.

- in linea generale gli omaggi destinati a privati consistono in beni di modico valore coerenti con l'attività della Società (ad esempio penne, agende, ecc.) e la loro distribuzione deve essere, per quanto possibile, pianificata ed avvenire in concomitanza con le campagne omaggi aziendali. La procedura di assegnazione dei beni da destinare a omaggi deve rispettare la pertinente procedura interna i cui contenuti devono intendersi qui integralmente richiamati e trascritti;

- gli omaggi, eccedenti i limiti di valore indicati nella pertinente procedura interna e/o che esulino dalle campagne omaggi, devono essere espressamente approvati dal Responsabile della Funzione richiedente e dall'Amministratore Delegato;

- il Responsabile Commerciale assicura l'ordinata raccolta ed archiviazione della documentazione relativa agli omaggi destinati ai clienti e ai fornitori;

- le spese di rappresentanza sono consentite nei limiti in proposito definiti nella pertinente procedura interna e la relativa richiesta di rimborso deve essere accompagnata da idonea documentazione giustificativa, con indicazione del motivo della spesa, dei nominativi degli ospiti e della società od ente al quale essi appartengono. L'Ufficio Amministrazione assicura l'ordinata raccolta ed archiviazione delle registrazioni contabili relative alle spese di rappresentanza e delle corrispondenti pezze giustificative;

- le spese di rappresentanza eccedenti i limiti di valore indicati nella pertinente procedura interna devono essere preventivamente ed espressamente autorizzate dal Responsabile della funzione richiedente e dall'Amministratore Delegato;

- le sponsorizzazioni e, più in generale, le attività promozionali sono ammesse esclusivamente al fine di promuove il brand e/o l'immagine della Società, le quali devono essere debitamente autorizzate dal Responsabile della Funzione Marketing di Gruppo o, nei casi previsti dalla pertinente procedura interna, dall'Amministratore Delegato e dall'Ufficio Legale di Gruppo;

- le sponsorizzazioni e, più in generale, le attività promozionali devono in ogni caso essere riferite ad un apposito accordo scritto approvato in via preventiva dall'Ufficio Legale di Gruppo;

- le erogazioni liberali sono ammesse esclusivamente in favore di enti, associazioni, comitati privi di scopo di lucro e devono essere preventivamente autorizzate dal Responsabile della Funzione interessata o dall'Amministratore Delegato, in conformità a quanto in proposito previsto dalla pertinente procedura interna;

- le erogazioni liberali devono, per quanto possibile, essere effettuate in natura;

- il soggetto che autorizza la singola erogazione liberale assicura l'ordinata raccolta ed archiviazione di tutta la relativa documentazione. Qualora l'impegno della Società si traduca in un esborso di denaro, la relativa corresponsione deve avvenire a mezzo bonifico bancario o altro mezzo equipollente, previa ricezione di regolare documentazione fiscale. In tal caso, l'Ufficio Amministrazione assicura l'ordinata raccolta ed archiviazione della documentazione relativa all'operazione.

Parte Speciale H

Gestione della tesoreria e dei rimborsi spese

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 riguardano la gestione della tesoreria e dei rimborsi spese. Nello specifico:

- gestione della cassa e dei rimborsi spese;

- gestione delle operazioni bancarie e dei rapporti con gli istituti di credito;

- gestione degli incassi e pagamenti.

2. GESTIONE DELLA CASSA E DEI RIMBORSI SPESE

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i delitti contro la criminalità organizzata (richiamati dall'art. 24-*ter* del D.Lgs. 231/2001);
- i reati contro la Pubblica Amministrazione (richiamati dall'art. 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:
  - art. 2621 c.c. – False comunicazioni sociali;
  - art. 2635 c.c. - Corruzione tra privati;
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante altri artifici

2.2. Principi di comportamento

I Destinatari devono:

- utilizzare le disponibilità di cassa in modo appropriato, nei limiti delle necessità aziendali e comunque per importi di modico valore;

- operare nel rispetto della normativa vigente, con particolare riferimento alla gestione di strumenti di pagamento, tracciabilità dei flussi finanziari e antiriciclaggio;

- consentire la tracciabilità dell'iter decisionale e autorizzativo e delle attività di controllo svolte all'interno del processo di gestione dei rimborsi spese;

- utilizzare le modalità e i mezzi di pagamento consentiti dalle prassi e dalle procedure interne;

- gestire l'autorizzazione e il controllo delle trasferte secondo criteri di economicità e di massima trasparenza, nel rispetto della regolamentazione interna e delle leggi e normative fiscali vigenti;

- richiedere / riconoscere il rimborso delle sole spese sostenute per motivi di lavoro;

- garantire l'erogazione di rimborsi spese solo a fronte dell'esibizione da parte del richiedente di appropriati giustificativi di spesa;

- consentire la tracciabilità dell'iter autorizzativo delle trasferte e delle attività di controllo svolte;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- effettuare pagamenti per cassa, eccetto per particolari tipologie di acquisto, e comunque per importi rilevanti;

- riconoscere rimborsi spese in favore di dipendenti, collaboratori o terzi che non trovino adeguata giustificazione in relazione al tipo di incarico svolto o in assenza di idonea documentazione giustificativa;

- creare fondi a fronte di rimborsi spese inesistenti in tutto o in parte.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione della cassa e dei rimborsi spese:

- Gestione della cassa

- Il cassiere è responsabile della gestione della piccola cassa.

- L'ammontare dei valori in cassa non deve superare la soglia individuata all'interno dell'apposita procedura in materia.

- Il cassiere deve provvedere alla registrazione a sistema dei movimenti di cassa e all'aggiornamento del registro cartaceo, riportante tutte le transazioni, per ciascuna delle quali devono essere specificati: la data, l'importo, il saldo dare e avere in partita doppia, il numero di fattura (se presente), il fornitore.

- Mensilmente il cassiere deve eseguire una riconciliazione tra il saldo della cassa riportato a sistema (in contabilità generale) e i valori effettivamente presenti nella cassa della Società.

- Le riconciliazioni eseguite dal cassiere devono essere verificate mensilmente da una risorsa, individuata mediante delega formale.

- Il reintegro del denaro contante, contenuto nella cassa della Società, è ammesso per un importo massimo di 2.000 € a settimana. Il reintegro di contanti deve avvenire tramite richiesta alla banca a mezzo lettera o attraverso il versamento di un assegno bancario o relativo deposito del contante presso la cassa. La lettera o l'assegno da versare devono essere firmati dalle persone autorizzate.

- Gestione dei rimborsi spese

- La gestione dei rimborsi spese è amministrata mediante il tool *Concur di Gruppo*.

- Le tipologie di spese non rimborsabili (quali a titolo meramente esemplificativo: pay tv, consumo di alcolici) sono formalmente definite e portate a conoscenza di tutto il personale della Società.

- La Società corrisponde al personale fuori sede il rimborso delle spese di trasferta sostenute per l'espletamento del servizio, tramite la compilazione del "*Report Nota Spese"*.

- Il dipendente, durante la compilazione della nota spese, deve indicare tutti i costi inerenti la trasferta per i quali viene richiesto il rimborso e allegare elettronicamente (mediante pdf) i giustificativi a supporto.

- Il responsabile di funzione deve approvare la nota spese del dipendente effettuando il controllo di merito tra gli importi indicati nel "*Report Nota Spese"* ed i relativi giustificativi.

- La notifica di richiesta di approvazione si genera automaticamente a seguito della chiusura del "*Report Nota Spese"* da parte del dipendente.

- Nel caso in cui vengano sostenute spese anche per conto di persone non dipendenti dalla Società, queste devono essere inserite nel "*Report Nota Spese"* indicando il numero esatto degli ospiti, il nominativo degli stessi e le società di appartenenza.

- La liquidazione del rimborso spese è di competenza dell'Ufficio Amministrazione.

3. GESTIONE DELLE OPERAZIONI BANCARIE CON GLI ISTITUTI DI CREDITO

3.1. I reati e gli illeciti potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i delitti contro la criminalità organizzata (richiamati dall'art. 24-*ter* del D.Lgs. 231/2001);
- i reati contro la Pubblica Amministrazione (richiamati dall'art. 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione;
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:
  - art. 2621 c.c. – False comunicazioni sociali;
  - art. 2635 c.c. - Corruzione tra privati;
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 10 D.Lgs. n. 74/2000 – Occultamento o distruzione di documenti contabili
- i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (richiamati dall'art. 25-*octies* del D.Lgs. 231/2001), e in particolare:
  - art. 648 c.p. - Ricettazione;
  - art. 648-*bis* c.p. - Riciclaggio;
  - art. 648-*ter* c.p. - Impiego di denaro, beni o utilità di provenienza illecita;
  - art. 648-*ter*.1 c.p. - Autoriciclaggio;

3.2. Principi di comportamento

I Destinatari devono:

- agire nel pieno rispetto della normativa vigente in materia di strumenti di incasso e pagamento, tracciabilità dei flussi finanziari e antiriciclaggio, nonché delle procedure interne e di controllo;

- effettuare controlli formali e sostanziali dei flussi finanziari aziendali;

- preferire, ove possibile, il canale bancario nell'effettuazione delle operazioni di incasso e pagamento derivanti da rapporti di acquisto o vendita di beni, servizi, consulenze e di partecipazioni, di finanziamento. L'utilizzo di pagamenti in contanti deve essere limitato ai soli casi espressamente consentiti e comunque nel rispetto dei limiti previsti dalla normativa vigente in materia di strumenti di pagamento;

- utilizzare la clausola di non trasferibilità per le operazioni a mezzo assegno bancario;

- consentire la tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte all'interno del processo di gestione dei pagamenti, degli incassi, della piccola cassa e delle altre operazioni finanziarie;

- disporre pagamenti congrui con la documentazione sottostante *(e.g. fattura autorizzata)* e sul conto corrente segnalato dal fornitore;

- non accettare incassi in denaro contante e titoli al portatore per importi complessivamente superiori alla soglia di riferimento indicata dalla normativa vigente;

- conservare la documentazione giustificativa a supporto degli incassi, dei pagamenti e dei movimenti di cassa;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- condurre le attività relative alla gestione dei flussi monetari e finanziari in maniera "anomala", impiegando, sostituendo o trasferendo disponibilità finanziarie di provenienza illecita, in modo da ostacolare l'identificazione della loro provenienza delittuosa;

- effettuare operazioni idonee a favorire il riciclaggio di denaro proveniente da attività illecite o criminali;

- approvare e pagare fatture passive a fronte di prestazioni simulate o inesistenti in tutto o in parte, e in generale atte ad eludere corretti adempimenti fiscali;

- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare conti aperti presso filiali in Paesi esteri ove ciò non sia correlato alla sottostante attività economica / commerciale;

- creare fondi a fronte di pagamenti non giustificati (in tutto o in parte);

- detenere / trasferire denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera per importi, anche frazionati, complessivamente pari o superiori ai limiti previsti dalla normativa;

- richiedere il rilascio e l'utilizzo di moduli di assegni bancari e postali in forma libera, in luogo di quelli con clausola di non trasferibilità;

- emettere assegni bancari e postali per importi pari o superiori ai limiti previsti dalla normativa che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;

- effettuare bonifici, anche, internazionali senza l'indicazione della controparte;

- effettuare pagamenti:

  - non adeguatamente documentati e autorizzati;
  - in contanti a fornitori oltre i limiti previsti dalla normativa;
  - in paesi diversi da quelli in cui risiede la controparte o in cui ha esecuzione il contratto;
  - per cassa, eccetto per particolari tipologie di acquisto, e comunque per importi rilevanti;

- accettare o effettuare pagamenti frazionati se non supportati da accordi commerciali (quali anticipo e saldo alla consegna e pagamenti rateizzati);

- promettere o versare somme di denaro, anche attraverso soggetti terzi, a funzionari della Pubblica Amministrazione o a qualsiasi soggetto terzo privato con cui la Società si relaziona a titolo personale, con la finalità di promuovere o favorire interessi della Società o di società controllate, anche a seguito di illecite pressioni;

- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;

- operare con c.d. *conti transitori o di attesa*, se questi non sono funzionali allo svolgimento di operazioni commerciali correlate alle attività proprie di business;

- effettuare transazioni finanziarie "fuori mercato", ovvero a condizioni che differiscano in modo sostanziale da quelle prevalenti sul mercato al momento in cui la transazione è posta in essere;

- ricorrere a strumenti finanziari strutturati o comunque a qualsiasi strumento o combinazione di strumenti per i quali il rischio massimo non sia quantificabile in modo ragionevole;

- intrattenere qualsiasi tipo di rapporto (contrattuale, finanziario, etc.) con persone o organizzazioni indicate nelle principali Black List internazionali;

- effettuare, ove non fosse strettamente necessario al fine dell'esecuzione delle attività proprie di business:

  - intestazioni fiduciarie di strumenti finanziari;
  - operazioni di investimento in strumenti finanziari scarsamente negoziati e/o a limitata diffusione;
  - investimenti in strumenti finanziari non dematerializzati;

- procedere alla richiesta ed ottenimento di fideiussioni che non siano strettamente necessarie al fine dell'esecuzione delle attività proprie di business;

- stralciare crediti verso clienti, pubblici o privati, al solo fine di favorire illecitamente gli interessi della Società.

3.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione delle operazioni bancarie e dei rapporti con gli istituti di credito e le società di assicurazione che vanno a richiamare, riassumere o integrare quanto definito dalle procedure e linee guida aziendali già predisposte in materia.

- <u>Gestione dei rapporti con gli istituti di credito e dei conti correnti</u>

- Le operazioni di apertura e chiusura dei conti correnti bancari devono essere eseguite da persone formalmente delegate.

- I poteri di firma per le operazioni sui conti correnti bancari devono essere sempre esercitati nel rispetto delle deleghe e procure in essere.

- Le riconciliazioni bancarie devono essere svolte con cadenza mensile dal FISS. Questa deve verificare la congruenza tra gli importi riportati negli estratti conto bancari con quelli risultanti dalle schede contabili. In caso di discordanza tra saldo contabile ed il saldo dell'estratto conto bancario devono essere evidenziati i movimenti che originano tali differenze. Tali operazioni devono essere registrate/annotate nell'estratto conto entro il mese successivo a quello di riferimento.

- Le riconciliazioni bancarie devono essere mensilmente verificate dal Responsabile Finance.

- L'esito delle verifiche sulle riconciliazioni bancarie deve essere sintetizzato in una scheda riepilogativa delle risultanze. Questa deve essere sottoscritta dal Responsabile Finance.

- Gestione di incassi e pagamenti

- Sono ammesse le seguenti modalità di incassi e pagamenti: Bonifico bancario automatico / Bonifico bancario manuale / R.I.D. (Rapporto Interbancario Diretto) / Ricevuta Bancaria;

- É ammesso il ricorso al pagamento in contanti in caso di:

  - Spese postali, raccomandate, acquisto francobolli, marche da bollo
  - Piccole spese varie (duplicazione chiavi, ricarica chiave caffè ospiti, spese per acquisti vari con scontrino fiscale)
  - Spese per certificati Tribunali e CCIAA
  - Diritti consolari e autentiche di firme
  - Reintegro cassa ufficio accettazione se in essere (piccole consegne contrassegno)

- I colleghi che richiedono il "rimborso della spesa" a mezzo cassa devono consegnare al cassiere il giustificativo della spesa firmato dal Responsabile del centro di costo di appartenenza, o dal livello gerarchico superiore se il richiedente sia il responsabile del centro di costo stesso.

- In fase di incasso/pagamento di operazioni anomale e/o straordinarie la Funzione Finance deve almeno svolgere verifiche sulla sede legale/amministrativa delle società controparti, degli istituti di credito utilizzati e di eventuali schermi societari e strutture fiduciarie utilizzate per tali transazioni, anche con l'ausilio di terzi professionisti.

- Incassi

- La gestione degli incassi viene svolta dallo Share Service Center (SSC) e dal personale della Funzione Finance della Società secondo quanto stabilito dal *Master Supply Agreement*.

- Lo SSC si occupa della gestione operativa degli incassi: attraverso un apposito scadenziario crediti verifica le posizioni dei clienti. A fronte di ritardi avvia l'iter di sollecito.

- Settimanalmente il Credit Manager monitora le azioni intraprese dallo SSC. Per alcuni clienti la gestione dei solleciti è direttamente in capo al Credit Manager.

- La registrazione degli incassi, a mezzo bonifico, viene eseguita dallo SSC che abbina le singole partite (banca e cliente).

- Giornalmente, la persona dell'Ufficio Amministrazione delegata dal Credit Manager scarica i movimenti di *home banking* e svolge un controllo puntuale su ciascun movimento. La stampa dei movimenti viene archiviata dall'Ufficio Amministrazione.

- In caso di anomalie/delucidazioni la persona delegata dal Credit Manager interpella, via mail, l'Ufficio Amministrazione della BU o della capogruppo SE.

- In fase di registrazione degli incassi nel caso si verifichino potenziali anomalie: (I) le prime due lettere del codice IBAN del cliente denotano che il pagamento provenga da un Paese non collaborativo, (II) il nome dell'ordinante differisce da quello del cliente, la Funzione Finance prima di procedere con la contabilizzazione dell'incasso deve svolgere le dovute comunicazioni alla Funzione Vendite, accertarsi che la prestazione sia stata effettivamente resa, ed in ogni caso sanare preventivamente eventuali anomalie.

- La presentazione delle ricevute bancarie cd. RIBA (circa il 70% dei clienti utilizza questa forma di pagamento) viene svolta da persona delegata dal Credit Manager. Un programma *ad hoc* genera l'elenco delle RIBA da incassare, il Credit Manager importa il file in SAP, che genera la distinta che riporta nel sistema di *home banking*. Per procedere con l'incasso è necessaria la doppia firma da parte di persone dotate di idonei poteri. Tutte le distinte sono archiviate.

- Pagamenti

- I pagamenti vengono eseguiti mensilmente all'occorrenza dalla BU da persona delegata dall'Amministratore Delegato (AD).

- La persona delegata dall'AD verifica l'allineamento tra l'anagrafica fornitori presente sull'ERP e l'anagrafica del remote banking.

- il pagamento per cassa viene esclusivamente utilizzato per il pagamento degli oneri doganali e di piccole spese.

- L'autorizzazione al pagamento viene resa, tramite doppia firma, dai procuratori abilitati.

Parte Speciale I

Gestione dei sistemi informativi

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 con riferimento alla gestione dei sistemi informativi sono:

- gestione degli accessi logici ai dati e ai sistemi;

- gestione della sicurezza di rete e fisica;

- gestione di software, apparecchiature, dispositivi e programmi informatici.

2. GESTIONE DEI SISTEMI INFORMATIVI AZIENDALI

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i delitti informatici e trattamento illecito di dati (richiamati dall'art. 24-*bis* del D.Lgs. 231/2001), ed in particolare:
  - art. 491-*bis* c.p. - Documenti informatici;
  - art. 615-*ter* c.p. - Accesso abusivo ad un sistema informatico o telematico;
  - art. 615-*quater* c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
  - art. 615-*quinquies* c.p. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
  - art. 617-*quater* c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
  - art. 617-*quinquies* c.p. - Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
  - art. 635-*bis* c.p. - Danneggiamento di informazioni, dati e programmi informatici;
  - art. 635-*ter* c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
  - art. 635-*quater* c.p. - Danneggiamento di sistemi informatici o telematici;
  - art. 635-*quinquies* c.p. - Danneggiamento di sistemi informatici o telematici di pubblica utilità;
- i delitti in materia di violazione del diritto d'autore (richiamati dall'art. 25-*novies* del D.Lgs. 231/2001).

2.2. Principi di comportamento

La funzione *Information Technology* di gruppo, in base al proprio ruolo e responsabilità, pone in essere le azioni necessarie per:

- verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;

- identificare le potenziali vulnerabilità nel sistema dei controlli informatici;

- valutare la corretta implementazione tecnica del sistema "deleghe e poteri" aziendale a livello di sistemi informativi ed abilitazioni utente riconducibile ad una corretta segregazione dei compiti;

- monitorare i cambiamenti organizzativi o tecnici che potrebbero determinare l'esposizione del sistema informativo a nuove minacce, rendendo inadeguato il sistema di controllo accessi;

- monitorare e svolgere le necessarie attività di gestione degli accessi ai sistemi informativi aziendali e di terze parti;

- garantire l'installazione a tutti gli utenti esclusivamente software originali, debitamente autorizzati o licenziati;

- monitorare la corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e il trattamento illecito dei dati.

Tutti i soggetti Destinatari del Modello sono tenuti a rispettare, per le attività di rispettiva competenza, le seguenti regole:

- gli strumenti aziendali devono essere utilizzati nel rispetto delle procedure aziendali definite ed esclusivamente per l'espletamento della propria attività lavorativa;

- ogni Direzione / Funzione aziendale ha la responsabilità di definire e verificare periodicamente le credenziali dell'utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;

- non deve essere consentito l'accesso nelle aree riservate *(e.g. server rooms, locali tecnici, etc.)* alle persone prive di idonea autorizzazione, temporanea o permanente e, in ogni caso, tale accesso deve essere attuato nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali;

- la navigazione in Internet e l'utilizzo della posta elettronica attraverso i sistemi informativi aziendali deve essere di norma limitato alle sole attività lavorative;

- le regole atte ad assicurare l'aggiornamento delle password dei singoli utenti sui diversi applicativi aziendali devono essere applicate secondo le regole aziendali definite e in linea con i requisiti normativi;

- garantire che la sicurezza logica e fisica dei sistemi informativi della Società sia gestita nel rispetto delle regole interne e mantenendo e aggiornando costantemente le componenti infrastrutturali (HW e SW) che ne garantiscano l'efficacia;

- le attività svolte da parte di fornitori terzi devono rispettare i principi e le regole aziendali al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed infrastrutturali;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:

  - acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
  - danneggiare o distruggere dati contenuti nei suddetti sistemi informativi;

- utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;

- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria (e.g. bilancio d'esercizio, attestazioni o autocertificazioni dirette ad enti pubblici, documenti creati con l'ausilio di strumenti di firma digitale, etc.) in assenza, ove consentito dalla legge, di una specifica autorizzazione;

- utilizzare o installare programmi diversi da quelli autorizzati dal personale dalla funzione *Information Technology* e privi di licenza;

- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (e.g. numero massimo di installazioni o di utenze);

- effettuare *download* illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;

- salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore;

- aggirare o tentare di aggirare i sistemi di sicurezza aziendali (e.g. Antivirus, Firewall, Proxy server, etc.) della Società o di terze parti;

- porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali di terze parti;

- lasciare il proprio Personal Computer senza protezione password e controllo degli accessi;

- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti / sistemi;

- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;

- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;

- rivelare ad altri (se non a seguito di delega formale) od utilizzare in modo improprio gli strumenti di firma digitale assegnati;

- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;

- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per la Società.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione dei sistemi informativi:

- <u>Gestione degli accessi logici ai dati e ai sistemi</u>

- La creazione/modifica delle utenze agli applicativi aziendali è di competenza dell'IT Manager di gruppo, che provvede alla creazione/modifica su richiesta del Responsabile di funzione e/o della funzione HR del soggetto cui l'utenza si riferisce. La creazione/modifica delle utenze è gestita tramite apposito tool di ticketing.

- A ciascuna utenza vengono assegnati profili coerenti con la mansione che l'utente è chiamato a svolgere.

- La disabilitazione delle utenze viene effettuata dall'IT Manager a seguito della comunicazione della funzione HR.

- L'accesso agli applicativi aziendali è garantito solo al personale autorizzato mediante codice identificativo (*user id*) e password.

- Le password per l'accesso agli applicativi aziendali devono essere rinnovate periodicamente.

- Con cadenza almeno annuale la Funzione IT svolge una revisione periodica dei profili associati alle utenze.

- I *log* degli amministratori di sistema dell'ERP aziendale sono tracciati in report mensili.

- La Società garantisce la tracciabilità degli accessi e delle attività critiche svolte per mezzo dei sistemi informativi aziendali.

- <u>Gestione della sicurezza di rete e fisica</u>

- I server ed i client sono dotati di software antivirus che si aggiornano automaticamente.

- Il server di posta elettronica è gestito dalla Capogruppo ed è dotato di tecnologie antispam.

- L'accesso alla rete aziendale dall'esterno è reso possibile grazie al collegamento mediante VPN ed è reso possibile solo ai dipendenti/collaboratori dotati di un portatile aziendale.

- La Società dispone di un solido piano di *backup* periodico dei dati, file, programmi e sistemi operativi, al fine di garantire la salvaguardia del patrimonio informativo aziendale.

- La sala CED è chiusa a chiave. Possono accedervi, mediante badge e chiavi, le persone della Funzione IT ed il SERE Manager.

- <u>Gestione di software, apparecchiature, dispositivi o programmi informativi</u>

- Le postazioni di lavoro devono essere dotate esclusivamente di software con regolare licenza.

- La funzione IT di gruppo svolge una revisione periodica dei software installati sulle macchine dei dipendenti e dei collaboratori.

- Le modifiche agli applicativi prima del rilascio definitivo in produzione vengono sviluppate e testate in ambiente di test, separato dall'ambiente di produzione.

Parte Speciale L

Gestione degli adempimenti in materia di salute e sicurezza sul lavoro ed ambientale

1. LE ATTIVITÀ SENSIBILI

Le attività che la Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito dei processi relativi alla gestione degli adempimenti in materia di salute e sicurezza sul lavoro e ambientale sono:

- Gestione degli adempimenti in materia di salute e sicurezza sul lavoro;

- Gestione degli adempimenti in materia ambientale.

2. GESTIONE DEGLI ADEMPIMENTI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro richiamati dall'art. 25-*septies* del D.Lgs. 231/2001.

2.2. Principi di comportamento

Tutti i lavoratori[9] devono:

- rispettare gli obblighi previsti dalla legislazione applicabile in materia di salute e sicurezza sul lavoro, nonché osservare scrupolosamente le disposizioni e le istruzioni impartite dai soggetti preposti, al fine di preservare la salute e la sicurezza propria e di tutti i lavoratori;

- rispettare le linee guida aziendali e le procedure/protocolli a regolamentazione delle tematiche in materia di salute, igiene e sicurezza sul lavoro;

- collaborare, mediante i propri rappresentanti, alla valutazione di tutti i rischi per la sicurezza e salute sul lavoro;

- segnalare tempestivamente alle strutture individuate e con le modalità definite nelle procedure/protocolli aziendali in vigore, eventuali situazioni di pericolo e rischio, infortuni, malattie professionali o situazioni di *near miss* (o quasi incidenti), e violazioni alle regole di comportamento e alle procedure aziendali;

[9] Rientrano in tale categoria: datore di lavoro; dirigente e preposti per la sicurezza; Responsabile del Servizio di Prevenzione e Protezione (RSPP); Safety Environment Real Estate (SERE); Rappresentante dei Lavoratori per la Sicurezza (RLS); medico competente; squadra di gestione delle emergenze (addetto/i prevenzione incendi e al primo soccorso); altri responsabili di funzione competenti e, infine, i lavoratori (dipendenti e collaboratori) della Società.

- utilizzare, secondo le istruzioni, le attrezzature presenti sul luogo di lavoro, nonché i dispositivi di protezione individuali e collettivi, ove previsti;

- non rimuovere o modificare in nessun modo i dispositivi di sicurezza di macchine e attrezzature o altri dispositivi di segnalazione o di controllo;

- non compiere di propria iniziativa operazioni o manovre che possano compromettere la sicurezza propria o di altri lavoratori o che possano esporre sé stessi, i propri colleghi o terzi a situazioni di pericolo;

- segnalare ogni anomalia, situazione o rischio per la sicurezza e salute differenti da quelli noti o particolarmente significativi;

- partecipare alle sessioni formative e di addestramento organizzate dalla Società sui rischi per la sicurezza e salute del lavoro.

Gli esponenti aziendali della Società specificatamente responsabili devono inoltre:

- mantenere aggiornato e rispettare il corpo regolamentare ed il sistema di procure e deleghe in materia di salute e sicurezza in vigore;

- perseguire l'eliminazione dei rischi e, ove ciò non è possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;

- garantire la programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione le condizioni produttive e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro;

- perseguire l'obiettivo di "nessun danno alle persone" e la riduzione dei rischi alla fonte;

- promuovere una cultura nella quale tutti i lavoratori partecipino a questo impegno;

- garantire il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro;

- contenere l'utilizzo di agenti chimici e biologici sul luogo di lavoro;

- garantire la definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori in caso di pericolo grave e immediato;

- garantire l'idoneità delle risorse umane - in termini di numero, qualifiche professionali e formazione - e dei materiali, necessaria al raggiungimento degli obiettivi prefissati dalla Società per il mantenimento e/o miglioramento dei livelli di sicurezza e salute dei lavoratori;

- garantire l'acquisizione e la gestione dei mezzi, delle attrezzature, degli impianti e, in generale, delle strutture aziendali nel rispetto degli standard tecnico-strutturali di legge, anche attraverso un processo continuo di manutenzione (ordinaria e straordinaria) degli stessi;

- definire gli obiettivi per la sicurezza e la salute dei lavoratori, valutando i rischi connessi con l'attività svolta presso la società o presso i clienti, identificando i pericoli e i rischi introdotti presso la Società da attività ivi svolte da terzi e presso i clienti attraverso un efficace e preventivo scambio di informazioni e cooperazione/ coordinamento con il Datore di lavoro delle società esterne che dovessero operare presso la Società o la Società presso i clienti;

- garantire un adeguato livello di formazione, addestramento e informazione ai lavoratori, nonché richiedere che un adeguato livello di formazione, addestramento e informazione sia garantito dai Datore di lavoro delle ditte terze in appalto/subappalto per quanto di loro competenza e relativamente ai rischi da interferenza,

sul sistema di gestione aziendale della sicurezza definito dalla Società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società stessa;

- segnalare tempestivamente alle strutture individuate a norma di legge e/o internamente eventuali segnali / eventi di rischio / pericolo indipendentemente dalla loro gravità.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione degli adempimenti in materia di salute e sicurezza:

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

Il Datore di lavoro, in collaborazione con il RSPP, con i Dirigenti per la sicurezza e la Funzione SERE provvedono a:

- individuare, anche a seguito della redazione del Documento di Valutazione dei Rischi (DVR) e successivi aggiornamenti, lo stato di conformità (e le eventuali azioni di miglioramento) rispetto agli standard tecnico-strutturali di legge, di attrezzature, impianti (ad esclusivo titolo esemplificativo, impianti termici ed elettrici, di messa a terra, di prevenzione incendi), luoghi di lavoro, agenti chimici, fisici e biologici, e le relative responsabilità di attuazione;

- effettuare controlli periodici dei luoghi di lavoro finalizzati a garantire il mantenimento nel tempo degli standard di legge;

- pianificare ed effettuare, o verificare che siano effettuate da società/professionisti esterni qualificati, le manutenzioni periodiche e straordinarie delle macchine e delle attrezzature di lavoro utilizzate, registrandone l'avvenuta effettuazione in idonea documentazione e in coerenza con le indicazioni dei manuali d'uso e manutenzione dei singoli impianti tecnologici e delle informazioni acquisite dai fornitori/produttori delle macchine e attrezzature;

- definire i requisiti di sicurezza che i referenti aziendali preposti devono verificare preliminarmente all'approvvigionamento di attrezzature, impianti, agenti chimici, fisici e biologici, per lo sviluppo e realizzazione di prodotti/servizi;

- garantire un monitoraggio continuo sull'evoluzione degli standard tecnico-strutturali e della normativa.

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

Il Datore di Lavoro, coadiuvato dal RSPP, dal Medico Competente e dal RLS e con il supporto eventuale della Funzione SERE effettuano la valutazione dei rischi per la salute e la sicurezza, al fine di identificare ed attuare le misure di prevenzione e protezione dei lavoratori, riducendo a livelli accettabili i rischi connessi, in relazione alle conoscenze acquisite ed alla priorità definita.

Tale analisi è formalizzata in apposito documento ("Documento di Valutazione dei Rischi" o "DVR"), così come previsto dal D.Lgs. 81/2008 e s.m.i. e dalla ulteriore normativa vigente in materia di salute e sicurezza sul lavoro, contenente, tra l'altro, l'identificazione e la valutazione dei rischi per ogni mansione aziendale, le misure di prevenzione e protezione ed i dispositivi di protezione individuale assegnati a ciascun lavoratore.

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

- valutare tutti i rischi associati alle attività ed alle mansioni dei lavoratori della Società e ad elaborare e formalizzare il documento di valutazione dei rischi sia per gli stabilimenti che per lavorazioni in esterno, presso i clienti;

- aggiornare il DVR per sopravvenuti mutamenti organizzativi e procedurali, modifiche tecniche, modifiche rese necessarie da evoluzione normative, nonché a seguito di infortuni significativi che ne evidenzino la necessità, in tempi brevi e comunque non oltre un mese dagli avvenuti mutamenti e modifiche;

- formalizzare una valutazione dei rischi specifica per ogni mansione e/o attività svolta dai propri lavoratori con identificazione e valutazione di ogni specifico pericolo e rischio connesso e delle misure per la loro mitigazione e riduzione;

- valutare i rischi di interferenza con le mansioni di lavoratori di società terze operanti presso la Società con la redazione del Documento Unico dei Rischi per Interferenze (DUVRI).

Il Datore di Lavoro provvede inoltre a:

- garantire il diritto di accesso e utilizzo, senza costi, per ogni lavoratore a idonei Dispositivi di Protezione Individuale (DPI) - e/o collettivi - adeguati alla mansione svolta, assicurando anche la registrazione dei dispositivi di sicurezza assegnati;

- assicurare l'attuazione delle metodologie per l'analisi e la classificazione degli incidenti e degli eventi pericolosi eventualmente registrati;

- assicurare la definizione delle responsabilità per l'attuazione di misure atte a mitigare le conseguenze a seguito di incidenti o non conformità, nonché per l'avvio e il completamento di misure correttive.

Più in particolare, per l'attività presso clienti, la Società, a tutela dei propri dipendenti, ha in essere una procedura di controllo e monitoraggio dei presidi di sicurezza esistenti presso il cliente e, se del caso, la Società, su istanza e richiesta dei propri dipendenti, impone al cliente l'istituzione di maggiori presidi di sicurezza e prevenzione, arrivando anche all'interdizione a lavorare presso il cliente in caso di inottemperanza o di vigenza di pericoli per la salute e sicurezza dei propri dipendenti.

- <u>Attività di natura organizzativa, comprese emergenze, primo soccorso, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza</u>

La Società è dotata di un sistema di nomine e deleghe che definisce le responsabilità, i compiti e i poteri in materia di sicurezza, prevenzione infortuni e igiene sul lavoro. Il Datore di Lavoro provvede al mantenimento ed eventuale aggiornamento (e connesse comunicazioni e flussi informativi) delle individuazioni dei Dirigenti e dei Preposti, del RSPP e del Medico Competente; sono designati i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza (addetti al primo soccorso e addetti alle emergenze in caso d'incendio, etc.).

A supporto della gestione delle emergenze è presente il Piano di Emergenza.

Il Datore di Lavoro, con il supporto del RSPP e dei Dirigenti per la sicurezza garantisce l'adeguatezza, efficacia di ruolo, indipendenza per quanto di competenza e aggiornamento formativo delle squadre di emergenza.

Inoltre:

- i responsabili in materia di sicurezza sul lavoro sopra identificati devono esercitare, per l'area di loro competenza, tutti i poteri attribuiti ed adempiere a tutti gli obblighi previsti dal D.Lgs. 81/2008 e s.m.i., nonché da tutte le altre leggi e regolamenti in materia di sicurezza, prevenzione infortuni ed igiene ambientale applicabili;

- tutti i lavoratori sono opportunamente formati (ed addestrati in occasione delle esercitazioni di emergenza) in merito ai riferimenti (sia interni che esterni) da contattare in caso di emergenza e le azioni da compiere per una sicura evacuazione.

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

- garantire la sicurezza e salute sul luogo di lavoro;

- gestire le attività in appalto e subappalto ed i relativi rischi di interferenza;

- regolamentare i flussi informativi;

- garantire l'effettuazione di attività operative e definire istruzioni per svolgere correttamente ed in sicurezza le attività relative ad ogni figura professionale;

-garantire la corretta gestione delle situazioni d'emergenza e prevedere prove di emergenza/evacuazione periodiche.

Il Datore di Lavoro, con il supporto del RSPP e dei Dirigenti per la sicurezza e con la collaborazione della Funzione SERE, garantiscono che:

- siano indette**,** come previsto dall'art. 35 del D.Lgs. 81/2008, almeno una volta all'anno, riunioni periodiche alle quali partecipino tutte le figure chiave della sicurezza;

- sia assicurata la continua formazione, sensibilizzazione e competenza in materia di salute e sicurezza del lavoro di tutti i lavoratori, per le linee guida generali e sui rischi specifici connessi alla loro mansione, nonché del personale responsabile, per le relative specifiche competenze;

- sia effettuata la registrazione dell'avvenuta effettuazione delle suddette attività, nonché l'archiviazione della documentazione relativa.

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

- il documento di valutazione dei rischi e conseguenti misure di prevenzione;

- l'andamento degli infortuni, delle malattie professionali e della sorveglianza sanitaria;

- i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale;

- i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute.

- <u>Gestione degli appalti e delle forniture</u>

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

Il processo di qualifica dei fornitori effettuato dalla Società impone la richiesta e la verifica (in ogni caso in fase di prima qualifica, nonché con periodicità definita in caso di forniture continuative e/o ripetute nel tempo), anche con il supporto del RSPP e della Funzione SERE, del possesso dei requisiti di idoneità tecnico-professionale dell'impresa appaltatrice o dei lavoratori autonomi per lo svolgimento dell'attività nonché di documentazione specifica quale, ad esempio, l'iscrizione alla Camera di Commercio, l'indicazione del nominativo del/i soggetto/i incaricato/i dell'assolvimento dei compiti di cui all'art. 97 del D.Lgs. 81/2008 e s.m.i. (con l'indicazione delle specifiche mansioni, il DURC o la posizione INAIL, il Documento di Valutazione

dei Rischi, il Piano Operativo di Sicurezza che identifica le generalità dei lavoratori, le mansioni, l'esperienza lavorativa e la posizione INAIL - ove necessario), le nomine dei RSPP e dei Medici Competenti.

Il Datore di Lavoro, coadiuvato dai dirigenti per la sicurezza, dal RSPP e dai preposti per la sicurezza, assicura, durante l'esecuzione dei lavori:

- la cooperazione tra il Datore di Lavoro per all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro di incidenti sull'attività lavorativa oggetto dell'appalto;

- il coordinamento degli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori (reciprocamente scambio di informazioni anche al fine di ridurre i rischi dovuti alle interferenze - qualora si presentassero - tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva);

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

- <u>Attività di sorveglianza sanitaria</u>

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

È responsabilità del Medico Competente, purché non a scapito degli accertamenti obbligatori previsti a norma di legge, valutare l'adeguatezza ed eventualmente aggiornare il programma di sorveglianza in base alle eventuali sopravvenute esigenze. In particolare, il Medico Competente deve, così come previsto dall'art. 25 del Testo Unico della Sicurezza sul lavoro (TUS), tra l'altro:

- collaborare con il Datore di Lavoro, con il Servizio Prevenzione e Protezione e con il RLS nella valutazione dei rischi;

- programmare ed effettuare: (i) accertamenti preventivi intesi a constatare l'assenza di controindicazioni al lavoro cui i lavoratori sono destinati, ai fini della valutazione della loro idoneità alla mansione specifica, (ii) accertamenti periodici, volti a controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica;

- istituire, aggiornare e custodire la cartella sanitaria e di rischio di ogni lavoratore;

- visitare gli ambienti di lavoro una o due volte all'anno in base ai dettami legislativi e produrre relativo verbale delle verifiche effettuate;

- collaborare alle attività di formazione e informazione;

- collaborare alla predisposizione del servizio di Pronto Soccorso;

- formalizzare e comunicare al lavoratore l'esito delle analisi svolte, contenente giudizi di idoneità o inidoneità, rilasciandone duplice copia (una al lavoratore e una al Datore di Lavoro per la relativa archiviazione);

- partecipare alla riunione periodica di sicurezza ex art. 35 del TUS, rendicontando sulle visite effettuate, l'andamento degli infortuni e delle malattie professionali, ecc.

Gli obblighi di sorveglianza sanitaria sono riferiti a tutti i lavoratori della Società. La Società può promuovere azioni di sensibilizzazione e formazione ai terzi collaboratori.

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

Il Datore di lavoro, con il supporto del RSPP e della Funzione Risorse Umane ed eventualmente la Funzione SERE, anche con il supporto di professionisti specializzati in materia, garantiscono che siano attivate le azioni necessarie a:

- predisporre il Piano Annuale di Addestramento e Formazione con individuazione delle necessità di formazione ai lavoratori;

- organizzare ed erogare programmi di formazione/addestramento ai lavoratori neoassunti/soggetti a cambio mansione;

- organizzare ed erogare programmi di formazione specifici e periodici anche per gruppi particolari (es. antincendio e primo soccorso);

- registrare le attività di formazione e conservare le tabelle riassuntive della formazione svolta nel corso dell'anno con relativa documentazione (fogli presenza dei partecipanti, eventuali schede di verifica apprendimento, materiale didattico distribuito);

- effettuare periodicamente verifiche volte ad accertare il livello di apprendimento e la consapevolezza in ambito di sicurezza dei lavoratori, formalizzando e archiviando i risultati, previa condivisione con il RLS;

- organizzare prove di simulazione di emergenza e di evacuazione con periodicità almeno annuale;

- comunicare ai fornitori e agli appaltatori dettagliate informazioni sui rischi specifici esistenti nella sede della Società, nonché le regole comportamentali e di controllo adottate dalla medesima, definite nel presente documento e nelle procedure aziendali;

- provvedere all'erogazione della necessaria formazione, informazione ed addestramento dei lavoratori a seguito di aggiornamenti normativi ed a seguito di mutamenti organizzativi, tecnici o procedurali con impatto sulla attività lavorativa ai fini della sicurezza.

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

Il Datore di Lavoro vigila sul corretto espletamento delle attività in materia di salute e sicurezza sul lavoro; i Dirigenti per la sicurezza ed i Preposti, ciascuno nell'ambito delle proprie competenze, sovrintendono e vigilano sull'osservanza, da parte dei lavoratori, degli obblighi di legge e delle disposizioni aziendali in materia di salute e sicurezza sul lavoro.

La vigilanza si esplica anche mediante i sopralluoghi svolti dal RSPP in collaborazione con la Funzione SERE, nonché dal Medico Competente presso i luoghi di lavoro.

Nel caso di *audit* in materia di salute e sicurezza sul lavoro, il Datore di lavoro, con il supporto della Funzione SERE e con il supporto del SPP assicura che:

- sulla base di un "piano di verifica", sia effettuata l'attività di verifica periodica sul sistema aziendale di gestione della sicurezza e salute, anche con l'eventuale supporto di professionisti esterni formalmente incaricati nel rispetto delle regole comportamentali e di controllo definite nel presente Modello;

- siano esaminati i verbali delle verifiche periodiche, con particolare riferimento ai rilievi emersi (non conformità e/o osservazioni) e al relativo piano di azione in cui sono indicati gli interventi necessari per rimuovere le non conformità riscontrate, il soggetto responsabile della loro attuazione e le tempistiche;

- Sistemi di registrazione implementati

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

2.4. Sorveglianza e sistema disciplinare

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

È presente un sistema disciplinare della società, in coerenza con il Contratto Collettivo Nazionale applicato.

È previsto un flusso informativo concernente i provvedimenti disciplinari in materia antinfortunistica adottati al fine di consentire, se del caso e in collaborazione con il RSPP, la definizione di adeguate misure di controllo del rischio.

3. GESTIONE DEGLI ADEMPIMENTI IN MATERIA AMBIENTALE

3.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito della conduzione delle attività in oggetto (si rimanda al "*Catalogo Reati Presupposto*" previsti dal D.Lgs. 231/2001 per una descrizione di dettaglio di ciascuna fattispecie di reato richiamata) sono:

- i reati in materia ambientale richiamati dall'art. 25-*undecies* del D.Lgs. 231/2001 (D.Lgs. 121/11 e Legge 68/15), in particolare:
  - attività organizzate per il traffico illecito di rifiuti, previsti dagli artt. 259, comma 1, e 260, comma 1, del D.Lgs. 152/2006;
  - violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari, previsto dall'art. 258 comma 4, secondo periodo, D.Lgs. 152/2006;
  - false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti o inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti previsto dall'art. 260-*bis* comma 6 e 7, del D. Lgs. 152/2006;
  - inquinamento ambientale (art. 452-*bis* c.p.);
  - delitti colposi contro l'ambiente (art. 452-*quinquies* c.p.).

3.2. Principi di comportamento

I Destinatari devono:

- rispettare la normativa ambientale vigente ed osservare tutte le prescrizioni inserite in eventuali autorizzazioni ambientali;

- osservare le indicazioni aziendali atte a garantire la prevenzione dell'inquinamento e la pronta risposta alle emergenze ambientali;

- segnalare tempestivamente alle strutture individuate eventuali situazioni di pericolo per l'ambiente;

- perseguire l'obiettivo di "nessun danno all'ambiente";

- partecipare alle sessioni formative e di addestramento organizzate dalla Società sui rischi per l'ambiente;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

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

- operare in coerenza, mantenere aggiornato e rispettare il corpo regolamentare ed il sistema di procure e deleghe in materia ambientale in vigore;

- provvedere alla redazione ed aggiornamento di specifiche linee guida / procedure / istruzioni operative ambientali, formare il personale sui contenuti delle stesse e vigilare sull'osservanza della loro applicazione;

- attenersi alle regole impartite attraverso modalità operative consolidate, procedure e istruzioni operative scritte al fine di prevenire ogni impatto ambientale derivante dalle proprie lavorazioni;

- preventivamente richiedere, acquisire e rinnovare nei tempi indicati dall'autorità competente le eventuali autorizzazioni ambientali necessarie per lo svolgimento della propria attività, laddove applicabile;

- diffondere ad ogni livello dell'organizzazione i principi della buona pratica ambientale e sensibilizzare tutti i propri fornitori affinché assicurino prodotti e servizi in linea con tali principi.

Inoltre, i Destinatari hanno il diritto di:

- essere informati, formati, consultati e resi partecipi delle questioni riguardanti la tutela ambientale, con particolare riferimento ai rischi specifici della Società, sulle conseguenze di questi e sulle misure di prevenzione, nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del D.Lgs. 231/2001;

- ricevere istruzioni adeguate, anche attraverso corsi di formazione dedicati, sulla prevenzione ambientale.

3.3. Presidi di controllo

Alla luce di quanto emerso, sono di seguito elencati i presidi specifici di controllo di cui deve essere garantito il rispetto da parte dei soggetti, ognuno nell'ambito di propria competenza, che, nell'ambito dell'organizzazione della Società, sono coinvolti nella gestione degli adempimenti previsti dalla vigente normativa in materia di tutela dell'ambiente:

- <u>Gestione dei rifiuti</u>

Il Datore di Lavoro, con il supporto dei dirigenti e dei preposti per la sicurezza, della Funzione SERE e con la collaborazione del personale operativo, sono responsabili di:

- definire formalmente i ruoli, le responsabilità e le modalità operative per la verifica della corretta gestione operativa dei rifiuti prodotti;

- identificare le aree da utilizzare come deposito temporaneo dei rifiuti prodotti, garantendo il rispetto delle prescrizioni normative;

- supervisionare lo svolgimento di un controllo del volume e del tempo di giacenza dei rifiuti collocati del deposito temporaneo affinché siano rispettate le prescrizioni di legge in materia;

- gestire i rifiuti sanitari prodotti nel rispetto della vigente normativa specifica, con particolare riferimento alla raccolta, confezionamento e tempi di smaltimento;

- supervisionare la corretta collocazione dei rifiuti stoccati, evitando che gli stessi vengano miscelati (ove questi dovessero essere miscibili), assicurando inoltre la presenza dei contrassegni indicanti i corretti contenitori;

- verificare l'esistenza dei requisiti *ex lege* dei fornitori dei servizi di smaltimento dei rifiuti (quali, a titolo esemplificativo, autorizzazioni e iscrizione all'Albo Nazionale Gestori Rifiuti), acquisendo copia cartacea conforme della relativa documentazione, laddove non fosse possibile ottenere la copia in originale oppure tramite gli elenchi ufficiali degli Enti che hanno rilasciato l'autorizzazione;

- verificare che i mezzi di trasporto rifiuti siano effettivamente autorizzati per il trasporto dello specifico rifiuto; in caso contrario non procedere all'operazione di consegna del rifiuto;

- effettuare periodiche verifiche del mantenimento nel tempo dei requisiti *ex lege* dei trasportatori e destinatari dei rifiuti affidati, verificati in fase di selezione;

- supervisionare e predisporre ogni azione necessaria affinché la caratterizzazione dei rifiuti e la definizione delle specifiche modalità di smaltimento avvenga secondo i principi di accuratezza e nel rispetto delle prescrizioni normative, avvalendosi anche di laboratori terzi accreditati ai quali sono fornite chiare ed esaustive informazioni in merito al processo di produzione del rifiuto e garantendo la veridicità e completezza delle dichiarazioni inerenti, nonché di campioni rappresentativi del rifiuto;

- verificare la correttezza dei dati registrati nella dichiarazione annuale dei rifiuti (MUD) prima di sottoscriverlo e predisporne l'invio agli Enti preposti;

- assicurare periodicamente della avvenuta ricezione entro i termini di legge della quarta copia del Formulario di Identificazione Rifiuti;

- verificare che la movimentazione dei rifiuti (produzione, stoccaggio, esitazione) avvenga in condizioni di massima prevenzione ambientale;

- rispettare tutti gli adempimenti RENTRI (Registro elettronico nazionale per la tracciabilità dei rifiuti) in qualità di Produttore dei rifiuti;

- erogare specifiche sessioni formative dedicate al personale destinato alla gestione dei rifiuti ove illustrare le attività in termini di gestione stessa dei rifiuti consentite e vietate.

3.4. Sorveglianza e sistema disciplinare

La Società, attraverso i Preposti, effettua attività di sorveglianza sull'applicazione, anche da parte dei lavoratori, della normativa e degli adempimenti previsti in materia ambientale, nonché effettua, anche con l'intervento di società terze specializzate, periodiche attività di controllo atte a verificare l'efficacia dei protocolli adottati e a garantire il mantenimento nel tempo delle condizioni di idoneità delle misure adottate. La Società applica, in caso di comportamento non conforme alle suddette norme e prescrizioni, gli adeguati provvedimenti disciplinari in coerenza con il Contratto Collettivo Nazionale applicato.

Parte Speciale M

Gestione dei rapporti con gli agenti

1. LE ATTIVITÀ SENSIBILI

La Società, a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 la gestione dei rapporti con gli agenti.

2. GESTIONE DEI RAPPORTI CON GLI AGENTI

2.1. I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Società ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda al "Catalogo *Reati Presupposto"* previsti dal D.Lgs. 231/2001 per un elenco dettagliato di ciascuna fattispecie richiamata) sono:

- i delitti contro la criminalità organizzata (richiamati dall'art. 24-*ter* del D.Lgs. 231/2001), in particolare:
  - art. 416 c.p. – Associazione per delinquere
- i reati contro la Pubblica Amministrazione (richiamati dall'art. 25 del D.Lgs. 231/2001), e in particolare:
  - art. 318 c.p. - Corruzione per l'esercizio della funzione;
  - art. 319 c.p. - Corruzione per un atto contrario ai doveri d'ufficio;
  - art. 319-*quater* c.p. - Induzione indebita a dare o promettere utilità;
  - art. 320 c.p. - Corruzione di persona incaricata di un pubblico servizio;
  - art. 321 c.p. - Pene per il corruttore;
  - art. 322. c.p. - Istigazione alla corruzione.
- i reati societari (richiamati dall'art. 25-*ter* del D.Lgs. 231/2001), e in particolare:
  - art. 2621 c.c. - False comunicazioni sociali
  - art. 2635 c.c. - Corruzione tra privati
- i reati tributari (richiamati dall'art. 25 – *quinquiesdecies* del D.Lgs. 231/2001), in particolare:
  - art. 2 D.Lgs. n. 74/2000 – Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
  - art. 3 D.Lgs. n.74/2000 – Dichiarazione fraudolenta mediante altri artifici;
  - art. 8 D.Lgs. n.74/2000 – Emissione di fatture o altri documenti per operazioni inesistenti;
  - art. 10 D.Lgs. n.74/2000 – Occultamento o distruzione di documenti contabili;

2.2. Principi di comportamento

I Destinatari devono:

- utilizzare sempre la forma scritta per la stipula di contratti con gli agenti;

- effettuare le attività di selezione e contrattualizzazione degli agenti sulla base delle valutazioni di idoneità tecnica, etica ed attitudinale;

- verificare preventivamente le informazioni disponibili sugli agenti al fine di instaurare rapporti unicamente con soggetti che godano di buona reputazione, che siano impegnati solo in attività lecite e la cui cultura etica sia in linea con quella della Società;

- definire livelli di provvigioni e premi in linea con quanto previsto dal mercato e dalle politiche commerciali definite dalla Società;

- riconoscere agli agenti provvigioni e premi commisurati ai contratti conclusi dagli stessi con la clientela;

- verificare, prima del pagamento delle fatture, che le prestazioni siano state effettivamente ricevute in rispondenza a quanto pattuito contrattualmente;

- liquidare i compensi in modo trasparente, sempre documentabile e ricostruibile *ex-post*;

- effettuare pagamenti agli agenti esclusivamente tramite bonifico bancario;

- rispettare le procedure aziendali emesse dalla Società e/o dal Gruppo Schneider Electric rese disponibili sul Portale Spiece+, con particolare riferimento alla CoA globale e locale.

È inoltre espressamente vietato:

- selezionare agenti vicini o suggeriti da funzionari pubblici o da altre controparti con cui la Società intrattenga relazioni commerciali, o corrispondere loro un compenso superiore a quello dovuto o di mercato, al fine di ottenere un trattamento di favore per la Società o creare disponibilità da utilizzarsi a fini corruttivi;

- promettere o concedere promesse di collaborazione o aumenti delle provvigioni / premi quale contropartita di attività difformi alle leggi ed alle norme e regole interne;

- approvare fatture passive a fronte di prestazioni inesistenti in tutto o in parte;

- creare fondi patrimoniali extra-contabili a fronte di operazioni contrattualizzate a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;

- effettuare pagamenti in favore di agenti in assenza di adeguata giustificazione;

- utilizzare agenti al fine di corrispondere, promettere od offrire, direttamente o indirettamente, pagamenti impropri o altre utilità non dovute a soggetti terzi, con la finalità di promuovere o favorire interessi della Società o a vantaggio di quest'ultima;

- sottoscrivere o effettuare patti o accordi segreti o contrari alla legge.

2.3. Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione dei rapporti con gli agenti:

- Gli agenti vengono contrattualizzati dalla Funzione Legal a seguito di un'apposita *due diligence* volta a misurarne l'affidabilità e la professionalità.

- La funzione competente a seguito di una valutazione di potenziale rischio della controparte, deve svolgere verifiche di professionalità ed eticità degli agenti richiedendo agli stessi, a titolo esemplificativo, la visura camerale (se trattasi di persona giuridica) o i carichi pendenti (se trattasi di persona fisica), autocertificazioni in merito al possesso di requisiti tecnici.

- Ai fini della stesura del contratto di agenzia, la funzione competente deve verificare la posizione dell'agente presso la Camera di Commercio ed inserire i dati anagrafici nel CCT (*Compliance Check Tool*).

- L'autorizzazione alla stipula del contratto di agenzia con l'agente è resa nel rispetto della *Chart of Approval (CoA)*.

- I contratti di agenzia devono essere redatti dalla funzione competente utilizzando il modello standard approvato dalla funzione Legal.

- Tali contratti devono contenere:

- un'apposita clausola che preveda che la controparte dichiari di essere a conoscenza e di rispettare la normativa di cui al D.Lgs. 231/2001 e di impegnarsi al rispetto della Carta della Fiducia adottata dalla Società;
- un'apposita clausola che preveda la risoluzione del contratto in caso di violazione di quanto dichiarato;
- un'apposita clausola che preveda espressamente che gli agenti non possano avere alcun potere di rappresentanza in nome e per conto della Società e che non possano concludere direttamente contratti di vendita con i clienti.

- I contratti di agenzia controfirmati dalle controparti devono essere archiviati, in formato elettronico dalla funzione Legal all'interno di Dilitrust (tool del Gruppo).

- Eventuali modifiche ai contratti di agenzia dovute ad eccezioni (quali ad esempio accordi puntuali per specifici prodotti, zone, clienti o percentuali di provvigioni in deroga a quanto pattuito) devono essere formalizzate utilizzando i modelli standard predisposti e validati dalla Funzione Legal.

- Le modifiche ai contratti di agenzia sono autorizzate nel rispetto della *Chart of Approval*. Tali modifiche devono essere archiviate, in formato digitale, dalla funzione Legal all'interno di Dilitrust (tool del Gruppo).

- L'inserimento dell'agente nell'anagrafica fornitori è di competenza della funzione Finance.

- Le provvigioni da riconoscere agli agenti sono definite contrattualmente.

- Il calcolo delle provvigioni da riconoscere agli agenti viene svolto dalla Funzione Finance con cadenza mensile/trimestrale. Per ciascun agente viene determinato l'ammontare della provvigione (in base all'incassato) sulla base della griglia prevista contrattualmente.

- I prospetti di calcolo per la liquidazione delle provvigioni vengono trasmessi per conoscenza alla Funzione Vendite.

- Il pagamento delle fatture agli agenti spetta alla funzione competente.

- La disdetta da parte della Società ad un contratto di agenzia in essere è assoggettata, salvo diverso accordo tra le parti, ad un preciso tempo di preavviso secondo la normativa vigente.