# Socio Sanitas Service - Società a responsabilità limitata

## Modello di organizzazione e gestione ai sensi del D.Lgs. 231/2001
## Parte Speciale

**Edizione novembre 2026**

## INDICE

1 La struttura della parte speciale 4
1.1 Funzioni aziendali e criteri di attuazione 5
2 Principi generali di comportamento del Modello di organizzazione, gestione e controllo 7
2.1 Reati contro la Pubblica Amministrazione (artt. 24 e 25 D. Lgs. 231/2001) 7
2.2 Reati informatici (art. 24 bis D. Lgs. 231/2001) 8
2.3 Reati di criminalità organizzata, ricettazione e riciclaggio e reati transnazionali (artt. 24 ter e 25 octies, D. Lgs. 231/2001; art. 10 Legge 146/2006) 9
2.4 Reati in materia di violazione delle misure restrittive dell'Unione europea (art. 25-octies.2 D.Lgs. 231/2001) 10
2.5 Reati contro l'industria e il commercio (art. 25 bis e 25 bis-1 D. Lgs. 231/2001) 10
2.6 Reati societari (art. 25 ter D. Lgs. 231/2001) 10
2.7 Reati in materia di violazione del diritto d'autore (art. 25 novies D. Lgs. 231/2001) 11
2.8 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies D. Lgs. 231/2001) 11
2.9 Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies D. Lgs. 231/2001) 12
2.10 Corruzione tra privati (art. 25 ter D. Lgs. 231/2001) 12
3 Principi generali di comportamento con riguardo alla salute e alla sicurezza sul lavoro 13
4 Principi generali di comportamento con riguardo alla tutela ambientale 14
**5 Ambito: Adempimenti societari e organizzazione aziendale** 15
5.1 Area di Rischio n. 1: Definizione delle risorse, dei ruoli, delle responsabilità e autorità nell'organizzazione. 15
5.2 Area di Rischio n. 2: Gestione degli adempimenti obbligatori previsti dalla legge. 16
5.3 Area di Rischio n. 3: Gestione degli adempimenti relativi al funzionamento degli organi sociali (Assemblea del Soci e Organo Amministrativo). 18
5.4 Area di Rischio n. 4: Gestione dei rapporti con gli Organi di Controllo (Sindaci o Revisori). 19
5.5 Area di Rischio n. 5: Gestione delle operazioni societarie: gestione dei conferimenti, degli utili e delle riserve, operazioni sulle partecipazioni e sul capitale. 20
**6 Ambito: Gestione delle attività amministrative, contabili e fiscali** 22
6.1 Area di Rischio n. 6: Approvvigionamento e gestione degli appalti; acquisizione di documentazioni / certificazioni obbligatorie di legge. 22
6.2 Area di Rischio n. 7: Gestione della contabilità e predisposizione dei bilanci. 24
6.3 Area di Rischio n. 8: Gestione della fiscalità. 26
6.4 Area di Rischio n. 9: Gestione delle attività amministrativo-contabili e delle transazioni finanziarie. 28
6.5 Area di Rischio n. 10: Gestione omaggi, attività promozionali/pubblicitarie e sponsorizzazioni, nonché gestione delle relative spese di rappresentanza/ospitalità. 31
6.6 Area di Rischio n. 11: Negoziazione, stipula ed esecuzione di contratti con terze parti per l'approvvigionamento di beni, servizi, consulenze/prestazioni professionali. 33
**7 Ambito: Gestione delle reti informatiche e dei software aziendali** 37
7.1 Area di Rischio n. 12: Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT. 37
7.2 Area di Rischio n. 13: Gestione dei software aziendali e delle banche dati ottenute in licenza d'uso. 39
7.3 Area di Rischio n. 14: Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici. 41
7.4 Area di Rischio n. 15: Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni. 42
7.5 Area di Rischio n. 16: Gestione, tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso. 44
**8 Ambito: Gestione delle risorse umane** 47
8.1 Area di Rischio n. 17: Approvvigionamento di servizi che prevedono l'utilizzo di manodopera indiretta. 47
8.2 Area di Rischio n. 18: Assunzione del personale e gestione delle note spese. 48
8.3 Area di Rischio n. 19: Definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori. 51
**9 Ambito: Rapporti con le pubbliche amministrazioni** 52
9.1 Area di Rischio n. 20: Gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici, e di partecipazione a gare nei pubblici incanti o nelle licitazioni private per conto di Pubbliche Amministrazioni. 52
9.2 Area di Rischio n. 21: Gestione di rapporti con funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla Pubblica Amministrazione e/o da incaricati di Pubblico servizio. 54

9.3 Area di Rischio n. 22: Gestione pre-conteziosi, contenziosi giudiziali e/o stragiudiziali, nonché gestione dei rapporti con le Autorità Giudiziarie. 57
9.4 Area di Rischio n. 23: Raccolta, elaborazione e presentazione a soggetti pubblici o a soggetti incaricati di pubblico servizio della documentazione tecnica, economica ed amministrativa necessaria all'ottenimento e mantenimento di certificazioni, autorizzazioni, licenze, concessioni e provvedimenti amministrativi per l'esercizio delle attività aziendali. 58
**10. Ambito: Salute e sicurezza sul lavoro** 61
10.1 Area di Rischio n. 24: Comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze. 61
10.2 Area di Rischio n. 25: Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.). 62
10.3 Area di Rischio n. 26: Gestione delle emergenze. 63
10.4 Area di Rischio n. 27: Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la salute e sicurezza sul lavoro. 65
10.5 Area di Rischio n. 28: Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali. 65
10.6 Area di Rischio n. 29: Sorveglianza sanitaria 66
**11 Ambito: Ammissioni, assistenza e tutela degli ospiti** 67
11.1 Area di Rischio n. 30: Ammissione, accesso e dimissione degli ospiti 67
11.2 Area di Rischio n. 31: Presenze, rette e rendicontazione ASL 68
11.3 Area di Rischio n. 32: Assistenza, PAI e documentazione clinica 69
11.4 Area di Rischio n. 33: Tutela degli ospiti, incidenti e reclami 69
11.5 Area di Rischio n. 34: Farmaci, dispositivi e approvvigionamenti sanitari 70
11.6 Area di Rischio n. 35: Gestione di denaro e beni degli ospiti 70
**12 Ambito: Tutela ambientale e sicurezza alimentare** 71
12.1 Area di Rischio n. 36: Rifiuti sanitari e tutela ambientale 71
12.2 Area di Rischio n. 37: Cucina interna, alimenti e fornitori 71
**13 Ambito: Segnalazioni e sicurezza informatica** 72
13.1 Area di Rischio n. 38: Segnalazioni, tutela del segnalante e flussi informativi 72
13.2 Area di Rischio n. 39: Sistemi informativi sanitari, cybersicurezza e incidenti 72

## 1 La struttura della parte speciale

La struttura del Modello, oltre alla Parte Generale, prevede una Parte Speciale strutturata seguendo il c.d. “approccio per aree a rischio reato”.

Le singole aree di rischio sono aggregate all’interno di ambiti.

• Ambito: Adempimenti societari e organizzazione aziendale:

- Area di Rischio n. 1: Definizione delle risorse, dei ruoli, delle responsabilità e autorità nell’organizzazione;

- Area di Rischio n. 2: Gestione degli adempimenti obbligatori previsti dalla legge;

- Area di Rischio n. 3: Gestione degli adempimenti relativi al funzionamento degli organi sociali (Assemblea del Soci e Organo Amministrativo);

- Area di Rischio n. 4: Gestione dei rapporti con gli Organi di Controllo (Sindaci o Revisori);

- Area di Rischio n. 5: Gestione delle operazioni societarie: gestione dei conferimenti, degli utili e delle riserve, operazioni sulle partecipazioni e sul capitale;

• Ambito: Gestione delle attività amministrative, contabili e fiscali:

- Area di Rischio n. 6: Approvvigionamento e gestione degli appalti; acquisizione di documentazioni / certificazioni obbligatorie di legge;

- Area di Rischio n. 7: Gestione della contabilità e predisposizione dei bilanci;

- Area di Rischio n. 8: Gestione della fiscalità;

- Area di Rischio n. 9: Gestione delle attività amministrativo-contabili e delle transazioni finanziarie;

- Area di Rischio n. 10: Gestione omaggi, attività promozionali/pubblicitarie e sponsorizzazioni, nonché gestione delle relative spese di rappresentanza/ospitalità;

- Area di Rischio n. 11: Negoziazione, stipula ed esecuzione di contratti con terze parti per l'approvvigionamento di beni, servizi, consulenze/prestazioni professionali;

• Ambito: Gestione delle reti informatiche e dei software aziendali:

- Area di Rischio n. 12: Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT;

- Area di Rischio n. 13: Gestione dei software aziendali e delle banche dati ottenute in licenza d’uso;

- Area di Rischio n. 14: Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;

- Area di Rischio n. 15: Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni;

- Area di Rischio n. 16: Gestione, tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell’ingegno strumentali all’attività societaria, con particolare riguardo alla presenza e validità di licenze d’uso;

• Ambito: Gestione delle risorse umane:

- Area di Rischio n. 17: Approvvigionamento di servizi che prevedono l'utilizzo di manodopera indiretta;

- Area di Rischio n. 18: Assunzione del personale e gestione delle note spese;

- Area di Rischio n. 19: Definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori;

• Ambito: Rapporti con le pubbliche amministrazioni:

- Area di Rischio n. 20: Gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici, e di partecipazione a gare nei pubblici incanti o nelle licitazioni private per conto di Pubbliche Amministrazioni;

- Area di Rischio n. 21: Gestione di rapporti con funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla Pubblica Amministrazione e/o da incaricati di Pubblico servizio;

- Area di Rischio n. 22: Gestione pre-conteziosi, contenziosi giudiziali e/o stragiudiziali, nonché gestione dei rapporti con le Autorità Giudiziarie;

- Area di Rischio n. 23: Raccolta, elaborazione e presentazione a soggetti pubblici o a soggetti incaricati di pubblico servizio della documentazione tecnica, economica ed amministrativa necessaria all'ottenimento e mantenimento di certificazioni, autorizzazioni, licenze, concessioni e provvedimenti amministrativi per l'esercizio delle attività aziendali;

• Ambito: Salute e sicurezza sul lavoro:

- Area di Rischio n. 24: Comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze;

- Area di Rischio n. 25: Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.);

- Area di Rischio n. 26: Gestione delle emergenze;

- Area di Rischio n. 27: Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la salute e sicurezza sul lavoro;

- Area di Rischio n. 28: Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali;

- Area di Rischio n. 29: Sorveglianza sanitaria;

• Ambito: Ammissioni, assistenza e tutela degli ospiti:

- Area di Rischio n. 30: Ammissione, accesso e dimissione degli ospiti;

- Area di Rischio n. 31: Presenze, rette e rendicontazione ASL;

- Area di Rischio n. 32: Assistenza, PAI e documentazione clinica;

- Area di Rischio n. 33: Tutela degli ospiti, incidenti e reclami;

- Area di Rischio n. 34: Farmaci, dispositivi e approvvigionamenti sanitari;

- Area di Rischio n. 35: Gestione di denaro e beni degli ospiti;

• Ambito: Tutela ambientale e sicurezza alimentare:

- Area di Rischio n. 36: Rifiuti sanitari e tutela ambientale;

- Area di Rischio n. 37: Cucina interna, alimenti e fornitori;

• Ambito: Segnalazioni e sicurezza informatica:

- Area di Rischio n. 38: Segnalazioni, tutela del segnalante e flussi informativi;

- Area di Rischio n. 39: Sistemi informativi sanitari, cybersicurezza e incidenti.

La presente Parte Speciale, oltre a rappresentare i principi generali di comportamento ai quali si ispira l'attività di Socio Sanitas Service S.r.l., identifica, per ciascuna area a rischio reato:

- i relativi reati presupposto astrattamente perpetrabili;

- le relative attività sensibili, ovvero quelle al cui espletamento è connesso il rischio di commissione dei reati previsti dal Decreto;

- le funzioni aziendali di Socio Sanitas Service S.r.l. coinvolte nelle attività sensibili e che, astrattamente, potrebbero commettere i reati presupposto previsti dal Decreto nell'interesse o a vantaggio della Società, sebbene tale individuazione non debba considerarsi, in ogni caso, tassativa, atteso che ciascun soggetto aziendale potrebbe, in linea teorica, essere coinvolto a titolo di concorso;

- i protocolli a presidio della singola area di rischio.

### 1.1 Funzioni aziendali e criteri di attuazione

Il richiamo alle categorie di reato non equivale ad affermare che ogni illecito o ogni violazione settoriale costituisca reato presupposto: il collegamento opera solo per le fattispecie, i presupposti, le condizioni e i soggetti previsti dal Decreto o dalle altre disposizioni che lo richiamano. Alcune misure proteggono

ospiti e lavoratori anche rispetto a rischi non automaticamente riconducibili alla responsabilità 231, come specificato nelle singole aree.

Per identificare le funzioni senza indicare nominativi si applicano le definizioni della Parte Generale. Le sigle adottate sono: AU Amministratore unico; DG Direzione gestionale o generale; AMM attività amministrative svolte dalla Direzione amministrativa e dal personale incaricato; RS Responsabile sanitario o Direzione sanitaria; CS Coordinatore dei servizi; AS Assistente sociale; UAC Ufficio accettazione e reception; RQ Referente accreditamento e qualità; DL Datore di lavoro; RSPP Responsabile del servizio di prevenzione e protezione; MC Medico competente; RLS Rappresentante dei lavoratori per la sicurezza; Le attività informatiche e privacy sono coordinate dalla Direzione gestionale e dalla funzione amministrativa, con il supporto dei soggetti esterni incaricati secondo le rispettive competenze. Il canale di segnalazione è gestito dal soggetto specificamente incaricato secondo legge e procedura aziendale; REV revisore legale; OC organo di controllo, ove nominato; OdV Organismo di Vigilanza. Gli incarichi e i relativi poteri risultano dagli atti applicabili; le sigle non attestano, da sole, la costituzione di uffici distinti né l'avvenuto conferimento di incarichi. La loro attribuzione è documentata negli atti applicabili; i richiami a compiti specialistici non attestano l'esistenza di uffici distinti o la preesistenza di incarichi non documentati.

Le funzioni possono essere cumulate o esternalizzate in base all'assetto effettivo; l'attribuzione e i poteri risultano da organigramma, contratti, atti di nomina e registro degli incarichi. Le sigle non creano automaticamente posizioni, poteri di rappresentanza o deleghe ai sensi di legge. Le funzioni indicate in ciascuna area collaborano nei limiti dei rispettivi compiti e poteri effettivi, secondo il funzionigramma, le procedure e gli incarichi applicabili. La Direzione gestionale coordina la raccolta delle evidenze, salvo diversa attribuzione formalizzata e ferme le competenze del Responsabile sanitario e gli obblighi non delegabili stabiliti dalla legge.

Ogni attività sensibile deve essere autorizzata, coerente con i poteri, tracciata e verificabile. Documenti, registrazioni e autorizzazioni sono conservati dai responsabili in archivi accessibili ai soli soggetti legittimati, secondo le norme di protezione dati e i tempi applicabili. Le correzioni indicano autore, data e motivo. Deroghe motivate e urgenze richiedono autorizzazione e verifica successiva; non è consentita la deroga a divieti di legge.

L'AU nomina l'OdV monocratico con decisione successiva all'approvazione del Modello. Dalla decorrenza dell'incarico, le funzioni trasmettono i flussi previsti nelle singole aree al recapito riservato comunicato dalla Società. I flussi periodici sono trasmessi anche in assenza di eventi rilevanti mediante attestazione negativa; un evento urgente non attende la scadenza periodica. L'OdV può motivatamente richiedere informazioni ulteriori o modificare la frequenza.

Prima dell'insediamento dell'OdV, le funzioni applicano i protocolli, comunicano senza ritardo ad AU le criticità di competenza e conservano gli elementi per la consegna all'OdV; non si attribuiscono all'AU le funzioni dell'OdV. I controlli ordinari e i canali previsti dalla legge restano operativi secondo la rispettiva disciplina.

La trasmissione di informazioni all'OdV è distinta dalla gestione delle segnalazioni protette. Il soggetto o servizio specificamente incaricato gestisce il canale whistleblowing; la relativa identità e le informazioni coperte da riservatezza non sono trasmesse automaticamente all'OdV. I dati clinici e personali sono minimizzati e pseudonimizzati quando sufficienti; l'accesso a dati identificativi richiede una necessità documentata e una base giuridica idonea.

I protocolli della Parte Speciale disciplinano le attività sensibili di Socio Sanitas e sono applicati dai destinatari secondo le rispettive competenze. Il Modello si inserisce nell'organizzazione aziendale valorizzando le procedure, i piani e le altre misure già documentati dalla Società. In particolare, la documentazione esaminata comprende il documento di valutazione dei rischi, la nomina del responsabile del servizio di prevenzione e protezione, il manuale di autocontrollo alimentare HACCP, la procedura di gestione dei farmaci, la Carta dei servizi e piani assistenziali individuali. Le disposizioni del Modello si coordinano con tali strumenti, che continuano ad essere applicati secondo il rispettivo ambito. Le prescrizioni ulteriori o più dettagliate contenute nei protocolli integrano i presidi aziendali: le funzioni competenti le attuano, utilizzando e aggiornando, ove necessario, la documentazione e le modalità organizzative esistenti. Non è richiesta una procedura separata per ciascun presidio, ferme le formalità previste dalla legge. Quando la separazione dei compiti non è concretamente praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, interno o esterno se incaricato, ferme le attribuzioni, le incompatibilità e i controlli inderogabili per legge.

## 2 Principi generali di comportamento del Modello di organizzazione, gestione e controllo

I referenti delle Direzioni, delle Funzioni e dei servizi coinvolti nelle Aree a rischio, nonché tutti i destinatari del Modello di Organizzazione, Gestione e Controllo (di seguito, il "Modello") ex D. Lgs. 231/2001 (nel seguito il "Decreto"), sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico di Socio Sanitas Service S.r.l. (di seguito anche la "Società").

È fatto assoluto divieto:

di porre in essere condotte tali da integrare le fattispecie di reato previste dal D. Lgs. 231/2001;

di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose, possa in astratto diventarlo;

di porre in essere o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con la Società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della Società e nel pieno rispetto delle norme del Codice Etico;

di porre in essere o agevolare operazioni o attività che non siano rispettose delle norme del Codice Etico;

di porre in essere attività che siano in contrasto con le procedure e i principi di controllo in esse previste ai fini della prevenzione dei reati di contraffazione di segni distintivi di opere dell'ingegno o di prodotti industriali.

È, inoltre, necessario:

che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;

che sia assicurata la massima rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure interne, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività sensibili (le "aree di rischio") previste nella Parte Speciale del Modello;

che coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi all'espletamento delle suddette attività sensibili pongano particolare attenzione all'attuazione degli adempimenti stessi e riferiscano immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità e, in ogni caso, tutte le informazioni previste dal Modello.

In aggiunta alle norme di comportamento sopra menzionate, di seguito sono indicati gli ulteriori principi di comportamento da rispettare al fine di mitigare il rischio di commissione dei reati presupposto di volta in volta specificati.

### 2.1 Reati contro la Pubblica Amministrazione (artt. 24 e 25 D. Lgs. 231/2001)

È fatto assoluto divieto:

di elargire, offrire o promettere denaro a Pubblici Ufficiali o Incaricati di Pubblico Servizio;

di distribuire, offrire o promettere omaggi e regali che non siano di modico valore, in violazione di quanto previsto dal Codice Etico e dalla prassi aziendale;

di accordare, offrire o promettere altri vantaggi, di qualsiasi natura essi siano, in favore di Pubblici Ufficiali o Incaricati di Pubblico Servizio;

di effettuare prestazioni in favore dei Partner e/o dei consulenti e/o dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto associativo con essi costituito;

di riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;

di presentare dichiarazioni e/o documenti e/o dati e/o informazioni non rispondenti al vero o incompleti ad organismi pubblici nazionali, comunitari o esteri, tanto meno al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

di destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti, per scopi differenti da quelli cui erano destinati originariamente.

Inoltre, al fine di garantire il rispetto dei principi generali indicati in premessa:

nelle aree a rischio, i rapporti con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio devono essere gestiti in modo unitario, procedendo alla nomina di uno o più responsabili interni per ogni azione o pluralità di operazioni svolte;

gli accordi di associazione con i Partner devono essere definiti per iscritto, ponendo in evidenza tutte le condizioni dell'accordo stesso, in particolare per quanto concerne le condizioni economiche concordate per la partecipazione congiunta alla procedura di gara;

gli incarichi conferiti ai collaboratori esterni devono essere redatti per iscritto, con l'indicazione del compenso pattuito, ed essere sottoscritti conformemente alle deleghe ricevute;

nessun tipo di pagamento può essere effettuato in natura;

le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto.

### 2.2 Reati informatici (art. 24 bis D. Lgs. 231/2001)

Tutte le risorse aziendali e, in particolare, coloro i quali rivestono posizioni rilevanti nell'utilizzo e nell'amministrazione dei sistemi informatici, devono ispirare la loro azione ai seguenti principi di comportamento:

Riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla.

Integrità: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati.

Disponibilità: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

È fatto divieto, in particolare, di:

alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;

detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;

svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;

evitare di introdurre e/o conservare in Azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo che siano stati acquisiti con il loro espresso consenso e per motivi strettamente lavorativi;

evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

evitare l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative;

rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;

astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;

osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

### 2.3 Reati di criminalità organizzata, ricettazione e riciclaggio e reati transnazionali (artt. 24 ter e 25 octies, D. Lgs. 231/2001; art. 10 Legge 146/2006)

In coerenza con i principi del Codice Etico in materia di antiriciclaggio e ricettazione, la Società assicura la tracciabilità delle operazioni economiche e finanziarie, la valutazione dell'affidabilità delle controparti e la verifica della coerenza tra prestazioni, documentazione e corrispettivi. Le operazioni prive di adeguata giustificazione economica o che presentino anomalie devono essere sottoposte ai controlli previsti dal Modello prima della loro esecuzione.

Al fine di garantire il rispetto dei principi generali indicati in premessa:

con riferimento all'attendibilità commerciale/professionale dei fornitori e dei partner devono essere richieste tutte le informazioni necessarie, utilizzando all'uopo anche gli strumenti messi a disposizione da consulenti esterni;

gli incarichi conferiti ad eventuali aziende di servizi e/o persone fisiche che curino gli interessi economico/finanziari della Società devono essere anch'essi redatti per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite;

è necessario che le funzioni competenti assicurino il controllo della avvenuta regolarità dei pagamenti nei confronti di tutte le controparti (incluse le Società dello stesso Gruppo); in particolare, dovrà essere precisamente verificato che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;

il controllo deve essere sia formale che sostanziale (verifica della sede legale della società controparte, verifica degli istituti di credito utilizzati, verifica relativamente all'utilizzo di società fiduciarie) deve essere garantito con riferimento ai flussi finanziari aziendali e ai pagamenti verso terzi e verso società del Gruppo;

devono essere rispettati scrupolosamente i requisiti minimi fissati ai fini della selezione dei soggetti offerenti i beni e/o servizi che la Società intende acquisire;

devono essere fissati i criteri di valutazione delle offerte;

in caso di conclusione di accordi/joint venture finalizzati alla realizzazione di investimenti, deve essere garantita la massima trasparenza;

deve essere garantita la piena collaborazione con l'Autorità Giudiziaria, anche attraverso il rifiuto di influenzare gli eventuali i soggetti chiamati a rendere dichiarazioni o di indurre questi ad avvalersi della facoltà di non rispondere.

### 2.4 Reati in materia di violazione delle misure restrittive dell'Unione europea (art. 25-octies.2 D.Lgs. 231/2001)

In considerazione dell'introduzione dell'art. 25-octies.2 del D.Lgs. 231/2001 ad opera del D.Lgs. 30 dicembre 2025, n. 211, tutti i destinatari del presente Modello sono tenuti ad osservare i principi di comportamento di seguito indicati.

È fatto assoluto divieto di:

porre in essere operazioni commerciali, finanziarie o contrattuali in violazione delle misure restrittive adottate dall'Unione europea;

utilizzare soggetti terzi, intermediari o altri strumenti negoziali allo scopo di eludere l'applicazione delle predette misure restrittive;

effettuare operazioni prive di adeguata giustificazione economica o commerciale che possano determinare la violazione della normativa unionale;

omettere la conservazione della documentazione relativa alle operazioni commerciali di maggiore rilievo.

Inoltre, al fine di garantire il rispetto dei principi generali indicati in premessa:

i rapporti commerciali devono essere improntati ai principi di correttezza, trasparenza e tracciabilità;

qualora l'attività lo renda necessario, devono essere effettuate le opportune verifiche sull'identità delle controparti e sulla regolarità delle operazioni;

eventuali situazioni di anomalia o dubbi circa l'applicabilità di misure restrittive devono essere tempestivamente segnalati all'Amministratore Unico, che potrà avvalersi del supporto dei consulenti della Società.

### 2.5 Reati contro l'industria e il commercio (art. 25 bis e 25 bis-1 D. Lgs. 231/2001)

Al fine di garantire il rispetto dei principi generali indicati in premessa, la Società:

dispone di regole sull'utilizzo di materiale protetto da privativa industriale;

assicura il controllo, anche mediante l'ausilio di consulenti, della corrispondenza alla normativa del materiale promozionale/pubblicitario presentato all'esterno.

### 2.6 Reati societari (art. 25 ter D. Lgs. 231/2001)

Alla luce dei principi di controllo prima evidenziati, è necessario che tutte le operazioni svolte nell'ambito delle attività sensibili ricevano debita evidenza.

Nell'esecuzione di tali operazioni, occorre che sia garantito il rispetto dei principi di comportamento di seguito indicati:

garantire il rispetto delle regole comportamentali previste nel Codice Etico della Società, con particolare riguardo all'esigenza di assicurare che ogni operazione e transazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua;

tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'esecuzione di tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;

tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni necessarie per consentire di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società;

garantire il rispetto dei principi di integrità, correttezza e trasparenza così da consentire ai destinatari di pervenire ad un fondato ed informato giudizio sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi;

osservare le prescrizioni imposte dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo;

astenersi dal compiere qualsivoglia operazione o iniziativa qualora vi sia una situazione di conflitto di interessi, ovvero qualora sussista, anche per conto di terzi, un interesse in conflitto con quello della Società;

assicurare il regolare funzionamento della Società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale prevista dalla legge, nonché la libera formazione della volontà assembleare;

astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false e/o non corrette e/o fuorvianti, idonee a provocare l'alterazione del prezzo di strumenti finanziari;

gestire con la massima correttezza e trasparenza il rapporto con le Pubbliche Autorità, ivi incluse quelle di Vigilanza;

effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza, non ostacolando l'esercizio delle funzioni di vigilanza da queste intraprese;

tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione;

improntare le attività ed i rapporti con le altre Società del Gruppo alla massima correttezza, integrità e trasparenza, così da garantire il rispetto delle leggi e dei regolamenti vigenti.

### 2.7 Reati in materia di violazione del diritto d'autore (art. 25 novies D. Lgs. 231/2001)

A tutti i soggetti destinatari del Modello è fatto assoluto divieto:

di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose delineate, possa in astratto diventarlo;

di duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale, o comunque per trarne profitto, senza averne diritto, programmi per elaboratori, banche dati protette ovvero qualsiasi opera protetta dal diritto d'autore e da diritti connessi, incluse opere a contenuto letterario, musicale, multimediale, cinematografico, artistico;

di diffondere tramite reti telematiche - senza averne diritto - un'opera dell'ingegno o parte di essa;

di mettere in atto pratiche di file sharing, attraverso lo scambio e/o la condivisione di qualsivoglia tipologia di file attraverso piattaforme di tipo peer to peer.

Inoltre, al fine di garantire il rispetto dei principi generali indicati in premessa, la Società richiede:

l'osservanza di regole sull'utilizzo di materiale protetto da diritto d'autore;

la formalizzazione dei contratti relativi all'acquisizione e all'utilizzo di software, banche dati e altre opere protette, con clausole sui diritti di utilizzo e, ove pertinenti, sui diritti di terzi;

il divieto di installazione e utilizzo non autorizzato di sistemi di file sharing.

### 2.8 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies D. Lgs. 231/2001)

È fatto assoluto divieto:

di coartare, in qualsiasi forma e con qualsiasi modalità, la volontà di rispondere all'Autorità Giudiziaria di soggetti chiamati a rendere dichiarazioni o di indurre questi ad avvalersi della facoltà di non rispondere;

di indurre, in qualsiasi modo, i soggetti chiamati a rendere dichiarazioni di fronte all'Autorità Giudiziaria, a rendere dichiarazioni non veritiere;

di elargire, offrire o promettere denaro, omaggi, regali o altri vantaggi a persone chiamate a rendere dichiarazioni di fronte all'Autorità Giudiziaria;

di porre in essere qualsiasi comportamento che, pur non integrando in concreto l'ipotesi criminosa sopra delineate, possa in astratto diventarlo;

di porre in essere o agevolare operazioni o attività che non siano rispettose delle norme del Codice Etico.

Inoltre, al fine di garantire il rispetto dei principi generali indicati in premessa:

nei rapporti con l'Autorità Giudiziaria, occorre assicurare che gli indagati o imputati in un procedimento penale, specie ove avente ad oggetto procedimenti in cui la Società può essere direttamente o indirettamente coinvolta, siano liberi di esprimere liberamente le proprie rappresentazioni dei fatti ove decidano di sottoporsi alle domande.

### 2.9 Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies D. Lgs. 231/2001)

I destinatari del Modello dovranno attenersi ai seguenti principi:

nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, assicurarsi che tali soggetti si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;

assicurarsi con apposite clausole contrattuali che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;

che siano rispettate le misure previste dalle procedure aziendali dirette alla prevenzione dell'impiego del lavoro irregolare ed alla tutela dei lavoratori;

non fare ricorso, in alcun modo, al lavoro minorile o non collaborare con soggetti che vi facciano ricorso;

disporre un adeguato sistema di deleghe e procure in materia di assunzione dei lavoratori;

implementare un sistema di monitoraggio delle vicende relative ai permessi di soggiorno (scadenze, rinnovi, ecc.).

### 2.10 Corruzione tra privati (art. 25 ter D. Lgs. 231/2001)

Nei rapporti fra soggetti privati e nei rapporti tra dipendenti, è vietato:

sollecitare o ricevere, direttamente, o tramite un intermediario, un indebito vantaggio di qualsiasi natura, ovvero accettare la promessa di tale vantaggio, per sé o per un terzo, nello svolgimento di funzioni direttive o lavorative di qualsiasi tipo per conto della Società, al fine di commettere o omettere un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà in generale;

promettere, offrire o concedere, direttamente o tramite un intermediario, un indebito vantaggio di qualsiasi natura a soggetti che svolgono funzioni direttive o lavorative di qualsiasi tipo all'interno della società o per conto di un'entità del settore privato, affinché compiano o omettano un atto in violazione di un dovere.

Inoltre, al fine di garantire il rispetto dei principi indicati in premessa:

occorre documentare in modo adeguato i regali o gli omaggi o le spese di cortesia per consentire le verifiche da parte dell'Organismo di Vigilanza;

l'eventuale reclutamento del personale nonché la gestione dello stesso deve avvenire nel rispetto delle regole aziendali assicurando:

un processo di pianificazione delle risorse da assumere che tiene conto del fabbisogno;

l'individuazione dei requisiti minimi necessari per ricoprire il ruolo e il relativo livello di retribuzione nel rispetto di quanto previsto dai CCNL (ove applicabili) ed in coerenza con le tabelle retributive di riferimento;

la definizione di un processo di selezione del personale che disciplina: (i) la ricerca di una pluralità di candidature in funzione della complessità del ruolo da ricoprire; (ii) la gestione dei conflitti di interesse tra il selezionatore e il selezionato; (iii) la verifica, attraverso diverse fasi di screening, della coerenza delle candidature con il profilo definito;

lo svolgimento di verifiche pre-assuntive finalizzate a prevenire l'insorgere di situazioni pregiudizievoli che espongano la Società al rischio di commissione dei reati presupposto;

autorizzazione all'assunzione da parte di adeguati livelli;

sistemi che garantiscano la tracciabilità delle rilevazioni delle presenze e la correttezza delle retribuzioni erogate;

- i contratti tra la Società e i referenti di agenzie, fornitori, consulenti e clienti devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti:

nei contratti con tutte le terze parti (agenzie, consulenti, distributori ecc.) deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Modello;

le agenzie o il loro referenti, i fornitori, i distributori e, in generale, le terze parti devono essere scelti con metodi trasparenti e secondo criteri qualitativi e quantitativi predefiniti;

approvazione del contratto secondo adeguati livelli autorizzativi;

nella gestione dei contratti devono essere svolte verifiche sulla coerenza dell'ordine d'acquisto rispetto ai parametri previsti nel contratto medesimo; sulla completezza ed accuratezza della fattura e della conformità della stessa alle prescrizioni di legge, così come previsto dalle procedure aziendali;

nell'ambito dei rapporti con società, fondazioni, associazioni ed altri enti privati devono essere individuate le tipologie di rapporti e le relative modalità di gestione nonché le modalità di raccolta, verifica e approvazione della documentazione da trasmettere agli esponenti di società, fondazioni, associazioni ed altri enti privati;

devono essere rispettate le procedure per il controllo dei flussi finanziari e la tracciabilità dei pagamenti.

## 3 Principi generali di comportamento con riguardo alla salute e alla sicurezza sul lavoro

La Società impronta la propria attività ai principi di legalità, correttezza e trasparenza richiamati dal Codice Etico.

In particolare, la Società ha da sempre dimostrato costante attenzione al miglioramento continuo della sicurezza, intesa come prevenzione degli infortuni, degli incidenti e dei comportamenti pericolosi, nonché igiene e medicina del lavoro, sicurezza degli impianti, conduzione e manutenzione.

Per attuare efficacemente il proprio impegno, a tutti i livelli, la Società ha come obiettivo quello di impegnarsi per:

considerare la tutela della salute e della sicurezza dei lavoratori come un obiettivo aziendale da raggiungere e migliorare costantemente, nel rispetto degli standard tecnico-strutturali di legge relativi ad impianti, attrezzature luoghi di lavoro, agenti chimici, fisici e biologici, ecc.;

analizzare e valutare i rischi di incidenti in relazione alle disposizioni legislative, garantire la sicurezza dei lavoratori e dell'ambiente circostante ed adottare le misure per limitarne le eventuali conseguenze;

agire nel rispetto di tutte le leggi nazionali e dei regolamenti locali vigenti, adottando tutte le misure di prevenzione necessarie nelle proprie attività e aggiornandole secondo il progresso tecnico e l’esperienza acquisita;

verificare che la progettazione degli impianti, delle macchine e delle attrezzature nonché dei luoghi di lavoro, siano realizzati in modo da salvaguardare la salute dei lavoratori;

attribuire compiti e responsabilità in materia di sicurezza sul lavoro, mediante la creazione di idonea struttura di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

rendere partecipe tutta la struttura aziendale, secondo le proprie attribuzioni e competenze, al raggiungimento degli obiettivi di sicurezza assegnati;

assicurare l’attività di sorveglianza sanitaria preventiva, periodica e straordinaria, nonché l’informazione, la formazione e l’addestramento dei lavoratori;

garantire la disponibilità degli equipaggiamenti/dispositivi di protezione e prevenzione previsti e a verificarne l'impiego;

predisporre le misure atte a garantire che i soggetti terzi operanti all’interno dei locali della realtà adottino comportamenti, prassi e procedure coerenti con i principi della presente Politica;

condurre o verificare l'esercizio di impianti e apparecchiature in modo da assicurarne compatibilità con la tutela della sicurezza dei lavoratori;

coinvolgere i propri dipendenti nella definizione concreta degli obiettivi e nell'attuazione del piano di modifica e miglioramento, fornendo loro tutti gli strumenti e le conoscenze affinché operino secondo le disposizioni e le procedure di sicurezza;

assicurare idonea attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

rivedere periodicamente i contenuti del Documento di Valutazione Rischi ex D. Lgs 81/08 (Testo Unico della Sicurezza sul lavoro) al fine di verificarne l'adeguatezza, l'efficacia e l'applicabilità.

## 4 Principi generali di comportamento con riguardo alla tutela ambientale

Nell'espletamento della propria attività per conto della Società, i destinatari del Modello sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e dal Codice Etico.

A tutti i soggetti i destinatari del Modello, segnatamente, è fatto assoluto divieto:

di tenere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nell'articolo 25 undecies del Decreto;

di tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

I destinatari del Modello dovranno, inoltre, attenersi ai seguenti principi:

considerare sempre prevalente la necessità di tutelare l'ambiente rispetto a qualsiasi considerazione economica;

contribuire, per quanto di propria competenza, all'adempimento degli obblighi previsti a tutela dell'ambiente;

valutare sempre gli effetti della propria condotta in relazione al rischio di danno all'ambiente: ogni azione che possa avere impatto ambientale deve tendere alla riduzione al minimo dei danni reali o potenziali causabili all'ambiente;

conformemente alla propria formazione ed esperienza, nonché alle istruzioni e ai mezzi forniti ovvero predisposti dal datore di lavoro, non adottare comportamenti imprudenti che potrebbero recare danno all'ambiente;

astenersi dal compiere di propria iniziativa operazioni o manovre che non rientrino nelle proprie mansioni o, comunque, che siano suscettibili di recare danni all'ambiente;

devono essere rispettate le misure previste dalle procedure aziendali dirette alla prevenzione della produzione e alla riduzione della nocività dei rifiuti;

deve essere assicurata la tutela del suolo e del sottosuolo, la conservazione del territorio nonché la tutela delle acque superficiali, marine e sotterranee;

devono essere prese tutte le precauzioni necessarie a limitare al minimo l'inquinamento dell'aria e a contenere comunque le emissioni al di sotto dei limiti fissati dalla legge;

il deposito temporaneo e il successivo conferimento dei rifiuti deve essere effettuato in condizioni di sicurezza e nel rispetto della normativa vigente;

devono essere rispettate le procedure volte a prevenire le emergenze ambientali ed a limitare i danni qualora le stesse dovessero verificarsi;

partecipare ai corsi di formazione specifica in materia ambientale.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'Organismo di Vigilanza avrà facoltà di effettuare i controlli ritenuti più opportuni.

Per i rifiuti e le attività affidate a fornitori esterni, la Società verifica classificazione, requisiti degli operatori e tracciabilità, secondo i protocolli del presente Modello e la normativa applicabile.

## 5 Ambito: Adempimenti societari e organizzazione aziendale

### 5.1 Area di Rischio n. 1: Definizione delle risorse, dei ruoli, delle responsabilità e autorità nell'organizzazione.

Attività sensibili:

- procedure riguardanti la gestione e il governo della società.

**Funzioni coinvolte nelle attività sensibili:**

AU; DG; AMM; RS; CS; RQ; DL

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

- Procedure - Organizzazione

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) valutazione e controllo periodico dei requisiti di idoneità e professionalità del responsabile del servizio di prevenzione e protezione (c.d. "RSPP") e degli addetti al servizio di prevenzione e protezione (c.d. "ASPP"); ii) definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso; iii) processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza delle modalità e della tempistica in caso di avvicendamento nel ruolo; iv) presenza e l'aggiornamento dell' Organigramma della Sicurezza di Sede/Società (es. RSPP, RLS, Medico Competente, Addetti antincendio e primo soccorso, Preposti), monitorando tempestivamente ogni cambiamento intercorso e/o di progetti di cambiamento tecnologico, impiantistico, organizzativo e procedurale; v) sono correttamente nominati, nel caso di presenza di cantieri, i soggetti previsti dal titolo IV del D.Lgs. 81/2008 e sono loro conferiti adeguati poteri necessari allo svolgimento del ruolo agli stessi assegnato.

- Ruoli e responsabilità - Organizzazione e aree di rischio

Ruoli e Responsabilità: devono essere assegnati ruoli e responsabilità dei soggetti responsabili dell'identificazione e valutazione dell'applicabilità della normativa vigente e sono identificate le fonti di approfondimento normativo consultabili. L'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale è congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti situazioni di rischio.

- Segregazione dei compiti - Organizzazione

Il processo è condotto assicurando, ove concretamente praticabile, la separazione fra attività autorizzative, esecutive e di controllo. Quando la separazione non sia concretamente praticabile, l'AU dispone verifiche compensative documentate; restano ferme le attribuzioni, le incompatibilità e i controlli inderogabili previsti dalla legge.

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Procure e deleghe

Procure e deleghe: devono essere garantiti i seguenti principi in forza dei quali i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Tutte le attività devono essere svolte nel rispetto del sistema interno di procure e di attribuzione dei poteri di

rappresentanza e firma sociale e dal sistema interno di deleghe allo svolgimento delle attività di competenza.

- Misure operative

- AU approva organigramma e funzionigramma, identificando titolare, sostituto, decorrenza, compiti e limiti
- le sigle non sostituiscono nomine o deleghe formali.
- I poteri di firma e spesa risultano da atti verificabili
- le deleghe in materia di sicurezza rispettano i requisiti di legge e non trasferiscono obblighi non delegabili.
- AU verifica almeno annualmente e a ogni modifica significativa cumuli, competenze, risorse e controlli compensativi
- i soggetti interessati ricevono gli atti di competenza.

**Evidenze e tracciabilità:**

Organigramma, funzionigramma, procure, deleghe, nomine, registro incarichi, verifiche e provvedimenti.

**Flussi informativi verso l'Organismo di Vigilanza:**

Variazioni significative, carenze di poteri o risorse e controlli compensativi: trimestrale; criticità gravi senza ritardo.

### 5.2 Area di Rischio n. 2: Gestione degli adempimenti obbligatori previsti dalla legge.

Attività sensibili:

- procedure riguardanti la gestione e il governo della società.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; DG; RQ; consulenti competenti

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 353 - Turbata libertà' degli incanti

Codice Penale, art. 353-bis - Turbata libertà del procedimento di scelta del contraente

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Protocolli di prevenzione:

- Procedure - Adempimenti obbligatori di legge

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) obbligo nell'espletamento degli adempimenti di improntare i rapporti con la Pubblica Amministrazione ai principi di correttezza, trasparenza e tracciabilità; ii) verifica preliminare, a cura del Responsabile della Funzione interessata, della documentazione relativa all'espletamento degli adempimenti (ad esempio: il Responsabile della funzione amministrativa (AMM), per quanto riguarda i dati propedeutici alla predisposizione delle dichiarazioni fiscali, delle dichiarazioni dei redditi e/o dei sostituti d'imposta, la funzione amministrativa e i soggetti incaricati per la documentazione relativa agli adempimenti INPS, ecc.); iii) modalità di archiviazione della documentazione rilevante prodotta.

- Segregazione dei compiti - Adempimenti di legge

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione tra chi predispone la documentazione e le dichiarazioni e chi, dopo aver verificato la corretta compilazione, la completezza e la veridicità dei dati riportati, le sottoscrive. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità - Adempimenti obbligatori previsti dalla legge

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate. La documentazione inerente le attività in oggetto (es. documentazione e certificati, dichiarazione dei redditi, documentazione inerente il trattamento retributivo, contributivo e previdenziale del personale, documenti identificativi dei rifiuti prodotti, comunicazioni periodiche agli Enti Competenti, ecc.) deve essere opportunamente archiviata presso le Funzioni competenti.

- Ruoli e responsabilità - Applicazione di normative

Ruoli e Responsabilità: devono essere assegnati ruoli e responsabilità dei soggetti responsabili dell'identificazione e valutazione dell'applicabilità della normativa vigente e sono identificate le fonti di approfondimento normativo consultabili.

- Misure operative

- AMM mantiene scadenzario con obbligo, fonte, funzione, termine, evidenza e soggetto firmatario
- le funzioni segnalano variazioni normative e organizzative.
- Il compilatore raccoglie e verifica documenti, dati e requisiti
- un diverso soggetto verifica completezza e coerenza prima della sottoscrizione, oppure AU documenta il controllo compensativo.
- Le trasmissioni sono effettuate da soggetti autorizzati
- ricevute, rettifiche e interlocuzioni sono conservate
- errori od omissioni sono corretti senza ritardo e comunicati ove dovuto.

**Evidenze e tracciabilità:**

Scadenzario, dichiarazioni, allegati, verifiche, ricevute, correzioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Scadenze mancate, dichiarazioni inesatte o richieste rilevanti: senza ritardo; riepilogo trimestrale.

### 5.3 Area di Rischio n. 3: Gestione degli adempimenti relativi al funzionamento degli organi sociali (Assemblea del Soci e Organo Amministrativo).

Attività sensibili:

- procedure riguardanti la gestione e il governo della società;

- redazione di comunicazioni sociali.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; OC; REV

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Civile, art. 2621 - False comunicazioni sociali

Codice Civile, art. 2621-bis - False comunicazioni sociali delle società non quotate - fatto di lieve entità

Protocolli di prevenzione:

- Procedure - Adempimenti relativi al funzionamento degli organi sociali (Assemblea del Soci e Organo amministrativo)

Gestione dei registri e dei libri sociali: deve esistere una disposizione chiara e formalizzata che identifichi ruoli e responsabilità, relativamente alla tenuta, alla trascrizione e alla conservazione dei registri contabili e dei libri sociali nel rispetto delle disposizioni normative.

- Segregazione dei compiti - Operazioni sociali

Il processo in oggetto deve essere condotto, ove concretamente praticabile, in accordo con il principio di segregazione dei compiti fra chi propone le operazioni sociali e chi le verifica ed autorizza. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità

La documentazione rilevante, l'ordine del giorno, le convocazioni, le delibere, i verbali devono essere messi agli atti, archiviati e conservati (in formato cartaceo ed elettronico). Le riunioni dell'Organo Amministrativo e dell'Assemblea dei Soci devono essere verbalizzate sui libri sociali. Il processo prevede che tutti i soggetti incaricati di svolgere attività di controllo devono avere accesso ai libri sociali secondo quanto disposto dalla normativa di riferimento.

- Procure e deleghe

Procure e deleghe: devono essere garantiti i seguenti principi in forza dei quali i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Tutte le attività devono essere svolte nel rispetto del sistema interno di procure e di attribuzione dei poteri di rappresentanza e firma sociale e dal sistema interno di deleghe allo svolgimento delle attività di competenza.

- Misure operative

- AU assicura convocazioni, disponibilità delle informazioni e deliberazioni nei termini statutari
- AMM conserva i verbali e i documenti di supporto.
- Ogni decisione individua oggetto, motivazioni, poteri, eventuali interessi e conseguenze
- nessuno altera o retrodata verbali o registrazioni.

- Le richieste dei soci sono gestite secondo legge e statuto, con tracciabilità di risposte e documenti resi disponibili.

**Evidenze e tracciabilità:**

Convocazioni, verbali, libri sociali, richieste e riscontri.

**Flussi informativi verso l'Organismo di Vigilanza:**

Decisioni straordinarie e anomalie rilevanti: trimestrale; irregolarità sostanziali senza ritardo.

### 5.4 Area di Rischio n. 4: Gestione dei rapporti con gli Organi di Controllo (Sindaci o Revisori).

Attività sensibili:

- rapporti con revisori e organi di controllo.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; OC; REV

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Civile, art. 2621 - False comunicazioni sociali

Codice Civile, art. 2622 - False comunicazioni sociali delle società quotate

Codice Civile, art. 2621-bis - False comunicazioni sociali delle società non quotate - fatto di lieve entità

Codice Civile, art. 2625 c.2 - Impedito controllo

Codice Civile, art. 2626 - Indebita restituzione di conferimenti

Codice Civile, art. 2627 - Indebita ripartizione di utili e delle riserve

Codice Civile, art. 2628 - Illecite operazioni sulle azioni o quote sociali o della società controllante

Codice Civile, art. 2629 - Operazione in danno dei creditori

Codice Civile, art. 2632 - Formazione fittizia del capitale

Codice Civile, art. 2633 - Indebita ripartizione dei beni sociali da parte dei liquidatori

Codice Civile, art. 2636 - Illecita influenza sull'assemblea

Codice Civile, art. 2637 - Aggiotaggio

Codice Civile, art. 2638 c.1-2 - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

Codice Civile, art. 2629-bis - Omessa comunicazione del conflitto d'interessi

Protocolli di prevenzione:

- Procedure - Rapporti con gli Organi di Controllo

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità delle Funzioni coinvolte; ii) obbligo di fornire, con la massima completezza, trasparenza, accuratezza, veridicità e tempestività, tutti i dati, le informazioni e i documenti richiesti dagli Organi di Controllo; iii) messa a disposizione dell'Organo di Controllo di tutti i documenti relativi agli argomenti posti all'ordine del giorno dell'Assemblea dei Soci e dell'Organo Amministrativo o sui quali l'Organo di Controllo debba esprimere un parere ai sensi di legge; iv) modalità di archiviazione della documentazione rilevante prodotta.

- Ruoli e responsabilità - Rapporti con gli Organi di Controllo

Ruoli e Responsabilità: devono essere assegnati ruoli e responsabilità dei soggetti coinvolti nelle diverse fasi del processo sensibile (es. raccolta e invio delle informazioni agli Organi di Controllo).

- Tracciabilità - Rapporti con gli Organi di Controllo

I principali rapporti con gli Organi di Controllo devono essere opportunamente documentati ed archiviati presso la Direzione competente, così come eventuali richieste di documentazione o rilievi.

- Segregazione dei compiti - Predisposizione ed invio documentazione per Sindaci o Revisori

Ove concretamente praticabile, deve essere garantita l'esistenza segregazione tra chi si occupa della predisposizione della documentazione da fornire agli Organi di Controllo e chi ne verifica e ne autorizza l'invio. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Previsione di clausole nei contratti con consulenti/professionisti esterni

Contratti: nei contratti con i consulenti/professionisti esterni devono essere presenti: i) specifiche clausole con cui detti terzi dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Codice Etico/Modello Organizzativo; ii) clausole risolutive espresse che attribuiscano alla Società la facoltà di risolvere i contratti in questione in caso di violazione di tale obbligo.

- Misure operative

- AU e AMM rispondono tempestivamente alle richieste di OC e REV, con documenti completi e non alterati e registrazione delle consegne.
- I rilievi sono assegnati a un responsabile, con scadenza, azione e verifica di chiusura
- ostacoli o ritardi sono motivati e documentati.
- AU tutela l'autonomia degli organi, evita incarichi o condotte incompatibili e assicura la distinta trasmissione dei rilievi rilevanti all'OdV.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Predisposizione di bilanci, relazioni e comunicazioni sociali in genere

Deve essere trasmessa all'Organismo di Vigilanza la seguente documentazione: i) comunicazioni del Revisore a cui sia stato affidato l'esercizio del controllo contabile; ii) comunicazioni di qualsiasi incarico conferito al Revisore o a società collegate, diverso da quello concernente la revisione del bilancio.

**Evidenze e tracciabilità:**

Richieste, trasmissioni, verbali, relazioni e piano di rimedio.

**Flussi informativi verso l'Organismo di Vigilanza:**

Rilievi, limitazioni, dimissioni o carenze significative: senza ritardo; stato rimedi semestrale.

### 5.5 Area di Rischio n. 5: Gestione delle operazioni societarie: gestione dei conferimenti, degli utili e delle riserve, operazioni sulle partecipazioni e sul capitale.

Attività sensibili:

- gestione delle operazioni societarie.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; OC; REV; soggetti esterni incaricati ove necessario

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Civile, art. 2625 c.2 - Impedito controllo

Codice Civile, art. 2626 - Indebita restituzione di conferimenti

Codice Civile, art. 2627 - Indebita ripartizione di utili e delle riserve

Codice Civile, art. 2628 - Illecite operazioni sulle azioni o quote sociali o della società controllante

Codice Civile, art. 2629 - Operazione in danno dei creditori

Codice Civile, art. 2632 - Formazione fittizia del capitale

Codice Civile, art. 2633 - Indebita ripartizione dei beni sociali da parte dei liquidatori

Codice Civile, art. 2636 - Illecita influenza sull'assemblea

Codice Civile, art. 2637 - Aggiotaggio

Codice Civile, art. 2638 c.1-2 - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

Codice Civile, art. 2629-bis - Omessa comunicazione del conflitto d'interessi

D.lgs. 74/2000, art. 3 - Dichiarazione fraudolenta mediante altri artifici

D.lgs. 74/2000, art. 2, c. 2 bis - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

D.lgs. 74/2000, art. 2, c.1 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

D.lgs. 74/2000, art. 8, c.1 - Emissione di fatture o altri documenti per operazioni inesistenti

D.lgs. 74/2000, art. 11 - Sottrazione fraudolenta al pagamento di imposte

D.lgs. 74/2000, art. 10 - Occultamento o distruzione di documenti contabili

D.lgs. 74/2000, art. 4 - Dichiarazione infedele

D.lgs. 74/2000, art. 5 - Omessa dichiarazione

D.lgs. 74/2000, art. 10-quater - Indebita compensazione

D.Lgs. 19/2023, art. 54 - False o omesse dichiarazioni per il rilascio del certificato preliminare

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Protocolli di prevenzione:

- Documentazione - Gestione dei conferimenti, degli utili e delle riserve, operazioni sulle partecipazioni e sul capitale

Si richiede la predisposizione di adeguata giustificazione, documentazione ed archiviazione dei documenti relativi al rispetto di tutti gli adempimenti legislativi richiesti per la gestione delle operazioni sul patrimonio della Società, nonché di eventuali modifiche apportate al progetto di bilancio/situazioni contabili infra-annuali da parte dell'Organo Amministrativo, con particolare riferimento agli utili ed alle riserve. Le stesse previsioni devono riguardare la documentazione relativa alle riparametrazioni delle partecipazioni al capitale sociale del socio.

- Segregazione dei compiti - Operazioni sociali

Il processo in oggetto deve essere condotto, ove concretamente praticabile, in accordo con il principio di segregazione dei compiti fra chi propone le operazioni sociali e chi le verifica ed autorizza. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile

- Procure e deleghe - Pagamenti

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Solo i soggetti muniti di apposita procura sono autorizzati a firmare le disposizioni di pagamento, entro i limiti autorizzativi interni/poteri di spesa.

- Veridicità, correttezza e completezza delle informazioni prodotte per le operazioni transfrontaliere

La documentazione, le informazioni e le dichiarazioni prodotte dalla società ai fini della realizzazione di operazioni societarie e, in particolare, ai fini del rilascio del "certificato preliminare" di cui all'art. 29 del D. lgs. 19/2023, devono fornire una rappresentazione veritiera, corretta e completa della società.

A tal fine la società si dota di procedure idonee a:

elaborare una posizione economica e patrimoniale veritiera e corretta;

predisporre le informazioni richieste dall'operazione societaria secondo criteri di trasparenza e senza omissione di fatti rilevanti;

garantire la tracciabilità della documentazione prodotta;

la separazione dei compiti, ove concretamente praticabile, tra chi indirizza, chi controlla e chi esegue nell'ambito dell'attività di produzione della documentazione e delle informazioni;

garantire il controllo dell'attività di produzione della documentazione e delle informazioni.

- Misure operative

• AMM predispone dossier su ragioni, controparti, valore, interesse sociale e condizioni

• le operazioni con parti correlate sono evidenziate separatamente.

• AU verifica competenze, conflitti, limiti statutari e disciplina dell'impresa sociale prima di decidere

• acquisisce le valutazioni indipendenti richieste.

• AMM registra correttamente flussi e prestazioni, conserva contratti e giustificativi e sottopone le operazioni ai controlli di OC e REV secondo competenza.

**Evidenze e tracciabilità:**

Delibere, pareri, valutazioni, contratti infragruppo e scritture.

**Flussi informativi verso l'Organismo di Vigilanza:**

Operazioni straordinarie, conflitti e anomalie: tempestivo; riepilogo semestrale.

## 6 Ambito: Gestione delle attività amministrative, contabili e fiscali

### 6.1 Area di Rischio n. 6: Approvvigionamento e gestione degli appalti; acquisizione di documentazioni / certificazioni obbligatorie di legge.

Attività sensibili:

- selezione partner commerciali;

- gestione dei rapporti commerciali;

- negoziazione di contratti;

- emissione e ricezione di pagamenti.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; DG; RS; CS; RQ; DL

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Codice Penale, art. 356 - Frode nelle pubbliche forniture

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Protocolli di prevenzione:

- Procedure - Approvvigionamento e gestione degli appalti

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) devono essere predisposti un budget, piani annuali e pluriennali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza; ii) devono essere definiti i meccanismi di predisposizione dei Documenti di Valutazione dei Rischi ("DVR", "DUVRI") per la Salute e la Sicurezza sul Lavoro; iii) devono essere previsti meccanismi di controllo che garantiscano l'inclusione nei contratti di appalto, subappalto e somministrazione, dei costi relativi alla sicurezza del lavoro; iv) deve essere garantito lo scambio informativo dei rischi con le Ditte Esterne incaricate di prestazioni di servizio, e presidiare l'andamento dei lavori relativamente ai rischi d'interferenza; v) devono essere definite le modalità di valutazione dei requisiti di salute e sicurezza degli stessi tenendo conto anche delle considerazioni dei lavoratori attraverso le loro

rappresentanze da svolgere preliminarmente alle attività di acquisto di attrezzature, macchinari ed impianti; vi) le attrezzature, i macchinari e gli impianti devono garantire la conformità a quanto previsto dalla normativa vigente (ad es. marcatura CE, possesso di dichiarazione di conformità rilasciata dall'installatore, ecc.); vii) deve essere previsto che, se del caso, in ragione dei disposti legislativi applicabili, la messa in esercizio di attrezzature, macchinari e impianti sarà subordinata a procedure di esame iniziale o di omologazione; viii) sono previste opportune attività di formazione e/o addestramento preliminarmente all'utilizzo di nuove attrezzature, macchinari o impianti da parte dei lavoratore incaricato; ix) sono previste, qualora applicabili, le modalità di esecuzione dei controlli in accettazione, degli esami iniziali e delle omologazioni necessarie alla messa in esercizio; x) nel caso di acquisti di servizi, anche di natura intellettuale (ad es. acquisto di servizi di progettazione da rendersi a favore della Società o di eventuali clienti), la Società subordina l'attività di affidamento alla verifica preliminare delle competenze dei propri fornitori anche sulla base della sussistenza di esperienze pregresse ed eventuali requisiti cogenti (ad es. iscrizione ad albi professionali; xi) sono stabilite le modalità di verifica del possesso di idonei requisiti tecnico-professionali del soggetto esecutore delle lavorazioni, anche attraverso la verifica dell'iscrizione alla CCIAA; xii) il soggetto esecutore delle lavorazioni dovrà dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di Regolarità Contributiva; xii) l'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi rilascia la dichiarazione di conformità alle regole dell'arte; xiii) con particolare riferimento a fornitori, installatori e manutentori esterni di macchinari, impianti e di qualsiasi tipo di presidio di sicurezza e attrezzature di lavoro da realizzarsi o installare all'interno di pertinenze poste sotto la responsabilità giuridica del datore di lavoro della Società, sono attuati specifici presidi di controllo che prevedono l'individuazione della normativa applicabile (art. 26 o Titolo IV del Testo Unico Sicurezza);

- Documentazione e correttezza dichiarazioni

Deve essere posta la massima attenzione affinché informazioni e dati indicati nelle dichiarazioni siano corretti e veritieri e adeguatamente documentati.

- Segregazione dei compiti - Adempimenti di legge

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione tra chi predispone la documentazione e le dichiarazioni e chi, dopo aver verificato la corretta compilazione, la completezza e la veridicità dei dati riportati, le sottoscrive. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità - Rapporti con la pubblica amministrazione per richieste autorizzative

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate. Le principali fasi del processo in oggetto devono essere opportunamente documentate ed archiviate presso gli uffici competenti. In particolare i documenti necessari alla predisposizione delle domande, compresi i documenti trasmessi dalle funzioni competenti per la compilazione delle stesse, le dichiarazioni trasmesse alla Pubblica Amministrazione e le relative ricevute di invio devono essere opportunamente tracciate ed archiviate.

- Segregazione dei compiti - Esecuzione d'opera

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione tra chi effettua la progettazione, chi autorizza il progetto e i costi stimati e chi deve garantire la corretta esecuzione dell'opera. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Procure e deleghe - Contratti

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Lo standard richiede che i soggetti che firmano i contratti devono essere muniti di appositi poteri autorizzativi.

- Clausole in materia di sicurezza nei contratti con i fornitori

Contratti: devono essere incluse nei contratti stipilati con i fornitori le clausole e le verifiche richieste in materia di salute e sicurezza per le attività di approvvigionamento e gestione degli appalti. In merito ad eventuali inadempimenti di lavoratori di terzi presso i siti aziendali relativamente alle tematiche sicurezza, che prevedano l'attivazione di segnalazioni apposite deve essere prevista l'applicazione di penali.

- Ruoli e responsabilità - Rapporti con soggetti pubblici per la presentazione di documentazione tecnica, economica ed amministrativa

Ruoli e Responsabilità: devono essere identificati i ruoli e le responsabilità di coloro che sono coinvolti nell'attività sensibile e/o intrattengono rapporti con soggetti pubblici.

- Misure operative

- La funzione richiedente descrive fabbisogno, requisiti e caratteristiche
- AU o delegato autorizza il budget e l'acquisto secondo i poteri.
- AMM documenta ricerca e confronto motivato di offerte compatibili, verificando affidabilità, requisiti professionali e autorizzazioni
- deroghe e urgenze sono motivate.
- RS, CS o il referente competente verifica consegna e prestazione
- AMM confronta contratto, ordine, evidenza del servizio e fattura prima del pagamento
- DL cura i controlli sulle interferenze applicabili.

**Evidenze e tracciabilità:**

Richieste, preventivi, verifiche, ordini, contratti, riscontri, fatture, DUVRI ove dovuto.

**Flussi informativi verso l'Organismo di Vigilanza:**

Affidamenti diretti anomali, contestazioni gravi e conflitti: tempestivo; riepilogo semestrale.

### 6.2 Area di Rischio n. 7: Gestione della contabilità e predisposizione dei bilanci.

Attività sensibili:

- gestione dei libri sociali;

- redazione di bilanci.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; REV; OC; eventuali consulenti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

Codice Penale, art. 630 - Sequestro di persona a scopo di rapina o di estorsione

D.P.R. 309/1990 (T.U. stupefacenti), art. 74 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Civile, art. 2621 - False comunicazioni sociali

Codice Civile, art. 2622 - False comunicazioni sociali delle società quotate

Codice Civile, art. 2621-bis - False comunicazioni sociali delle società non quotate - fatto di lieve entità

Codice Civile, art. 2635 - Corruzione tra privati

Codice Civile, art. 2625 c.2 - Impedito controllo

Codice Civile, art. 2626 - Indebita restituzione di conferimenti

Codice Civile, art. 2627 - Indebita ripartizione di utili e delle riserve

Codice Civile, art. 2628 - Illecite operazioni sulle azioni o quote sociali o della società controllante

Codice Civile, art. 2629 - Operazione in danno dei creditori

Codice Civile, art. 2632 - Formazione fittizia del capitale

Codice Civile, art. 2633 - Indebita ripartizione dei beni sociali da parte dei liquidatori

Codice Civile, art. 2636 - Illecita influenza sull'assemblea

Codice Civile, art. 2637 - Aggiotaggio

Codice Civile, art. 2638 c.1-2 - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

Codice Civile, art. 2629-bis - Omessa comunicazione del conflitto d'interessi

Codice Civile, art. 2635 bis - Istigazione alla corruzione tra privati

Codice Penale, art. 648 - Ricettazione

Codice Penale, art. 648 bis - Riciclaggio

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita

Codice Penale, art. 648-ter 1 - Autoriciclaggio

Protocolli di prevenzione:

- Procedure - Gestione contabilità e Bilanci

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità delle Funzioni coinvolte; ii) definizione delle modalità operative di svolgimento e di controllo del processo in oggetto; iii) livelli autorizzativi interni per la redazione e approvazione del Progetto di Bilancio; iv) identificazione chiara e completa dei dati e delle notizie che ciascuna Funzione deve fornire, i criteri per l'elaborazione dei dati e la tempistica per la loro consegna alla funzione amministrativa (AMM); v) definizione della responsabilità in capo alla funzione amministrativa (AMM), di procedere alla verifica di ogni operazione avente rilevanza economica, finanziaria o patrimoniale e di garantire l'esistenza, a fronte di ogni registrazione contabile, di adeguati supporti documentali; vi) utilizzo, da parte del personale coinvolto in attività di formazione/redazione del bilancio, di norme che definiscono con chiarezza i principi contabili da adottare e le modalità operative per la loro contabilizzazione; vii) previsione di almeno una riunione tra il Revisore e l'Organismo di Vigilanza prima della seduta dell'Organo Amministrativo indetta per l'approvazione del bilancio, che abbia per oggetto tale documento, con stesura del relativo verbale; viii) modalità di archiviazione della documentazione rilevante prodotta.

- Segregazione dei compiti - Predisposizione e approvazione Bilancio

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione dei compiti tra le Funzioni che predispongono i dati contabili e il Bilancio e le Funzioni che ne verificano la veridicità prima della sua approvazione. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Procedure - Attività amministrativo-contabili e delle transazioni finanziarie

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità dei soggetti coinvolti; ii) segregazione dei compiti; iii) definizione dei controlli effettuati in sede di registrazione delle fatture e dei pagamenti/incassi; iv) verifica della corrispondenza tra il nome del fornitore/cliente e l'intestazione del conto estero su cui far pervenire/da cui accettare il pagamento; v) tracciabilità di tutte le fasi relative alla gestione dei pagamenti (predisposizione dei documenti attestanti l'esecuzione della prestazione, registrazione della fattura, predisposizione del pagamento, riconciliazione) e alla gestione degli incassi (registrazione contabile dell'incasso, riconciliazione); vi) divieto di disporre/accettare pagamenti/incassi nei confronti o da parte di soggetti non presenti in anagrafica; vii) obbligo di effettuare solo pagamenti sul conto corrente indicato in fattura/contratto; viii) regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e urgenza; ix) modalità di archiviazione della documentazione rilevante

prodotta, x) verifica degli istituti finanziari utilizzati nelle transazioni finanziarie in merito alla loro autorizzazione ad operare e sugli strumenti di pagamento utilizzati.

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile

- Procure e deleghe

Procure e deleghe: devono essere garantiti i seguenti principi in forza dei quali i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Tutte le attività devono essere svolte nel rispetto del sistema interno di procure e di attribuzione dei poteri di rappresentanza e firma sociale e dal sistema interno di deleghe allo svolgimento delle attività di competenza.

- Misure operative

- AMM registra solo operazioni reali con giustificativi, attribuisce competenze temporali e riconcilia conti bancari, cassa, crediti e debiti almeno mensilmente.
- Il consulente o soggetto diverso controlla campionariamente giustificativi, scritture e stime
- AU valuta rettifiche e approva il progetto di bilancio.
- AMM assicura accesso di OC e REV, coerenza con inventari, contratti, rendiconti ASL e contabilità analitica
- correzioni restano identificabili.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Predisposizione di bilanci, relazioni e comunicazioni sociali in genere

Deve essere trasmessa all'Organismo di Vigilanza la seguente documentazione: i) comunicazioni del Revisore a cui sia stato affidato l'esercizio del controllo contabile; ii) comunicazioni di qualsiasi incarico conferito al Revisore o a società collegate, diverso da quello concernente la revisione del bilancio.

**Evidenze e tracciabilità:**

Fatture, registri, riconciliazioni, bilancio, controlli, pareri e rilievi.

**Flussi informativi verso l'Organismo di Vigilanza:**

Rilievi su attendibilità contabile o operazioni anomale: tempestivo; chiusura annuale e stato rimedi.

### 6.3 Area di Rischio n. 8: Gestione della fiscalità.

Attività sensibili:

- determinazione delle imposte dirette e indirette;

- predisposizione, approvazione e invio delle dichiarazioni fiscali o modelli di versamento;

- esecuzione dei versamenti relativi alle imposte dirette e indirette.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; eventuali consulenti esterni incaricati; REV

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

Codice Penale, art. 630 - Sequestro di persona a scopo di rapina o di estorsione

D.P.R. 309/1990 (T.U. stupefacenti), art. 74 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Penale, art. 648 - Ricettazione

Codice Penale, art. 648 bis - Riciclaggio

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita (proventi da delitti con pena max > 5 anni)

Codice Penale, art. 648-ter 1 - Autoriciclaggio

D.lgs. 74/2000, art. 2, c. 2 bis - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

D.lgs. 74/2000, art. 2, c.1 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

D.lgs. 74/2000, art. 3 - Dichiarazione fraudolenta mediante altri artifici

D.lgs. 74/2000, art. 4 - Dichiarazione infedele

D.lgs. 74/2000, art. 5 - Omessa dichiarazione

D.lgs. 74/2000, art. 10-quater - Indebita compensazione

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Protocolli di prevenzione:

- Procedure - Fiscalità

Deve essere adottata una procedura per la gestione delle dichiarazioni fiscali, sulla base della documentazione contabile e dei relativi adempimenti connessi, quali presentazione delle dichiarazioni, pagamento delle imposte connesse che preveda al suo interno i seguenti elementi essenziali: i) ruoli, responsabilità, modalità operative e di controllo delle funzioni coinvolte nella gestione del processo in oggetto; ii) responsabilità, a cura della funzione amministrativa (AMM) di procedere alla verifica di ogni dichiarazione/modello predisposto da consulenti esterni al fine di garantire la completezza e la veridicità; iii) obbligo, in capo ai soggetti incaricati di prestare la massima collaborazione e trasparenza nei rapporti con il Ministero delle Finanza, l'Agenzia delle Entrate e ogni altro Ente preposto, nonché di garantire la correttezza, veridicità ed aggiornamento delle informazioni fornite; iv) descrizione di quali sono i controlli interni sul processo, chi ed in quale modo li esercita; v) tracciabilità ed evidenza dei conteggi/calcoli eseguiti; vi) modalità di aggiornamento normativo; vii) modalità di archiviazione della documentazione rilevante prodotta.

- Segregazione dei compiti - Fiscalità

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione tra chi effettua i calcoli/ conteggi delle imposte da versare, chi ne verifica la loro correttezza e chi sottoscrive le dichiarazioni, i documenti e gli atti in genere, compresi i concordati previsti dalle norme in materia di imposte dirette, indirette e altri tributi ed altre imposte eventualmente introdotte. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità - Fiscalità

Le principali fasi del processo in oggetto devono essere opportunamente documentate ed archiviate presso la funzione amministrativa (AMM) e risorse umane.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile.

- Documentazione e correttezza dichiarazioni

Deve essere posta la massima attenzione affinché informazioni e dati indicati nelle dichiarazioni siano corretti e veritieri e adeguatamente documentati.

- Previsione di clausole nei contratti con studi esterni

Contratti: all'interno dei contratti con gli studi esterni che supportano la Società per la gestione fiscale specifiche clausole contrattuali devono esservi delle clausole che prevedano, ad esempio: i) rispetto dei principi etici adottati dalla Società e la facoltà della stessa di revocare i mandati in questione nel caso di violazione di tale obbligo; ii) obbligo di accettazione del Codice Etico e/o del Modello di Organizzazione ex d.lgs. 231/2001 da parte dei soggetti terzi.

- Misure operative

- AMM verifica esistenza, inerenza e corretta imputazione dei documenti e consegna al consulente dossier completo
- le operazioni con parti correlate sono verificabili.
- Il consulente riconcilia imponibili, versamenti e crediti con contabilità e documentazione
- AU approva dichiarazioni e compensazioni prima dell'invio.
- AMM conserva calcoli, pareri, deleghe, ricevute e eventuali rettifiche
- segnala scostamenti, richieste dell'autorità e crediti contestati.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici

Predisposizione e l'aggiornamento di un report riepilogativo delle domande di finanziamento presentate nel periodo di riferimento da trasmettere con cadenza periodica all'Alta Direzione e/o all'Organismo di Vigilanza che contenga per ciascuna verifica elementi quali la tipologia di finanziamento, l'Organo Pubblico coinvolto, eventuali Partner, ecc..

**Evidenze e tracciabilità:**

Registri, prospetti, dichiarazioni, F24, ricevute, riconciliazioni e corrispondenza.

**Flussi informativi verso l'Organismo di Vigilanza:**

Accessi, verifiche, contestazioni e compensazioni anomale: tempestivo; riepilogo annuale.

### 6.4 Area di Rischio n. 9: Gestione delle attività amministrativo-contabili e delle transazioni finanziarie.

Attività sensibili:

- gestione dei flussi finanziari;

- operazioni bancarie;

- acquisizione di beni e servizi;

- pagamenti e incassi.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; DG; AS

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

Codice Penale, art. 630 - Sequestro di persona a scopo di rapina o di estorsione

D.P.R. 309/1990 (T.U. stupefacenti), art. 74 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 270-bis (nel caso di pena inferiore a 10 anni di reclusione) - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

Codice Penale, art. 270-ter (nel caso di pena inferiore a 10 anni di reclusione) - Assistenza agli associati

Codice Penale, art. 270-quater (nel caso di pena inferiore a 10 anni di reclusione) - Arruolamento con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quinquies (nel caso di pena inferiore a 10 anni di reclusione) - Addestramento ad attività con finalità di terrorismo anche internazionale

Codice Penale, art. 270-sexies (nel caso di pena inferiore a 10 anni di reclusione) - Condotte con finalità di terrorismo

Codice Penale, art. 270-sexies (nel caso di pena non inferiore a 10 anni di reclusione) - Condotte con finalità di terrorismo

Codice Penale, art. 280 (nel caso di pena inferiore a 10 anni di reclusione) - Attentato per finalità terroristiche o di eversione

Codice Penale, art. 280 (nel caso di pena non inferiore a 10 anni di reclusione) - Attentato per finalità terroristiche o di eversione

Codice Penale, art. 280-bis (nel caso di pena inferiore a 10 anni di reclusione) - Atto di terrorismo con ordigni micidiali o esplosivi

Codice Penale, art. 289-bis (nel caso di pena inferiore a 10 anni di reclusione) - Sequestro di persona a scopo di terrorismo o di eversione

Codice Penale, art. 302 (nel caso di pena inferiore a 10 anni di reclusione) - Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo

Codice Penale, art. 302 (nel caso di pena non inferiore a 10 anni di reclusione) - Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo

D.L. 625/1979 convertito L. 15/1980, art. 1 - Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica

Codice Penale, art. 583-bis - Pratiche di mutilazione degli organi genitali femminili

Codice Penale, art. 648 - Ricettazione

Codice Penale, art. 648 bis - Riciclaggio

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita (proventi da delitti con pena max > 5 anni)

Codice Penale, art. 648-ter 1 - Autoriciclaggio

D.lgs. 74/2000, art. 3 - Dichiarazione fraudolenta mediante altri artifici

D.lgs. 74/2000, art. 2, c. 2 bis - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

D.lgs. 74/2000, art. 2, c.1 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

Codice Penale, art. 356 - Frode nelle pubbliche forniture

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 493-ter - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Protocolli di prevenzione:

- Procedure - Attività amministrativo-contabili e delle transazioni finanziarie

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità dei soggetti coinvolti; ii) segregazione dei compiti; iii) definizione dei controlli effettuati in sede di registrazione delle fatture e dei pagamenti/incassi; iv) verifica della corrispondenza tra il nome del fornitore/cliente e l'intestazione del conto estero su cui far pervenire/da cui accettare il pagamento; v) tracciabilità di tutte le fasi relative alla gestione dei pagamenti (predisposizione dei documenti attestanti l'esecuzione della prestazione, registrazione della fattura, predisposizione del pagamento, riconciliazione) e alla gestione degli incassi (registrazione contabile dell'incasso, riconciliazione); vi) divieto di disporre/accettare pagamenti/incassi nei confronti o da parte di soggetti non presenti in anagrafica; vii) obbligo di effettuare solo pagamenti sul conto corrente indicato in fattura/contratto; viii) regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e urgenza; ix) modalità di archiviazione della documentazione rilevante prodotta, x) verifica degli istituti finanziari utilizzati nelle transazioni finanziarie in merito alla loro autorizzazione ad operare e sugli strumenti di pagamento utilizzati.

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Procure e deleghe - Pagamenti

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Solo i soggetti muniti di apposita procura sono autorizzati a firmare le disposizioni di pagamento, entro i limiti autorizzativi interni/poteri di spesa.

- Tracciabilità - Attività amministrativo contabili e delle transazioni finanziarie

Le principali fasi del processo devono essere tracciate e la documentazione relativa alla gestione dei flussi finanziari (es. fatture passive autorizzate, liste fatture in pagamento, disposizioni di pagamento,

riconciliazioni bancarie, giustificativi, etc) deve essere archiviata presso gli Uffici della Funzione Competente.

- Segregazione dei compiti - Pagamenti

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione tra chi predispone la disposizione di pagamento e chi verifica la corretta compilazione della stessa, autorizzandola. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile

- Misure operative

- AMM associa ogni incasso o pagamento a contratto, fattura e causale
- non sono ammessi conti non registrati o movimenti privi di giustificativo.
- AU autorizza i pagamenti nei limiti dei poteri
- AMM predispone la distinta e un soggetto diverso esegue il riscontro con ordine, prestazione e fattura
- in caso di cumulo, l'AU dispone un controllo compensativo documentato da un soggetto diverso, secondo il paragrafo 1.1.
- Cambi IBAN e beneficiario sono verificati tramite canale autonomo con referente noto
- si rifiutano pagamenti a soggetti non giustificati e si riconciliano mensilmente conti e cassa.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività amministrativo-contabili e delle transazioni finanziarie

Il Responsabile competente deve comunicare periodicamente all'Organismo di Vigilanza eventuali pagamenti o incassi non supportati da documenti giustificativi.

**Evidenze e tracciabilità:**

Distinte, autorizzazioni, riscontri prestazioni, verifiche IBAN, riconciliazioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Operazioni anomale, cambi coordinate non verificabili o ammanchi: tempestivo; rendiconto trimestrale.

### 6.5 Area di Rischio n. 10: Gestione omaggi, attività promozionali/pubblicitarie e sponsorizzazioni, nonché gestione delle relative spese di rappresentanza/ospitalità.

Attività sensibili:

- gestione di omaggi e sponsorizzazioni.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; DG; AS

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 353 - Turbata liberta' degli incanti

Codice Penale, art. 353-bis - Turbata liberta' del procedimento di scelta del contraente

Protocolli di prevenzione:

- Procedure - Spese promozionali e di rappresentanza

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli, responsabilità e modalità operative delle Funzioni coinvolte per la concessione di omaggi (ad esempio distinguendoli dalle campionature omaggio) e per l'organizzazione/sponsorizzazione di eventi (es. individuazione delle principali tipologie di eventi a cui partecipa la Società); ii) definizione di uno specifico iter autorizzativo a secondo che si parli di omaggi, eventi e spese di rappresentanza iv) modalità di archiviazione della documentazione rilevante prodotta.

- Procure e deleghe - Spese varie

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Procure e deleghe: solo i soggetti muniti di apposita procura sono autorizzati a firmare gli accordi riguardo omaggi, attività promozionali e pubblicitarie, spese di rappresentanza, entro i limiti autorizzativi interni/poteri di spesa.

- Segregazione dei compiti - Omaggi, donazioni, sponsorizzazioni, facilitazioni e spese di rappresentanza

Ove concretamente praticabile, deve essere garantita la segregazione tra chi propone omaggi, donazioni, sponsorizzazioni, facilitazioni e spese di rappresentanza, chi ne valuta la fattibilità e chi ne autorizza la spesa. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Procedure - Materiale promozionale

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli, responsabilità, modalità operative e di controllo per lo svolgimento del processo in oggetto (es. il Responsabile della Funzione Marketing definisce i criteri per la predisposizione del catalogo, avendo cura di reperire il materiale illustrativo; la Funzione R&D si occupa dell'invio alla Funzione Marketing delle specifiche tecniche dei prodotti, ecc.); ii) indicazione delle modalità per lo svolgimento delle verifiche in merito alla correttezza delle informazioni riportate, con particolare riferimento alle caratteristiche tecniche del prodotto ed al prezzo; iii) indicazione delle modalità per assicurare che il catalogo non contenga immagini contraffatte (es. autorizzazione ex ante del produttore del prodotto); iv) creazione di un processo di clearance strutturato e documentato che tuteli la Società dall'indebito utilizzo di marchi di terzi; v) modalità di archiviazione della documentazione rilevante prodotta.

- Tracciabilità - Materiale promozionale

La documentazione rilevante a supporto del processo in oggetto (es. la documentazione tecnica di supporto utilizzata per la creazione/manutenzione periodica del catalogo e/o di altro materiale promozionale, ecc,) deve essere adeguatamente tracciata ed archiviata dalle Funzioni coinvolte.

- Misure operative

- Le iniziative sono preventivamente motivate e autorizzate da AU, con verifica di beneficiario, finalità, congruità e conflitti

- non devono condizionare decisioni pubbliche o assistenziali.
- Sono vietati denaro e altre utilità indebite, regali personali da ospiti collegati alle cure e rimborsi non reali
- cortesie modiche sono subordinate anche alle regole del destinatario.
- AMM conserva richiesta, approvazione, giustificativi, beneficiario, registrazione e riscontro della prestazione.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio- Gestione omaggi, attività promozionali/pubblicitarie e sponsorizzazioni, nonché gestione delle relative spese di rappresentanza/ospitalità

Obbligo di trasmissione all'Organismo di Vigilanza di un'informativa periodica, contenente l'indicazione degli omaggi e delle spese di rappresentanza in corso con indicazione dei relativi beneficiari e importi erogati.

**Evidenze e tracciabilità:**

Registro omaggi e contributi, autorizzazioni, giustificativi, verifiche.

**Flussi informativi verso l'Organismo di Vigilanza:**

Proposte o richieste indebite e conflitti: senza ritardo; riepilogo semestrale.

### 6.6 Area di Rischio n. 11: Negoziazione, stipula ed esecuzione di contratti con terze parti per l'approvvigionamento di beni, servizi, consulenze/prestazioni professionali.

Attività sensibili:

- selezione partner commerciali;

- negoziazione di contratti;

- gestione dei pagamenti:

- operazioni con soggetti a rischio.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; RS; CS; RQ; DL

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

D.P.R. 309/1990 (T.U. stupefacenti), art. 74 - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle

Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 455 - Spendita e introduzione nello Stato, senza concerto, di monete falsificate

Codice Penale, art. 457 - Spendita di monete falsificate ricevute in buona fede

Codice Penale, art. 474 - Introduzione nello Stato e commercio di prodotti con segni falsi

Codice Penale, art. 513 - Turbata libertà dell'industria o del commercio

Codice Penale, art. 513-bis - Illecita concorrenza con minaccia o violenza

Codice Penale, art. 514 - Frodi contro le industrie nazionali

Codice Penale, art. 515 - Frode nell'esercizio del commercio

Codice Penale, art. 270-bis (nel caso di pena inferiore a 10 anni di reclusione) - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

Codice Penale, art. 270-bis (nel caso di pena non inferiore a 10 anni di reclusione) - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

Codice Penale, art. 270-ter (nel caso di pena inferiore a 10 anni di reclusione) - Assistenza agli associati

Codice Penale, art. 270-ter (nel caso di pena non inferiore a 10 anni di reclusione) - Assistenza agli associati

Codice Penale, art. 270-quater (nel caso di pena inferiore a 10 anni di reclusione) - Arruolamento con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quater (nel caso di pena non inferiore a 10 anni di reclusione) - Arruolamento con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quinquies (nel caso di pena inferiore a 10 anni di reclusione) - Addestramento ad attività con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quinquies (nel caso di pena non inferiore a 10 anni di reclusione) - Addestramento ad attività con finalità di terrorismo anche internazionale

Codice Penale, art. 270-sexies (nel caso di pena inferiore a 10 anni di reclusione) - Condotte con finalità di terrorismo

Codice Penale, art. 270-sexies (nel caso di pena non inferiore a 10 anni di reclusione) - Condotte con finalità di terrorismo

Codice Penale, art. 280 (nel caso di pena inferiore a 10 anni di reclusione) - Attentato per finalità terroristiche o di eversione

Codice Penale, art. 280 (nel caso di pena non inferiore a 10 anni di reclusione) - Attentato per finalità terroristiche o di eversione

Codice Penale, art. 280-bis (nel caso di pena inferiore a 10 anni di reclusione) - Atto di terrorismo con ordigni micidiali o esplosivi

Codice Penale, art. 280-bis (nel caso di pena non inferiore a 10 anni di reclusione) - Atto di terrorismo con ordigni micidiali o esplosivi

Codice Penale, art. 289-bis (nel caso di pena inferiore a 10 anni di reclusione) - Sequestro di persona a scopo di terrorismo o di eversione

Codice Penale, art. 302 (nel caso di pena inferiore a 10 anni di reclusione) - Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo

Codice Penale, art. 302 (nel caso di pena non inferiore a 10 anni di reclusione) - Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo

D.L. 625/1979 convertito L. 15/1980, art. 1 - Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica

Codice Penale, art. 583-bis - Pratiche di mutilazione degli organi genitali femminili

Codice Penale, art. 648 - Ricettazione

Codice Penale, art. 648 bis - Riciclaggio

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita

Codice Penale, art. 648-ter 1 - Autoriciclaggio

L. 633/1941, art. 171 - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-bis - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-ter - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-septies - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-octies - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Codice Penale, art. 356 - Frode nelle pubbliche forniture

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Protocolli di prevenzione:

- Clausole in materia di sicurezza nei contratti con i fornitori

Contratti: devono essere incluse nei contratti stipulati con i fornitori le clausole e le verifiche richieste in materia di salute e sicurezza per le attività di approvvigionamento e gestione degli appalti. In merito ad eventuali inadempimenti di lavoratori di terzi presso i siti aziendali relativamente alle tematiche sicurezza, che prevedano l'attivazione di segnalazioni apposite deve essere prevista l'applicazione di penali.

- Clausole in materia di contraffazione nei contratti con i fornitori

Contratti: devono essere incluse opportune clausole contrattuali che: i) vietino al fornitore di beni, in esecuzione del contratto stipulato con la Società, di contraffare brevetti, modelli e disegni o fornire beni contraffatti e/o di provenienza illecita (cd, clausole di tutela della proprietà industriale, del commercio e del diritto d'autore); ii) contengano una dichiarazione con la quale il fornitore garantisce di aver pieno, libero e incondizionato diritto di produrre e/o vendere i beni oggetto della fornitura senza incorrere in violazioni di diritti di terzi, inclusi diritti di marchio, diritti di brevetto per invenzioni industriali, per modelli di utilità e per modelli e disegni ornamentali, e in generale diritti sulle opere dell'ingegno e sulle invenzioni industriali; iii) prevedano una manleva per il committente ed il cliente da qualsiasi responsabilità o pretesa di terzi in ordine allo sfruttamento e alla eventuale lesione dei diritti di brevetto per invenzioni industriali o modelli utilizzati dal fornitore stesso per la realizzazione della fornitura.

- Previsione di clausole nei contratti con fornitori

Contratti: devono essere previste, nei contratti con i fornitori di: i) specifiche clausole con cui detti terzi dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Codice Etico/Modello Organizzativo; ii) clausole risolutive espresse che attribuiscano alla Società la facoltà di risolvere i contratti in questione in caso di violazione di tale obbligo.

- Procure e deleghe - Contratti

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Lo standard richiede che i soggetti che firmano i contratti devono essere muniti di appositi poteri autorizzativi.

- Previsione di clausole nei contratti con consulenti/professionisti esterni

Contratti: nei contratti con i consulenti/professionisti esterni devono essere presenti: i) specifiche clausole con cui detti terzi dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Codice Etico/Modello Organizzativo; ii) clausole risolutive espresse che attribuiscano alla Società la facoltà di risolvere i contratti in questione in caso di violazione di tale obbligo.

- Procedure - Approvvigionamento di beni, servizi, consulenze/prestazioni professionali

Deve essere adottata una procedura per la gestione degli approvvigionamenti di beni, servizi, consulenze e prestazioni professionali che disciplini: i) le responsabilità della Direzione gestionale, della funzione amministrativa e delle funzioni richiedenti secondo i rispettivi incarichi e poteri; ii) i livelli di autorizzazione delle richieste, degli ordini e della sottoscrizione dei contratti, nel rispetto dei poteri dell'Amministratore unico e delle deleghe conferite; iii) la raccolta e la valutazione comparativa di offerte, ove possibile in relazione al mercato, all'oggetto, all'urgenza e al valore dell'affidamento; iv) la motivazione documentata della scelta, compresi gli affidamenti in esclusiva, a fornitore unico o in emergenza; v) i criteri per le diverse tipologie di acquisti, la tracciabilità del processo e l'archiviazione della documentazione rilevante; vi) la verifica della corrispondenza tra prestazioni, condizioni contrattuali, fatture e pagamenti. L'eventuale impossibilità di separare le attività è gestita mediante controlli compensativi documentati disposti dall'Amministratore unico.

- Procedure - Software e diritti di terzi

La Società adotta una procedura per l'acquisizione, l'utilizzo, il rinnovo e la dismissione dei software e delle banche dati impiegati nell'attività aziendale. La procedura individua le funzioni responsabili e prevede:

i) la preventiva verifica della provenienza, del titolo d'uso e delle condizioni contrattuali applicabili, comprese le eventuali licenze open source;

ii) l'inventario dei programmi e dei servizi utilizzati, con indicazione del fornitore, della tipologia di licenza, delle eventuali scadenze, dei limiti d'uso e dei soggetti o dispositivi autorizzati, ove applicabile;

iii) il controllo delle installazioni e degli accessi, con divieto di utilizzare copie abusive o programmi non autorizzati;

iv) la verifica periodica della validità delle licenze e degli eventuali canoni o corrispettivi dovuti secondo contratto;

v) la conservazione della documentazione contrattuale e delle evidenze dei controlli;

vi) la comunicazione all'Organismo di Vigilanza, dalla decorrenza del suo incarico, delle irregolarità rilevanti ai fini del Modello, secondo i flussi informativi previsti.

Qualora la Società affidi a terzi lo sviluppo o la personalizzazione di software, i relativi contratti disciplinano i diritti di utilizzo, i componenti di terzi e le condizioni delle licenze applicabili.

- Misure operative

- AU stipula accordi scritti con oggetto, prestazioni, compenso, durata, responsabilità, obblighi di sicurezza, privacy e osservanza del Codice
- verifica requisiti e conflitti.
- Il responsabile del servizio controlla qualità, personale impiegato e prestazioni, registrando non conformità e rimedi
- DL cura cooperazione e coordinamento della sicurezza.
- AMM verifica corrispettivi e documentazione, rinnovi e accessi
- variazioni sono autorizzate e non si consentono corrispettivi fittizi o retrocessioni.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio:

- Negoziazione, stipula ed esecuzione di contratti con terze parti per l'approvvigionamento di beni, servizi, consulenze/prestazioni professionali

Obbligo di trasmissione all'Organismo di Vigilanza di un'informativa periodica, contenente l'indicazione degli acquisti effettuati in emergenza e/o a fornitore unico e/o in esclusiva con indicazione dei relativi fornitori e importi delle spese sostenute.

- Gestione omaggi, attività promozionali/pubblicitarie e sponsorizzazioni, nonché gestione delle relative spese di rappresentanza/ospitalità

Obbligo di trasmissione all'Organismo di Vigilanza di un'informativa periodica, contenente l'indicazione degli omaggi e delle spese di rappresentanza in corso con indicazione dei relativi beneficiari e importi erogati.

**Evidenze e tracciabilità:**

Contratti, due diligence, verbali, verifiche, fatture, contestazioni, autorizzazioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Inadempimenti gravi, servizi non verificabili o irregolarità: senza ritardo; riepilogo semestrale.

## 7 Ambito: Gestione delle reti informatiche e dei software aziendali

### 7.1 Area di Rischio n. 12: Gestione degli accessi fisici ai locali in cui sono localizzati i sistemi e le infrastrutture IT.

Attività sensibili:

- gestione dei sistemi informatici;

- accesso e trattamento dei dati;

- sicurezza informatica;

- gestione delle credenziali di accesso.

**Funzioni coinvolte nelle attività sensibili:**

DG; AMM; soggetti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 615-ter - Accesso abusivo ad un sistema informatico o telematico)

Codice Penale, art. 615-quater - Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

Codice Penale, art. 617-quater - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Codice Penale, art. 617-quinquies - Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Codice Penale, art. 640-quinquies - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Codice Penale, art. 635-bis - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Codice Penale, art. 635-ter - Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico

Codice Penale, art. 635-quater - Danneggiamento di sistemi informatici o telematici

Codice Penale, art. 635-quinquies - Danneggiamento di sistemi informatici o telematici di pubblico interesse

Codice Penale, art. 491-bis - Documenti informatici

Codice Penale, art. 635-quater.1 - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Codice Penale, art. 629 - Estorsione

Protocolli di prevenzione:

- Procure e deleghe - Accessi locali IT

Procure e deleghe: coerenti con le responsabilità organizzative e gestionali assegnate e chiaramente definiti e conosciuti all'interno della Società. Le chiavi e i badge degli accessi ai locali in cui sono localizzati i sistemi e le infrastrutture IT devono essere assegnati tramite comunicazione nominativa.

- Procedure - Accesso ai locali IT

Procedure: disposizioni aziendali formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili e criteri di archiviazione della documentazione rilevante. È adottata una procedura in grado di: i) regolamentare in modo chiaro e formalizzato l'accesso fisico ai locali in cui risiedono le infrastrutture IT, definendo facoltà di accesso, misure di sicurezza e di vigilanza e la relativa assunzione di responsabilità; ii) definire il processo di reporting delle violazioni, ivi comprese eventuali effrazioni dei locali tecnici o delle misure di sicurezza, nonché le contromisure da attivare; iii) definire, implementare e comunicare ai soggetti coinvolti regole che stabiliscano la necessità di credenziali fisiche di accesso (es. codici, badge) ai siti ove risiedono i sistemi informativi e le infrastrutture IT, nonché la tracciabilità del loro utilizzo. In relazione ai locali nei quali sono collocati apparati di rete, server o altri dispositivi informatici critici, la Società adotta misure idonee a limitarne l'accesso ai soli soggetti espressamente autorizzati, mediante sistemi di chiusura fisica e/o altri strumenti di controllo, secondo quanto previsto dalle procedure interne. La Società disciplina, inoltre, le modalità di custodia e utilizzo di notebook, dispositivi mobili e supporti rimovibili (quali chiavette USB e dischi esterni), prevedendo l'obbligo di proteggerli da accessi non autorizzati e, ove tecnicamente possibile, di adottare misure di sicurezza (quali credenziali di accesso e cifratura dei dati) coerenti con le regole interne di sicurezza informatica.

- Segregazione dei compiti - Accessi locali e sistemi IT

Segregazione dei compiti: separare, ove concretamente praticabile, le attività di autorizzazione, esecuzione e controllo. Quando ciò non sia praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, fermi gli obblighi inderogabili. Si richiede che: i) sia rispettato il sistema di gestione delle utenze, con particolare riferimento alla definizione di nuove utenze e della loro cancellazione; ii) sia effettuata una verifica periodica dei profili di accesso, di concessione di utenze e della modifica dei profili; l'identificazione dell'utente per l'accesso alle informazioni avvenga attraverso un identificativo univoco preventivamente assegnatogli.

- Ruoli e responsabilità - Accesso locali IT

Ruoli e Responsabilità: devono essere definite le misure di sicurezza adottate, le modalità di vigilanza, la relativa frequenza e le responsabilità nell'ambito della gestione degli accessi fisici.

- Ruoli e responsabilità - Accesso a sistemi IT e applicazioni

Ruoli e Responsabilità: è fatto espresso divieto di i) introdursi abusivamente o permanere contro la volontà espressa o tacita dell 'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza; (ii) procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo (iii) distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda ; (iv) distruggere, danneggiare, rendere in tutto o in parte inservibile sistemi informatici o telematici altrui o della Società ovvero ostacolarne gravemente il funzionamento; (v) intercettare fraudolentemente, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi; (vi) rivelare, mediante qualsiasi mezzo di informazione al pubblico, il contenuto delle comunicazioni fraudolentemente intercettate relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

- Tracciabilità - Accesso sistemi e infrastrutture IT

Si richiede che: i) sia assicurata la tracciabilità delle persone che hanno avuto accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT; ii) la documentazione riguardante le attività sia conservata, ad opera del Responsabile della Funzione coinvolta, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

- Misure operative

- La Direzione gestionale, con il supporto dei soggetti esterni incaricati, censisce locali, dispositivi e soggetti autorizzati

- accessi fisici sensibili sono limitati e registrati.
- Fornitori intervengono su autorizzazione, con identificazione, accompagnamento ove necessario e verbale degli interventi.
- La Direzione gestionale, con il supporto dei soggetti esterni incaricati, verifica periodicamente protezioni fisiche, disattiva accessi cessati e segnala intrusioni, guasti o indisponibilità.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni

Gli incidenti informatici e le violazioni di dati personali che possano presentare profili rilevanti ai fini del D.Lgs. 231/2001 sono comunicati tempestivamente all'OdV dalla decorrenza dell'incarico, nel rispetto della riservatezza e della minimizzazione dei dati. Restano distinti gli eventuali obblighi di notifica all'autorità e di comunicazione agli interessati, da valutare secondo i presupposti e i termini degli artt. 33 e 34 del Regolamento (UE) 2016/679.

**Evidenze e tracciabilità:**

Inventario, elenco accessi, registri interventi, segnalazioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Accessi anomali o incidenti: tempestivo; riesame semestrale.

### 7.2 Area di Rischio n. 13: Gestione dei software aziendali e delle banche dati ottenute in licenza d'uso.

L'acquisizione e l'utilizzo di software, banche dati e altri contenuti protetti avvengono nel rispetto delle condizioni di licenza, dei diritti dei titolari e dei principi previsti dal Codice Etico. Le funzioni competenti verificano la legittimità dell'utilizzo e conservano la documentazione relativa alle licenze applicabili.

Attività sensibili:

- gestione dei sistemi informatici;

- accesso e trattamento dei dati;

- sicurezza informatica;

- gestione delle credenziali di accesso.

**Funzioni coinvolte nelle attività sensibili:**

DG; AMM; soggetti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 515 - Frode nell'esercizio del commercio

Codice Penale, art. 640-ter - Frode informatica

L. 633/1941, art. 171 - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-bis - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-octies - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-septies - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-ter - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Codice Penale, art. 493-quater - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti

Codice Penale, art. 640-ter - Frode informatica (realizzazione di trasferimento di denaro, di valore monetario o di valuta virtuale)

Protocolli di prevenzione:

- Procedure - Inventario IT e licenze d'uso

Procedure: disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili. Deve essere adottata una procedura che gestisca l'inventario degli asset a supporto delle attività di gestione , che permetta di mantenere la

visibilità dello stato delle risorse e ne faciliti la manutenzione , l'implementazione e la gestione e manutenzione di reti. Tale inventario deve includere, tra l'altro, per ogni asset censito le informazioni sulle funzionalità e sulle tipologie di dati gestiti (fornitori, clienti, etc.), sul responsabile funzionale e sul soggetto incaricato dei sistemi informatici, sulle misure di sicurezza minime previste anche per evitare possibili commissioni di reati. Occorre inoltre dare evidenza dei soggetti che effettuano la manutenzione hardware e software degli asset aziendali dandone opportuna informazione all'Organismo di Vigilanza. La Società adotta una procedura di gestione degli aggiornamenti e delle patch dei sistemi operativi e delle applicazioni utilizzate, definendo responsabilità, modalità operative e frequenza degli interventi, al fine di ridurre il rischio di sfruttamento di vulnerabilità note. La Società assicura l'adozione di misure antivirus e antimalware adeguate ai sistemi utilizzati, con aggiornamenti e monitoraggio degli eventi rilevanti secondo le procedure applicabili e gli incarichi conferiti. Eventuali vulnerabilità di sicurezza rilevate su sistemi e applicazioni vengono valutate e gestite attraverso specifici interventi di remediation, che sono pianificati e documentati in coerenza con la criticità dei sistemi coinvolti.

- Tracciabilità - Inventario IT e licenze d'uso

I software e i servizi informatici utilizzati dalla Società sono censiti in un inventario aggiornato, con indicazione del fornitore, del titolo e delle condizioni di utilizzo, degli eventuali limiti, della data di attivazione e delle scadenze o dei rinnovi, ove previsti. Sono documentate le verifiche periodiche sulle licenze, comprese quelle gratuite o open source, e conservati i relativi contratti o altri titoli d'uso.

- Ruoli e responsabilità - Inventario IT e licenze d'uso

Ruoli e Responsabilità: devono essere promossi controlli finalizzati a garantire la gestione e la manutenzione hardware e software (ivi compresi l'inventario e i divieti o limitazioni di utilizzo) e deve attivare procedure di controllo di installazione di software potenzialmente pericolosi sui sistemi operativi. È fatto espresso divieto di: i) accedere in maniera non autorizzata ai sistemi informativi utilizzati da soggetti privati o dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare informazioni a vantaggio dell'azienda o di terzi, o comunque al fine di procurare un indebito vantaggio all'azienda od a terzi; ii) distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda; iii) distruggere, danneggiare, rendere in tutto o in parte inservibile sistemi informatici o telematici altrui o della Società ovvero ostacolarne gravemente il funzionamento; iv) utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio virus, worm, troian, spyware, dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, v) porre in essere azioni idonee a commettere reati, in particolare riguardanti strumenti di pagamento diversi dai contanti.

- Procedure - Software e diritti di terzi

La Società adotta una procedura per l'acquisizione, l'utilizzo, il rinnovo e la dismissione dei software e delle banche dati impiegati nell'attività aziendale. La procedura individua le funzioni responsabili e prevede:

i) la preventiva verifica della provenienza, del titolo d'uso e delle condizioni contrattuali applicabili, comprese le eventuali licenze open source;

ii) l'inventario dei programmi e dei servizi utilizzati, con indicazione del fornitore, della tipologia di licenza, delle eventuali scadenze, dei limiti d'uso e dei soggetti o dispositivi autorizzati, ove applicabile;

iii) il controllo delle installazioni e degli accessi, con divieto di utilizzare copie abusive o programmi non autorizzati;

iv) la verifica periodica della validità delle licenze e degli eventuali canoni o corrispettivi dovuti secondo contratto;

v) la conservazione della documentazione contrattuale e delle evidenze dei controlli;

vi) la comunicazione all'Organismo di Vigilanza, dalla decorrenza del suo incarico, delle irregolarità rilevanti ai fini del Modello, secondo i flussi informativi previsti.

Qualora la Società affidi a terzi lo sviluppo o la personalizzazione di software, i relativi contratti disciplinano i diritti di utilizzo, i componenti di terzi e le condizioni delle licenze applicabili.

- Misure operative

  • La Direzione gestionale, con il supporto dei soggetti esterni incaricati, mantiene inventario di programmi, licenze, versioni e titolari e impedisce installazioni non autorizzate.

  • AU approva acquisti e rinnovi

  • La Direzione gestionale, con il supporto dei soggetti esterni incaricati, controlla licenze, requisiti di sicurezza e accordi con fornitori.

  • La Direzione gestionale, con il supporto dei soggetti esterni incaricati, esegue aggiornamenti, verifica anomalie e dismissioni

  • AMM conserva licenze e documenti contrattuali.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni

Gli incidenti informatici e le violazioni di dati personali che possano presentare profili rilevanti ai fini del D.Lgs. 231/2001 sono comunicati tempestivamente all'OdV dalla decorrenza dell'incarico, nel rispetto della riservatezza e della minimizzazione dei dati. Restano distinti gli eventuali obblighi di notifica all'autorità e di comunicazione agli interessati, da valutare secondo i presupposti e i termini degli artt. 33 e 34 del Regolamento (UE) 2016/679.

**Evidenze e tracciabilità:**

Inventario, licenze, ordini, registri aggiornamento e verifiche.

**Flussi informativi verso l'Organismo di Vigilanza:**

Software non autorizzato o licenze irregolari: tempestivo; verifica annuale.

### 7.3 Area di Rischio n. 14: Gestione della creazione, protezione, emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici.

Attività sensibili:

- gestione dei sistemi informatici;

- accesso e trattamento dei dati;

- sicurezza informatica;

- gestione delle credenziali di accesso.

**Funzioni coinvolte nelle attività sensibili:**

DG; AMM; RS; CS; soggetti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 615-ter - Accesso abusivo ad un sistema informatico o telematico)

Codice Penale, art. 615-quater - Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

Codice Penale, art. 617-quater - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Codice Penale, art. 617-quinquies - Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Codice Penale, art. 640-quinquies - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Codice Penale, art. 635-bis - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Codice Penale, art. 635-ter - Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico

Codice Penale, art. 635-quater - Danneggiamento di sistemi informatici o telematici

Codice Penale, art. 635-quinquies - Danneggiamento di sistemi informatici o telematici di pubblico interesse

Codice Penale, art. 491-bis - Documenti informatici

Codice Penale, art. 635-quater.1 - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Codice Penale, art. 629 - Estorsione

Protocolli di prevenzione:

- Procedure - Gestione ed utilizzo documenti informatici

Procedure: disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili. Deve essere adottata una procedura in grado di definire, aggiornare e approvare formalmente le policy aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e deve essere assicurata la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento al piano di back up, disaster recovery e alla gestione della posta elettronica. La Società adotta procedure di salvataggio periodico (backup) dei dati e delle configurazioni ritenuti critici, prevedendo modalità e frequenze di esecuzione coerenti con le esigenze operative e con il livello di rischio individuato. Sono altresì previsti test periodici di ripristino dei dati, al fine di verificare l'efficacia delle procedure di backup. I log di sistema e di applicazione ritenuti rilevanti ai fini della sicurezza informatica e del controllo interno sono conservati per un periodo di tempo adeguato alle esigenze di audit e agli obblighi normativi, secondo quanto stabilito nelle procedure interne. Per i servizi informativi essenziali, la Società fa riferimento a piani di disaster recovery e di continuità operativa, che disciplinano le modalità di ripristino dei sistemi e dei dati in caso di eventi che ne compromettano la disponibilità.

- Ruoli e responsabilità - Utilizzo e gestione documenti informatici

Ruoli e responsabilità: è fatto espresso divieto di: i) formare falsamente (sia sotto il profilo materiale sia per quanto attiene al contenuto) documenti societari aventi rilevanza esterna; ii) procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o comunque mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti.

- Misure operative

- Le funzioni creano e modificano solo atti di competenza con credenziali individuali
- firme digitali sono personali e conservate in sicurezza.
- La Direzione gestionale, con il supporto dei soggetti esterni incaricati, protegge integrità e disponibilità degli archivi, gestisce log, versioni e backup
- modifiche a dati clinici o rendicontazioni sono attribuibili e motivate.
- La Direzione gestionale e la funzione amministrativa, con i soggetti esterni incaricati, definiscono tempi, accessi, cancellazioni e gestione delle violazioni dati in base alle finalità e alla legge.

**Evidenze e tracciabilità:**

Log, registri, versioni, backup, prove ripristino, procedure di conservazione.

**Flussi informativi verso l'Organismo di Vigilanza:**

Alterazioni, perdite o accessi indebiti: immediato; esiti backup semestrali.

### 7.4 Area di Rischio n. 15: Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni.

Attività sensibili:

- gestione dei sistemi informatici;

- accesso e trattamento dei dati;

- sicurezza informatica;

- gestione delle credenziali di accesso.

**Funzioni coinvolte nelle attività sensibili:**

DG; AU; AMM; RS; soggetti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 615-ter - Accesso abusivo ad un sistema informatico o telematico)

Codice Penale, art. 615-quater - Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici

Codice Penale, art. 617-quater - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Codice Penale, art. 617-quinquies - Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Codice Penale, art. 640-quinquies - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Codice Penale, art. 635-bis - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Codice Penale, art. 635-ter - Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico

Codice Penale, art. 635-quater - Danneggiamento di sistemi informatici o telematici

Codice Penale, art. 635-quinquies - Danneggiamento di sistemi informatici o telematici di pubblico interesse

Codice Penale, art. 491-bis - Documenti informatici

Codice Penale, art. 635-quater.1 - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Codice Penale, art. 629 - Estorsione

Protocolli di prevenzione:

- Procedure - Accesso a sistemi e applicazioni IT

Procedure: disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante. Devono essere definite, aggiornate e approvate formalmente le policy aziendali, le procedure in materia di sicurezza informatica/telematica e il regolamento sull'utilizzo delle risorse informatiche aziendali e ne deve assicurare la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione con particolare riferimento ai requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e all'accesso remoto da parte di terzi soggetti. La definizione dei profili di autorizzazione agli applicativi e ai sistemi informativi avviene nel rispetto del principio del minimo privilegio, limitando i diritti di accesso a quanto strettamente necessario per lo svolgimento delle mansioni assegnate. Per gli account amministrativi e per gli accessi a sistemi o applicazioni ritenuti critici, la Società può prevedere l'utilizzo di meccanismi di autenticazione rafforzata, secondo quanto stabilito dalle procedure IT interne.

La creazione, la modifica e la revoca degli account utente e dei relativi profili di autorizzazione avvengono sulla base di richieste formalizzate e tracciate; in particolare, la revoca degli account dei soggetti cessati o trasferiti ad altre funzioni è effettuata in tempi coerenti con le procedure interne, al fine di prevenire utilizzi non autorizzati delle credenziali.

- Segregazione dei compiti - Accessi locali e sistemi IT

Segregazione dei compiti: separare, ove concretamente praticabile, le attività di autorizzazione, esecuzione e controllo. Quando ciò non sia praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, fermi gli obblighi inderogabili. Si richiede che: i) sia rispettato il sistema di gestione delle utenze, con particolare riferimento alla definizione di nuove utenze e della loro

cancellazione; ii) sia effettuata una verifica periodica dei profili di accesso, di concessione di utenze e della modifica dei profili; l'identificazione dell'utente per l'accesso alle informazioni avvenga attraverso un identificativo univoco preventivamente assegnatogli.

- Tracciabilità - Accesso sistemi e infrastrutture IT

Si richiede che: i) sia assicurata la tracciabilità delle persone che hanno avuto accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT; ii) la documentazione riguardante le attività sia conservata, ad opera del Responsabile della Funzione coinvolta, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

- Ruoli e responsabilità - Accesso a sistemi IT e applicazioni

Ruoli e Responsabilità : è fatto espresso divieto di i ) introdursi abusivamente o permanere contro la volontà espressa o tacita dell 'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza; (ii) procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo (iii) distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda; (iv) distruggere, danneggiare, rendere in tutto o in parte inservibile sistemi informatici o telematici altrui o della Società ovvero ostacolarne gravemente il funzionamento; (v) intercettare fraudolentemente, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi; (vi) rivelare, mediante qualsiasi mezzo di informazione al pubblico , il contenuto delle comunicazioni fraudolentemente intercettate relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

- Misure operative

- Il responsabile richiede per iscritto accessi coerenti con mansioni e necessità
- La Direzione gestionale, con il supporto dei soggetti esterni incaricati, abilita credenziali personali e livello minimo necessario.
- AU e la Direzione gestionale, con il supporto dei soggetti esterni incaricati, riesaminano almeno semestralmente utenze privilegiate, inattive e fornitori
- alla cessazione o cambio ruolo la funzione responsabile comunica tempestivamente e la Direzione gestionale, tramite i soggetti incaricati, dispone la revoca o l'adeguamento.
- Sono vietati scambio di password, account condivisi non giustificati e accessi alle cartelle senza necessità
- eventi anomali sono esaminati dalla Direzione gestionale con il supporto dei soggetti esterni incaricati, secondo le rispettive competenze.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni

Gli incidenti informatici e le violazioni di dati personali che possano presentare profili rilevanti ai fini del D.Lgs. 231/2001 sono comunicati tempestivamente all'OdV dalla decorrenza dell'incarico, nel rispetto della riservatezza e della minimizzazione dei dati. Restano distinti gli eventuali obblighi di notifica all'autorità e di comunicazione agli interessati, da valutare secondo i presupposti e i termini degli artt. 33 e 34 del Regolamento (UE) 2016/679.

**Evidenze e tracciabilità:**

Richieste, autorizzazioni, inventario utenze, log, verifiche e revoche.

**Flussi informativi verso l'Organismo di Vigilanza:**

Accessi non autorizzati, mancata revoca o incidente: tempestivo; report semestrale.

### 7.5 Area di Rischio n. 16: Gestione, tenuta dell'inventario e/o configurazione dei prodotti hardware, software, banche dati ed altre opere dell'ingegno strumentali all'attività societaria, con particolare riguardo alla presenza e validità di licenze d'uso.

Attività sensibili:

- gestione dei sistemi informatici;

- accesso e trattamento dei dati;

- sicurezza informatica;

- gestione delle credenziali di accesso.

**Funzioni coinvolte nelle attività sensibili:**

DG; AMM; soggetti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

L. 633/1941, art. 171 - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-bis - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-ter - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-septies - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

L. 633/1941, art. 171-octies - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 493-quater - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti

Codice Penale, art. 635-quater.1 - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Protocolli di prevenzione:

- Procedure - Inventario IT e licenze d'uso

Procedure: disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili. Deve essere adottata una procedura che gestisca l'inventario degli asset a supporto delle attività di gestione , che permetta di mantenere la visibilità dello stato delle risorse e ne faciliti la manutenzione , l'implementazione e la gestione e manutenzione di reti. Tale inventario deve includere, tra l'altro, per ogni asset censito le informazioni sulle funzionalità e sulle tipologie di dati gestiti (fornitori, clienti, etc.), sul responsabile funzionale e sul soggetto incaricato dei sistemi informatici, sulle misure di sicurezza minime previste anche per evitare possibili commissioni di reati. Occorre inoltre dare evidenza dei soggetti che effettuano la manutenzione hardware e software degli asset aziendali dandone opportuna informazione all'Organismo di Vigilanza. La Società tiene un inventario aggiornato delle principali dotazioni hardware (quali, a titolo esemplificativo, server, personal computer, notebook, dispositivi mobili, apparati di rete e supporti rimovibili), nel quale sono indicati, per quanto possibile, il soggetto assegnatario e le informazioni essenziali per la loro identificazione. L'utilizzo di dispositivi esterni di memorizzazione (come chiavette USB e dischi esterni) è disciplinato dalle procedure interne, che possono prevedere limitazioni tecniche e organizzative, nonché il divieto di utilizzo di dispositivi non autorizzati. L'assegnazione e l'utilizzo di smartphone e di altri dispositivi mobili aziendali avvengono nel rispetto delle regole interne in materia di sicurezza (aggiornamenti, protezione mediante credenziali, modalità sicure di connessione ai sistemi aziendali).

- Ruoli e responsabilità - Inventario IT e licenze d'uso

Ruoli e Responsabilità: devono essere promossi controlli finalizzati a garantire la gestione e la manutenzione hardware e software (ivi compresi l'inventario e i divieti o limitazioni di utilizzo) e deve attivare procedure di controllo di installazione di software potenzialmente pericolosi sui sistemi operativi. È fatto espresso divieto di: i) accedere in maniera non autorizzata ai sistemi informativi utilizzati da soggetti privati o dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare informazioni a vantaggio dell'azienda o di terzi, o comunque al fine di procurare un indebito vantaggio all'azienda od a terzi; ii) distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda ; iii) distruggere,

danneggiare, rendere in tutto o in parte inservibile sistemi informatici o telematici altrui o della Società ovvero ostacolarne gravemente il funzionamento; iv) utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio virus, worm, troian, spyware, dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, v) porre in essere azioni idonee a commettere reati, in particolare riguardanti strumenti di pagamento diversi dai contanti.

- Tracciabilità - Inventario IT e licenze d'uso

I software e i servizi informatici utilizzati dalla Società sono censiti in un inventario aggiornato, con indicazione del fornitore, del titolo e delle condizioni di utilizzo, degli eventuali limiti, della data di attivazione e delle scadenze o dei rinnovi, ove previsti. Sono documentate le verifiche periodiche sulle licenze, comprese quelle gratuite o open source, e conservati i relativi contratti o altri titoli d'uso.

- Procedure - Software e diritti di terzi

La Società adotta una procedura per l'acquisizione, l'utilizzo, il rinnovo e la dismissione dei software e delle banche dati impiegati nell'attività aziendale. La procedura individua le funzioni responsabili e prevede:

i) la preventiva verifica della provenienza, del titolo d'uso e delle condizioni contrattuali applicabili, comprese le eventuali licenze open source;

ii) l'inventario dei programmi e dei servizi utilizzati, con indicazione del fornitore, della tipologia di licenza, delle eventuali scadenze, dei limiti d'uso e dei soggetti o dispositivi autorizzati, ove applicabile;

iii) il controllo delle installazioni e degli accessi, con divieto di utilizzare copie abusive o programmi non autorizzati;

iv) la verifica periodica della validità delle licenze e degli eventuali canoni o corrispettivi dovuti secondo contratto;

v) la conservazione della documentazione contrattuale e delle evidenze dei controlli;

vi) la comunicazione all'Organismo di Vigilanza, dalla decorrenza del suo incarico, delle irregolarità rilevanti ai fini del Modello, secondo i flussi informativi previsti.

Qualora la Società affidi a terzi lo sviluppo o la personalizzazione di software, i relativi contratti disciplinano i diritti di utilizzo, i componenti di terzi e le condizioni delle licenze applicabili.

- Misure operative

- La Direzione gestionale, con il supporto dei soggetti esterni incaricati, censisce assegnatario, configurazione e ubicazione, applica aggiornamenti e protezioni e controlla periodicamente la corrispondenza con l'inventario.
- Consegna e restituzione sono tracciate
- dispositivi dismessi sono cancellati in modo sicuro e smaltiti da soggetti idonei.
- Fornitori cloud e manutentori sono valutati per sicurezza, ruoli privacy, accessi e continuità
- le deroghe sono autorizzate e motivate.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività di accesso e dei profili di autorizzazione ai sistemi informatici e/o telematici e alle applicazioni

Gli incidenti informatici e le violazioni di dati personali che possano presentare profili rilevanti ai fini del D.Lgs. 231/2001 sono comunicati tempestivamente all'OdV dalla decorrenza dell'incarico, nel rispetto della riservatezza e della minimizzazione dei dati. Restano distinti gli eventuali obblighi di notifica all'autorità e di comunicazione agli interessati, da valutare secondo i presupposti e i termini degli artt. 33 e 34 del Regolamento (UE) 2016/679.

Gestione degli incidenti informatici

La Società adotta specifiche procedure per la gestione degli incidenti informatici, intesi come eventi, anche solo sospetti, che possano compromettere la riservatezza, l'integrità o la disponibilità dei dati e dei sistemi informativi aziendali. Tali procedure definiscono i ruoli e le responsabilità dei soggetti coinvolti, le modalità di segnalazione interna degli incidenti, i flussi informativi verso le funzioni competenti e, ove necessario, verso l'Organismo di Vigilanza, nonché le principali azioni da

intraprendere per contenere e rimuovere gli effetti dell'incidente. La gestione degli incidenti informatici prevede, altresì, la conservazione delle evidenze rilevanti (quali, a titolo esemplificativo, log di sistema, file e comunicazioni elettroniche) secondo modalità idonee a garantirne integrità e tracciabilità, nonché la successiva analisi degli eventi, al fine di individuare eventuali misure correttive e di miglioramento dei presidi di sicurezza.

**Evidenze e tracciabilità:**

Inventari, verbali di consegna, contratti, cancellazioni e controlli.

**Flussi informativi verso l'Organismo di Vigilanza:**

Furti, perdite o dismissioni irregolari: tempestivo; verifica annuale.

## 8 Ambito: Gestione delle risorse umane

### 8.1 Area di Rischio n. 17: Approvvigionamento di servizi che prevedono l'utilizzo di manodopera indiretta.

Attività sensibili:

- selezione, assunzione, valutazione, impiego, remunerazione e incentivazione del personale.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; CS; DL; RQ

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 609-undecies - Adescamento di Minorenni

Codice Penale, art. 600 - Riduzione o mantenimento in schiavitù o in servitù

Codice Penale, art. 600 bis c.1 - Prostituzione Minorile

Codice Penale, art. 600 bis c.2 - Prostituzione Minorile

Codice Penale, art. 600-ter c. 1-2 - Pornografia Minorile

Codice Penale, art. 600-ter c. 3-4 - Pornografia Minorile

Codice Penale, art. 600-quater - Detenzione o accesso a materiale pornografico

Codice Penale, art. 600-quater 1 - Pornografia Virtuale

Codice Penale, art. 600 quinquies - Iniziative turistiche volte allo sfruttamento della prostituzione minorile

Codice Penale, art. 601 - Tratta di persone

Codice Penale, art. 602 - Acquisto e alienazione di schiavi

Codice Penale, art. 603-bis - Intermediazione illecita e sfruttamento del lavoro

Protocolli di prevenzione:

Per la sicurezza nelle attività affidate a terzi, la documentazione aziendale comprende un DUVRI relativo al servizio di pulizia e i contratti dei servizi esternalizzati. Le misure di cooperazione e coordinamento si applicano ai singoli affidamenti secondo i rispettivi presupposti di legge.

- Procedure - Approvvigionamento di servizi che prevedono l'utilizzo di manodopera indiretta

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità dei soggetti coinvolti nella gestione delle ditte appaltatrici; ii) modalità e tempistiche per lo svolgimento dei controlli sulla controparte; iii) obbligo di effettuare verifiche in merito alla regolarità contributiva e retributiva (es. tramite richiesta del DURC) prima di effettuare il pagamento dei corrispettivi della prestazione; iv) effettuazione di verifiche in merito alla regolarità fiscale (es. versamenti IVA, versamenti ritenute fiscali); v) indicazione delle modalità per segnalare alle funzioni aziendali competenti eventuali criticità rilevate; vi) dichiarazione da parte dell'affidatario del servizio di essere in piena regola con la vigente normativa e contrattualistica collettiva in materia assicurativa, contributiva, retributiva, previdenziale e di adempiere a tutti gli oneri assicurativi e previdenziali relativi ai propri dipendenti; vii) modalità di archiviazione della documentazione rilevante prodotta.

- Ruoli e responsabilità - servizi che prevedono l'utilizzo di manodopera indiretta

Ruoli e Responsabilità: devono essere assegnati ruoli e responsabilità dei soggetti coinvolti nelle diverse fasi del processo sensibile (es. scelta della controparte per la stipula del contratto, monitoraggio controparte, approvazione esecuzione lavori e pagamento fatture).

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Segregazione dei compiti

Deve essere assicurata, ove concretamente praticabile, la separazione dei compiti fra le funzioni coinvolte nelle attività autorizzative, esecutive e di controllo. Quando ciò non sia concretamente praticabile, l'AU dispone verifiche compensative documentate, ferme le attribuzioni e i controlli inderogabili previsti dalla legge.

- Procure e deleghe - Contratti

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Lo standard richiede che i soggetti che firmano i contratti devono essere muniti di appositi poteri autorizzativi.

- Previsione di clausole nei contratti con fornitori

Contratti: devono essere previste, nei contratti con i fornitori di: i) specifiche clausole con cui detti terzi dichiarino di conoscere e si obblighino a rispettare i principi contenuti nel Codice Etico/Modello Organizzativo; ii) clausole risolutive espresse che attribuiscano alla Società la facoltà di risolvere i contratti in questione in caso di violazione di tale obbligo.

- Misure operative

- Prima dell'affidamento AU verifica requisiti tecnico-professionali, regolarità contributiva quando dovuta, organizzazione e congruità dell'offerta.
- Il contratto descrive personale, prestazioni, obblighi di sicurezza e divieto di subaffidamenti non autorizzati
- DL attua coordinamento e DUVRI ove previsto.
- CS e referente contratto controllano accessi, turni, prestazioni e segnali di sfruttamento o irregolarità
- anomalie producono contestazione e misure documentate.

**Evidenze e tracciabilità:**

Contratti, verifiche requisiti, DURC ove dovuto, coordinamento e controlli servizio.

**Flussi informativi verso l'Organismo di Vigilanza:**

Sospetto sfruttamento, irregolarità gravi, infortuni o subaffidamenti non autorizzati: senza ritardo.

### 8.2 Area di Rischio n. 18: Assunzione del personale e gestione delle note spese.

Attività sensibili:

- selezione, assunzione, valutazione, impiego, remunerazione e incentivazione del personale.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; DG; CS; eventuali consulenti esterni incaricati

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

Codice Penale, art. 630 - Sequestro di persona a scopo di rapina o di estorsione

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 270-bis (nel caso di pena inferiore a 10 anni di reclusione) - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

Codice Penale, art. 270-bis (nel caso di pena non inferiore a 10 anni di reclusione) - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico

Codice Penale, art. 270-ter (nel caso di pena inferiore a 10 anni di reclusione) - Assistenza agli associati

Codice Penale, art. 270-ter (nel caso di pena non inferiore a 10 anni di reclusione) - Assistenza agli associati

Codice Penale, art. 270-quater (nel caso di pena inferiore a 10 anni di reclusione) - Arruolamento con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quater (nel caso di pena non inferiore a 10 anni di reclusione) - Arruolamento con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quinquies (nel caso di pena inferiore a 10 anni di reclusione) - Addestramento ad attività con finalità di terrorismo anche internazionale

Codice Penale, art. 270-quinquies (nel caso di pena non inferiore a 10 anni di reclusione) - Addestramento ad attività con finalità di terrorismo anche internazionale

Codice Penale, art. 270-sexies (nel caso di pena inferiore a 10 anni di reclusione) - Condotte con finalità di terrorismo

Codice Penale, art. 270-sexies (nel caso di pena non inferiore a 10 anni di reclusione) - Condotte con finalità di terrorismo

Codice Penale, art. 280 (nel caso di pena inferiore a 10 anni di reclusione) - Attentato per finalità terroristiche o di eversione

Codice Penale, art. 280 (nel caso di pena non inferiore a 10 anni di reclusione) - Attentato per finalità terroristiche o di eversione

Codice Penale, art. 280-bis (nel caso di pena inferiore a 10 anni di reclusione) - Atto di terrorismo con ordigni micidiali o esplosivi

Codice Penale, art. 280-bis (nel caso di pena non inferiore a 10 anni di reclusione) - Atto di terrorismo con ordigni micidiali o esplosivi

Codice Penale, art. 302 (nel caso di pena inferiore a 10 anni di reclusione) - Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo

Codice Penale, art. 302 (nel caso di pena non inferiore a 10 anni di reclusione) - Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo

D.L. 625/1979 convertito L. 15/1980, art. 1 - Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica

Codice Penale, art. 583-bis - Pratiche di mutilazione degli organi genitali femminili

Codice Penale, art. 648-ter 1 - Autoriciclaggio

D.lgs. 25 luglio 1998, n. 286 (T.U. sull'immigrazione), art. 22 c.12 bis - Impiego di lavoratori irregolari

D.lgs. 25 luglio 1998, n. 286 (T.U. sull'immigrazione), art. 12 c.3, 3-bis, 3-ter - Disposizioni contro le immigrazioni clandestine

D.lgs. 25 luglio 1998, n. 286 (T.U. sull'immigrazione), art. 12 c.5 - Disposizioni contro le immigrazioni clandestine

Codice Penale, art. 648 bis - Riciclaggio

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita

Codice Penale, art. 648 - Ricettazione

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 493-ter - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Protocolli di prevenzione:

- Procedure - Assunzione del personale e gestione delle note spese

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli, responsabilità, modalità operative delle Funzioni coinvolte nella gestione del processo in oggetto; ii) ruoli e responsabilità e modalità operative per lo svolgimento di controlli in merito all'onorabilità e professionalità del candidato iii) descrizione delle singole fasi del processo (es. nascita dell'esigenza di assunzione, definizione e autorizzazione della richiesta di assunzione del personale, ricerca delle candidature, selezione delle risorse, assunzione del candidato ed inserimento in azienda, ecc.); iv) definizione e inquadramento delle posizioni per il nuovo personale (personale di sede, personale tecnico o dirigenti); v) approvazione dell'assunzione (RAL, benefit, bonus, ecc.) del personale dirigente da parte dell'organo amministrativo della Società; vi) modalità di archiviazione della documentazione rilevante prodotta; vii) richiesta di permesso di soggiorno a candidati provenienti da paesi extra-UE e relativo monitoraggio per eventuali rinnovi.

- Segregazione dei compiti - Assunzione di personale

Ove concretamente praticabile, deve essere garantita la segregazione delle funzioni coinvolte nel processo di richiesta di assunzione di personale e in quello di valutazione/selezione del personale stesso. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità - Assunzione del personale e gestione delle note spese

Devono essere definite le modalità e delle tempistiche di archiviazione e conservazione della documentazione rilevante per le principali fasi dell'attività sensibile. Il processo di selezione/assunzione deve essere adeguatamente documentato, motivato ed approvato, e la documentazione conservata in apposito archivio cartaceo e/o elettronico presso l'Ufficio della Funzione Competente.

- Procure e deleghe - Assunzioni

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate

spese specificando i limiti e la natura delle spese. Procure e deleghe: solo i soggetti muniti di apposita procura sono autorizzati a firmare le assunzioni.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile

- Procedure - Strumenti di pagamento e Note spese

Deve essere adottata una specifica procedura per la gestione degli strumenti di pagamento e delle note spese che includa, tra l'altro: i) il rilascio di carte di credito, di debito e prepagate effettuato esclusivamente da istituti bancari autorizzati e operanti su circuiti riconosciuti in ambito nazionale ed internazionale, ii) l'acquisizione della documentazione (contratto, estratti conto) relativi alle carte aziendali, iii) l'indicazione del/i soggetto/i autorizzato/i per il compimento delle transazioni tramite strumenti di pagamento virtuali e delle limitazioni nel loro utilizzo, iii) l'indicazione di soglie (settimanali o mensili) massime di utilizzo e/o delle categorie merceologiche acquistabili tramite strumenti di pagamento virtuali, iv) l'eventuale utilizzo di piattaforme relative a monete virtuali, esclusivamente se munite di autorizzazione e regolarmente operanti in ambito nazionale ed internazionale, v) la trasmissione all'Organismo di Vigilanza di tutta la documentazione contrattuale e bancarie relativa alle carte aziendali e alle piattaforme di valuta virtuale, vi) la formazione del personale in merito al corretto utilizzo degli strumenti di pagamento.

- Misure operative

- Il fabbisogno è motivato
- AMM raccoglie candidature, verifica titoli, eventuali iscrizioni e titolo di soggiorno ove richiesto e conserva criteri e decisioni.
- CS registra turni e presenze
- AMM e consulente confrontano presenze, cedolini, pagamenti e versamenti
- anomalie sono corrette e tracciate.
- Rimborsi sono documentati e autorizzati da soggetto diverso dal richiedente, o con verifica compensativa
- è vietato assumere o rimborsare per ottenere favori indebiti.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Assunzione del personale e gestione delle note spese

il Responsabile competente comunichi all'Organismo di Vigilanza eventuali assunzioni effettuate in deroga alle procedure in vigore.

**Evidenze e tracciabilità:**

Fascicoli, contratti, verifiche, turni, cedolini, note spese, pagamenti.

**Flussi informativi verso l'Organismo di Vigilanza:**

Irregolarità retributive, documentali o assunzioni sospette: tempestivo; riepilogo semestrale.

### 8.3 Area di Rischio n. 19: Definizione dei requisiti di competenza, abilità e consapevolezza dei lavoratori.

Attività sensibili:

- selezione, assunzione, valutazione, impiego, remunerazione e incentivazione del personale.

**Funzioni coinvolte nelle attività sensibili:**

AU; DG; RS; CS; AMM; RQ; DL

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

- Procedure - Requisiti di competenza, abilità e consapevolezza dei lavoratori

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) sono previste attività di informazione e formazione di tutto il personale circa le corrette modalità di espletamento dei propri incarichi, nonché nei casi previsti dalla normativa; ii) devono essere organizzati i corsi di formazione e addestramento necessari in funzione del programma formativo approvato dal Datore di Lavoro; iii) devono essere segnalati eventuali carenze formative, informative e relative all'addestramento del personale in funzione dei rischi a cui è esposto e delle mansioni assegnate; iv) la Società si avvale delle funzioni di competenza per l'individuazione, divulgazione e monitoraggio dei requisiti di competenza, abilità e consapevolezza necessari per lo svolgimento delle attività aziendali; v) la funzione amministrativa (AMM), con il supporto di eventuali consulenti esterni incaricati, provvede a comunicare nuove assunzioni e cambio mansioni, per l'individuazione dei lavoratori da sottoporre alle attività formative; vi) la Società provvede a monitorare le esigenze formative attraverso uno scadenziario con le schede relative a ciascun lavoratore; vii) gli attestati e certificazioni di formazione del personale sono archiviati.

- Documentazione e correttezza dichiarazioni

Deve essere posta la massima attenzione affinché informazioni e dati indicati nelle dichiarazioni siano corretti e veritieri e adeguatamente documentati.

- Segregazione dei compiti - Organizzazione

Il processo è condotto assicurando, ove concretamente praticabile, la separazione fra attività autorizzative, esecutive e di controllo. Quando la separazione non sia concretamente praticabile, l'AU dispone verifiche compensative documentate; restano ferme le attribuzioni, le incompatibilità e i controlli inderogabili previsti dalla legge.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile.

- Misure operative

- RS e AMM verificano prima dell'impiego titoli, iscrizioni e requisiti professionali, controllando scadenze e sospensioni nei limiti di legge.
- CS programma turni e sostituzioni coerenti con qualifiche, fabbisogno e requisiti autorizzativi
- scoperture sono documentate ed escalation immediata a DG e RS.
- AU approva piano formativo per ruolo e turno
- RQ conserva contenuti, presenze, recuperi e valutazione dell'apprendimento, incluse sicurezza, tutela ospiti e 231.

**Evidenze e tracciabilità:**

Fascicoli titoli, turni, scadenziario, piani e registri di formazione.

**Flussi informativi verso l'Organismo di Vigilanza:**

Mancanza di requisiti, scoperture significative o formazione obbligatoria omessa: tempestivo; report semestrale.

## 9 Ambito: Rapporti con le pubbliche amministrazioni

### 9.1 Area di Rischio n. 20: Gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici, e di partecipazione a gare nei pubblici incanti o nelle licitazioni private per conto di Pubbliche Amministrazioni.

Attività sensibili:

- rapporti con la P.A.;

- gestione di gare e appalti pubblici;

- ottenimento di autorizzazioni;

- gestione delle pratiche amministrative.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; RQ; consulenti

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 416 (escluso c. 6) - Associazione per delinquere

Codice Penale, art. 416-bis - Associazioni di tipo mafioso anche straniere

Codice Penale, art. 416 c. 6 - Associazione per delinquere

Codice Penale, art. 416-ter - Scambio elettorale politico-mafioso

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 648 - Ricettazione

Codice Penale, art. 648 bis - Riciclaggio

Codice Penale, art. 648-ter - Impiego di denaro, beni o utilità di provenienza illecita

Codice Penale, art. 648-ter 1 - Autoriciclaggio

L. 898/1986, art. 2 - Percezione indebita di contributi del Fondo europeo agricolo di orientamento e garanzia o del Fondo europeo agricolo per lo sviluppo rurale

Codice Penale, art. 353 - Turbata liberta' degli incanti

Codice Penale, art. 353-bis - Turbata liberta' del procedimento di scelta del contraente

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Protocolli di prevenzione:

- Segregazione dei compiti - Contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici

Ove concretamente praticabile, deve essere garantita l’esistenza di segregazione tra chi predispone le richieste di finanziamento/rendicontazione delle spese, chi ne verifica il contenuto e provvede alla loro autorizzazione, trasmettendole all’Ente Erogatore / Ente Istruttore e chi ne rendiconta l’utilizzo. Quando

la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Procedure - Rapporti con la pubblica amministrazione per concessioni, contributi/finanziamenti

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità delle funzioni coinvolte nella gestione delle richieste; ii) modalità operative e di controllo nella gestione dei contributi/finanziamenti; iii) modalità di tracciabilità dell'intero processo (ad esempio mediante una scheda di evidenza contenente il tipo di contributo/finanziamento/agevolazione, il soggetto pubblico erogante, il responsabile interno, i collaboratori/Partner esterni coinvolti, stato di avanzamento, ecc.) inclusa sia la documentazione relativa all'iter decisionale e alle relative motivazioni sia la formalizzazione dei principali contatti/incontri con soggetti pubblici (quali, ad esempio, i contatti preliminari, i chiarimenti in fase di istruttoria, ispezioni, i chiarimenti in fase di rendicontazione del finanziamento); iv) modalità di archiviazione della documentazione rilevante.

- Misure operative

- La funzione competente verifica requisiti effettivi, bando, condizioni, spese ammissibili e assenza di conflitti
- AU autorizza domanda e firma.
- AMM conserva documentazione di supporto e tiene distinta evidenza della destinazione delle risorse
- un soggetto diverso verifica i dati prima della trasmissione; se la separazione non è praticabile, si applica il controllo compensativo documentato previsto al paragrafo 1.1.
- Scostamenti, variazioni e recuperi sono gestiti secondo le regole dell'ente erogante
- non si rappresentano spese inesistenti né si usano fondi per scopi diversi.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici

Predisposizione e l'aggiornamento di un report riepilogativo delle domande di finanziamento presentate nel periodo di riferimento da trasmettere con cadenza periodica all'Alta Direzione e/o all'Organismo di Vigilanza che contenga per ciascuna verifica elementi quali la tipologia di finanziamento, l'Organo Pubblico coinvolto, eventuali Partner, ecc..

**Evidenze e tracciabilità:**

Bandi, domande, allegati, autorizzazioni, rendiconti, controlli, ricevute.

**Flussi informativi verso l'Organismo di Vigilanza:**

Revoche, contestazioni e anomalie: senza ritardo; riepilogo semestrale.

### 9.2 Area di Rischio n. 21: Gestione di rapporti con funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla Pubblica Amministrazione e/o da incaricati di Pubblico servizio.

Attività sensibili:

- rapporti con la P.A.

**Funzioni coinvolte nelle attività sensibili:**

AU; DG; RS; CS; RQ; AMM

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 316 - Peculato mediante profitto dell'errore altrui

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 316 - Peculato mediante profitto dell'errore altrui

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 346-bis - Traffico di influenze illecite

Protocolli di prevenzione:

- Procedure - Rapporti con la pubblica amministrazione per attività ispettive

La Società disciplina l’attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) definizione delle responsabilità, in capo ai Responsabili delle Funzioni coinvolte, di curare la gestione dei contatti con i componenti dell’Ente Ispettivo; ii) definizione delle responsabilità, in capo ai Responsabili delle Funzioni

coinvolte, di verificare i contenuti del verbale finale di ispezione redatto dall'Organo Ispettivo e provvedere alla controfirma dello stesso; iii) obbligo, in capo ai soggetti incaricati per la gestione dell'ispezione, di prestare la massima collaborazione e trasparenza nei rapporti con l'Ente Ispettivo, di assicurare sempre la presenza di almeno due soggetti aziendali durante le operazioni ispettive, nonché di garantire la correttezza, veridicità ed aggiornamento delle informazioni fornite; iv) istituzione ed aggiornamento, a cura del Responsabile identificato, di un registro delle visite ispettive (indicante, per ciascuna verifica, le informazioni essenziali quali, ad esempio: oggetto della verifica, Ente Ispettivo, periodo di riferimento, elenco della documentazione richiesta e consegnata, eventuali rilievi/sanzioni/prescrizioni); v) trasmissione all'Organismo di Vigilanza con cadenza periodica, a cura del Responsabile competente, delle informazioni contenute nel verbale; vii) modalità di archiviazione della documentazione rilevante prodotta.

- Segregazione dei compiti - Rapporti con la pubblica amministrazione nelle attività ispettive

Ove concretamente praticabile, deve essere garantita la segregazione tra chi gestisce i rapporti con la PA durante le fasi ispettive e chi ha il compito di supervisionarne lo svolgimento e firmare il verbale ispettivo. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità - Rapporti con la pubblica amministrazione nelle attività ispettive

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate. Le principali fasi del processo in oggetto devono essere opportunamente documentate ed archiviate, in versione cartacea e/o elettronica, presso gli Uffici delle Funzioni competenti (es. elenco documentazione prodotta dall'Ente Ispettivo, copia del verbale di ispezione ecc.).

- Misure operative

- Il referente riceve e identifica gli ispettori, informa AU e funzione competente e registra oggetto, richieste e documenti consegnati.
- La Società collabora, consegna dati veri e completi e conserva copia di verbali
- sono vietate promesse, regali indebiti, alterazioni od occultamenti.
- AU attribuisce ogni prescrizione a un responsabile con termine, azione e prova di chiusura
- RQ verifica gli adempimenti ed eventuali comunicazioni all'ente.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio:

- Gestione di rapporti con funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla Pubblica Amministrazione e/o da incaricati di Pubblico servizio

Predisposizione e l'aggiornamento di un report riepilogativo delle verifiche ispettive ricevute nel periodo di riferimento da trasmettere con cadenza periodica all'Organismo di Vigilanza; tale report deve contenere per ciascuna verifica elementi quali l'oggetto, l'Ente Ispettivo (es. Guardia di Finanza, Ispettorato del Lavoro ecc.), il periodo di riferimento, l'elenco della documentazione richiesta e consegnata, l'elenco della documentazione eventualmente non consegnata, in quanto non disponibile ed eventuali rilievi/sanzioni/prescrizioni.

- Raccolta, elaborazione e presentazione a soggetti pubblici o a soggetti incaricati di pubblico servizio della documentazione tecnica, economica ed amministrativa necessaria all'ottenimento e mantenimento di certificazioni, autorizzazioni, licenze, concessioni e provvedimenti amministrativi per l'esercizio delle attività aziendali

Predisposizione e aggiornamento di un report riepilogativo delle istanze presentate nel periodo di riferimento da trasmettere con cadenza periodica all'Alta Direzione e/o all'Organismo di Vigilanza che contenga per ciascuna verifica elementi quali la tipologia di autorizzazione o l'Organo Pubblico coinvolto.

**Evidenze e tracciabilità:**

Registro visite, richieste, verbali, prescrizioni, piano di rimedio e prove di chiusura.

**Flussi informativi verso l'Organismo di Vigilanza:**

Accessi, rilievi gravi e prescrizioni: tempestivo; stato rimedi trimestrale.

### 9.3 Area di Rischio n. 22: Gestione pre-conteziosi, contenziosi giudiziali e/o stragiudiziali, nonché gestione dei rapporti con le Autorità Giudiziarie.

Attività sensibili:

- rapporti con la P.A..

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; soggetti esterni incaricati ove necessario; funzioni interessate

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 377 bis - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 316 - Peculato mediante profitto dell'errore altrui

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 346-bis - Traffico di influenze illecite

Protocolli di prevenzione:

- Procedure - Rapporti con l'autorità giudiziaria - Incarico a studio legale esterno

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità dei soggetti coinvolti; ii) autorizzazione, a cura dell'Amministratore unico, del mandato alle liti da conferirsi al Legale esterno; iii) obbligo di improntare i rapporti con l'Autorità Giudiziaria e con la Pubblica Amministrazione nell'ambito dei contenziosi giudiziali e dei rapporti con la Magistratura ai principi di correttezza, trasparenza e tracciabilità; iv) supervisione, a cura del Responsabile della Funzione coinvolta nel procedimento, dell'operato dei professionisti esterni; v) verifica e autorizzazione,

da parte dei soggetti muniti dei necessari poteri, delle parcelle relative alle prestazioni ricevute dal professionista incaricato; vi) valutazione di congruità della parcella del legale esterno incaricato al momento della certificazione della prestazione del professionista; vi) modalità di archiviazione della documentazione rilevante prodotta.

- Ruoli e responsabilità - Rapporti con soggetti pubblici o autorità giudiziaria

Ruoli e Responsabilità: deve essere garantita (i) la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile e/o intrattengono rapporti con soggetti pubblici (ii) il monitoraggio sull'avanzamento del progetto di finanziamento (a seguito dell'ottenimento del contributo pubblico) e sul relativo reporting alla Pubblica Amministrazione, con evidenza e gestione delle eventuali anomalie (iii) i controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati.

- Misure operative

- AU conferisce incarichi scritti e motivati a professionisti qualificati con compensi congrui
- AMM controlla prestazioni e fatture.
- Le funzioni conservano atti e prove senza cancellazioni o manipolazioni
- ogni richiesta dell'autorità è gestita dalle persone autorizzate.
- Sono vietate pressioni su testimoni, compensi occulti o accordi indebiti
- il diritto di difesa e la riservatezza delle comunicazioni difensive sono salvaguardati.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Gestione pre-conteziosi, contenziosi giudiziali e/o stragiudiziali, nonché gestione dei rapporti con le Autorità Giudiziarie

Predisposizione di un'informativa periodica, contenente l'indicazione dei contenziosi in corso, di quelli chiusi e di quelli da avviare, da trasmettere periodicamente all'Alta Direzione e/o all'Organismo di Vigilanza da parte delle Funzioni interessate. Prevede inoltre un'informativa all'Organismo di Vigilanza nel caso in cui la Società sia coinvolta in un procedimento ai sensi del D.Lgs. 231/01, ivi compresa la nomina del legale esterno.

**Evidenze e tracciabilità:**

Mandati, parcelle, atti, registri di conservazione e comunicazioni pertinenti.

**Flussi informativi verso l'Organismo di Vigilanza:**

Procedimenti potenzialmente 231 e condotte indebite: senza ritardo nel rispetto del segreto difensivo.

### 9.4 Area di Rischio n. 23: Raccolta, elaborazione e presentazione a soggetti pubblici o a soggetti incaricati di pubblico servizio della documentazione tecnica, economica ed amministrativa necessaria all'ottenimento e mantenimento di certificazioni, autorizzazioni, licenze, concessioni e provvedimenti amministrativi per l'esercizio delle attività aziendali.

Attività sensibili:

- rapporti con la P.A.;

- gestione di gare e appalti pubblici;

- ottenimento di autorizzazioni;

- gestione delle pratiche amministrative.

**Funzioni coinvolte nelle attività sensibili:**

AU; RQ; DG; RS; AS; AMM

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 316 bis - Malversazione di erogazioni pubbliche

Codice Penale, art. 316-ter - Indebita percezione di erogazioni pubbliche

Codice Penale, art. 640 - Truffa

Codice Penale, art. 640-bis - Truffa aggravata per il conseguimento di erogazioni pubbliche

Codice Penale, art. 640-ter - Frode informatica

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 346-bis - Traffico di influenze illecite

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 353 - Turbata liberta' degli incanti

Codice Penale, art. 353-bis - Turbata liberta' del procedimento di scelta del contraente

Codice Penale, art. 512-bis - Trasferimento fraudolento di valori

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Codice Penale, art. 317 - Concussione

Codice Penale, art. 319-bis - Corruzione aggravata per un atto contrario ai doveri d'ufficio

Codice Penale, art. 320 - Corruzione di persona incaricata di un pubblico servizio

Codice Penale, art. 319-ter c.1 - Corruzione in atti giudiziari

Codice Penale, art. 319-ter c.2 - Corruzione in atti giudiziari

Codice Penale, art. 318 - Corruzione per l'esercizio della funzione

Codice Penale, art. 319 - Corruzione per un atto contrario ai doveri di ufficio

Codice Penale, art. 314-bis - Indebita destinazione di denaro o cose mobili

Codice Penale, art. 319-quater - Induzione indebita a dare o promettere utilità

Codice Penale, art. 322 c. 2-4 - Istigazione alla corruzione

Codice Penale, art. 322 c. 1-3 - Istigazione alla corruzione

Codice Penale, art. 314 c.1 - Peculato

Codice Penale, art. 316 - Peculato mediante profitto dell'errore altrui

Codice Penale, art. 322-bis - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri

Codice Penale, art. 321 - Pene per il corruttore

Codice Penale, art. 346-bis - Traffico di influenze illecite

Protocolli di prevenzione:

- Procedure - Rapporti con la pubblica amministrazione per richieste autorizzative

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) ruoli e responsabilità delle Funzioni coinvolte; ii) individuazione delle principali tipologie di atti, autorizzazioni, licenze e provvedimenti in genere necessari per il corretto svolgimento dell'attività della Società, per l'ottenimento dei quali la Società intrattiene rapporti con soggetti pubblici; iii) obbligo di improntare i rapporti con la Pubblica Amministrazione ai principi di correttezza, trasparenza e tracciabilità; iv) un sistema di controllo interno per il corretto e legittimo accesso ai sistemi informativi della Pubblica Amministrazione; v) aggiornamento di un report riepilogativo delle istanze presentate alla P.A. nel periodo di riferimento da trasmettere con cadenza periodica all'Organo Amministrativo e/o all'Organismo di Vigilanza (tale report deve contenere i dettagli della richiesta inoltrata, es. tipologia di autorizzazione, Pubblica Amministrazione coinvolta, funzione coinvolta, ecc.); vi) modalità di conservazione della documentazione rilevante prodotta.

- Segregazione dei compiti - Rapporti con la pubblica amministrazione per richieste autorizzazioni

Ove concretamente praticabile, deve essere garantita l'esistenza di segregazione tra chi predispone la domanda per l'ottenimento dell'autorizzazione da parte della Pubblica Amministrazione e chi verifica la corretta compilazione della stessa e ne autorizza la presentazione. Quando la separazione non è praticabile, l'AU dispone un controllo compensativo documentato da un soggetto diverso, ferme le competenze e le incompatibilità inderogabili per legge.

- Tracciabilità - Rapporti con la pubblica amministrazione per richieste autorizzative

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate. Le principali fasi del processo in oggetto devono essere opportunamente documentate ed archiviate presso gli uffici competenti. In particolare i documenti necessari alla predisposizione delle domande, compresi i documenti trasmessi dalle funzioni competenti per la compilazione delle stesse, le dichiarazioni trasmesse alla Pubblica Amministrazione e le relative ricevute di invio devono essere opportunamente tracciate ed archiviate.

- Ruoli e responsabilità - Rapporti con soggetti pubblici per la presentazione di documentazione tecnica, economica ed amministrativa

Ruoli e Responsabilità: devono essere identificati i ruoli e le responsabilità di coloro che sono coinvolti nell'attività sensibile e/o intrattengono rapporti con soggetti pubblici.

- Misure operative

- DG, con il supporto di RQ e delle funzioni coinvolte secondo competenza, assicura la disponibilità di un prospetto distinto per nucleo dei posti autorizzati, accreditati, contrattualizzati e concretamente attivi, con fonte e decorrenza
- non equipara tali categorie.
- RS, CS e AMM verificano periodicamente requisiti strutturali, assistenziali e di personale rispetto a titoli e accordi vigenti
- scostamenti sono comunicati ad AU prima delle dichiarazioni.
- AU firma comunicazioni basate su evidenze verificabili, dispone rimedi e segnala agli enti le variazioni dovute
- nessun posto è rendicontato oltre limiti o in assenza del titolo.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Raccolta, elaborazione e presentazione a soggetti pubblici o a soggetti incaricati di pubblico servizio della documentazione tecnica, economica ed amministrativa necessaria all'ottenimento e mantenimento di certificazioni, autorizzazioni, licenze, concessioni e provvedimenti amministrativi per l'esercizio delle attività aziendali

Predisposizione e aggiornamento di un report riepilogativo delle istanze presentate nel periodo di riferimento da trasmettere con cadenza periodica all'Alta Direzione e/o all'Organismo di Vigilanza che contenga per ciascuna verifica elementi quali la tipologia di autorizzazione o l'Organo Pubblico coinvolto.

**Evidenze e tracciabilità:**

Provvedimenti, contratti ASL, prospetto posti, turni, verifiche, comunicazioni e piani correttivi.

**Flussi informativi verso l'Organismo di Vigilanza:**

Variazioni, scadenze, perdita requisiti, contestazioni o attivazioni: tempestivo; prospetto trimestrale.

## 10. Ambito: Salute e sicurezza sul lavoro

### 10.1 Area di Rischio n. 24: Comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze.

Attività sensibili:

- gestione della sicurezza sul lavoro.

**Funzioni coinvolte nelle attività sensibili:**

DL; RSPP; MC; RLS; preposti

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

Per la prevenzione e protezione nei luoghi di lavoro la Società dispone del documento di valutazione dei rischi e della nomina del RSPP; tali strumenti si coordinano con le consultazioni e le misure previste dalla normativa sulla sicurezza.

- Procedure - Riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) devono essere previste riunioni periodiche con la dirigenza, con i lavoratori e i loro rappresentanti; ii) deve essere garantito l'accesso delle informazioni al Rappresentante Dei Lavoratori per la sicurezza (RLS); iii) deve essere coordinato il processo di coinvolgimento degli altri attori previsti dalla vigente normativa al fine di tenerli costantemente informati sugli obblighi di legge e sulle modalità di adeguamento agli stessi; iv) è convocata la riunione periodica nei casi e con la frequenza previsti dall'art. 35 del D.Lgs. 81/2008 e, ove opportuno, sono organizzati ulteriori incontri per discutere del DVR e delle misure preventive e protettive; v) la Società deve identificare dei Rappresentanti dei Lavoratori per la Sicurezza, che vengono consultati relativamente alla Valutazione dei Rischi; vi) la Società deve svolgere periodicamente la riunione periodica ai sensi dell'art. 35 del D.lgs. 81/2008; vii) sono disciplinate specifiche modalità che regolamentano il coinvolgimento e la consultazione dei lavoratori, in particolare:a) la comunicazione interna tra i vari livelli e funzioni dell'organizzazione;b) la comunicazione con i fornitori ed altri visitatori presenti sul luogo di lavoro;c) il ricevimento e risposta alle comunicazioni dalle parti esterne interessate;d) la partecipazione dei lavoratori, anche a mezzo delle proprie rappresentanze, attraverso:e) il loro coinvolgimento nell'identificazione dei pericoli, valutazione dei rischi e definizione delle misure di tutela;f) il loro coinvolgimento nelle indagini relative ad un incidente;g) la loro consultazione quando vi siano cambiamenti che possano avere significatività in materia di salute e sicurezza.

- Segregazione dei compiti - Organizzazione

Il processo è condotto assicurando, ove concretamente praticabile, la separazione fra attività autorizzative, esecutive e di controllo. Quando la separazione non sia concretamente praticabile, l'AU dispone verifiche compensative documentate; restano ferme le attribuzioni, le incompatibilità e i controlli inderogabili previsti dalla legge.

- Documentazione e correttezza dichiarazioni

Deve essere posta la massima attenzione affinché informazioni e dati indicati nelle dichiarazioni siano corretti e veritieri e adeguatamente documentati.

- Tracciabilità - Adempimenti obbligatori previsti dalla legge

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate. La documentazione inerente le attività in oggetto (es. documentazione e certificati, dichiarazione dei redditi, documentazione inerente il trattamento retributivo, contributivo e previdenziale del personale, documenti identificativi dei rifiuti prodotti, comunicazioni periodiche agli Enti Competenti, ecc.) deve essere opportunamente archiviata presso le Funzioni competenti.

- Ruoli e responsabilità - Applicazione di normative

Ruoli e Responsabilità: devono essere assegnati ruoli e responsabilità dei soggetti responsabili dell'identificazione e valutazione dell'applicabilità della normativa vigente e sono identificate le fonti di approfondimento normativo consultabili.

- Procure e deleghe - Dichiarazioni e comunicazioni

Procure e deleghe: i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. I soggetti che sottoscrivono le dichiarazioni e le comunicazioni in genere devono essere dotati di adeguati poteri.

- Misure operative

- DL consulta RLS nei casi previsti, assicura accesso alle informazioni e convoca riunione periodica ove obbligatoria.
- RSPP raccoglie indicazioni di lavoratori, preposti e MC e attribuisce responsabile e termine alle azioni
- DL approva le risorse.
- Esiti, ritardi e riscontri sono comunicati agli interessati e registrati senza divulgare dati sanitari personali.

Flussi verso l'Organismo di Vigilanza in relazione all'area di rischio - Comunicazione, partecipazione, consultazione, gestione delle riunioni periodiche di sicurezza e consultazione dei lavoratori e delle loro rappresentanze.

Deve essere trasmesso all'Organismo di Vigilanza un report che garantisca la tracciabilità e la disponibilità dei dati relativi alle attività inerenti al sistema di gestione della sicurezza con particolare l'invio periodico delle informazioni inerenti a: i) scostamenti tra i risultati ottenuti e gli obiettivi programmati e ii) risultati degli audit.

**Evidenze e tracciabilità:**

Verbali, consultazioni, comunicazioni, azioni e verifiche.

**Flussi informativi verso l'Organismo di Vigilanza:**

Mancate consultazioni, criticità irrisolte e infortuni: tempestivo; riepilogo semestrale.

### 10.2 Area di Rischio n. 25: Definizione delle misure per il controllo operativo e la gestione del cambiamento (macchinari, attrezzature, sistemi antincendio ecc.).

Attività sensibili:

- processi produttivi;

- gestione della manutenzione impianti.

**Funzioni coinvolte nelle attività sensibili:**

DL; RSPP; DG; CS; manutentori

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

- Procedure - Controllo operativo e la gestione del cambiamento

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) deve essere garantita l'idoneità degli edifici, la corretta manutenzione dei mezzi e attrezzature di lavoro, l'adempimento degli obblighi di legge; ii) devono essere definite, aggiornate e divulgate, attraverso il supporto del RSPP, le istruzioni operative per la sicurezza delle postazioni di lavoro e/o delle mansioni lavorative; iii) devono essere garantiti i controlli periodici previsti per legge su impianti, macchinari, attrezzature; Iv) la Società provvede a effettuare periodicamente le opportune verifiche e controlli di manutenzione presso i vari siti interessati (es. verifica impianti messa a terra, impianti antincendio); v) vengono effettuati sopralluoghi presso le diverse sedi, nei quali vengono notificate eventuali non conformità e programmati gli opportuni interventi risolutivi; vi) sono definite le modalità di registrazione delle manutenzioni effettuate e le relative responsabilità; vii) sono definite le modalità di segnalazione delle anomalie, individuati i mezzi più idonei per comunicare tali modalità, individuate le funzioni tenute ad attivare il relativo processo di manutenzione (manutenzioni non programmate); viii) gli eventuali interventi specialistici sono condotti da soggetti in possesso dei requisiti di legge che devono produrre le necessarie documentazioni.

- Ruoli e responsabilità - Controllo operativo e gestione del cambiamento

Ruoli e Responsabilità: devono essere individuati i requisiti e le competenze specifiche per la conduzione delle attività di audit sul modello di Salute e Sicurezza dei lavoratori nonché le modalità e le tempistiche delle verifiche sullo stato di attuazione delle misure adottate.

- Tracciabilità - Controlli su impianti e attrezzature

Le verifiche, le manutenzioni, le anomalie e le relative azioni correttive su impianti e attrezzature sono documentate e conservate dalle funzioni competenti, con evidenza delle scadenze e degli interventi effettuati.

- Ruoli e controlli - Manutenzioni e sicurezza

Le attività di richiesta, autorizzazione, esecuzione e verifica degli interventi sono attribuite secondo competenze e poteri effettivi. La separazione dei compiti è assicurata ove concretamente praticabile; in caso contrario l'AU dispone una verifica compensativa documentata da parte di un soggetto diverso, ferme le attribuzioni e le verifiche obbligatorie per legge.

- Misure operative

- DL assicura inventario e piano di manutenzione e controlli periodici con scadenze, responsabili e fornitori qualificati.
- Preposti sospendono l'uso di attrezzature non sicure e segnalano il guasto
- interventi urgenti sono autorizzati e tracciati.
- Prima di modifiche a reparti, processi o impianti DL e RSPP valutano rischi e aggiornano misure, formazione e documenti ove necessario.

**Evidenze e tracciabilità:**

Inventario, scadenziario, registri, verifiche, guasti e interventi.

**Flussi informativi verso l'Organismo di Vigilanza:**

Guasti critici, verifiche scadute o modifiche senza valutazione: immediato; riepilogo semestrale.

### 10.3 Area di Rischio n. 26: Gestione delle emergenze.

Attività sensibili:

- gestione delle emergenze.

**Funzioni coinvolte nelle attività sensibili:**

DL; RSPP; CS; RS; addetti emergenza

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

- Procedure - Gestione delle emergenze

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) l'identificazione delle situazioni che possono causare una potenziale emergenza; ii) definizione delle modalità per rispondere alle condizioni di emergenza e prevenire o mitigare le relative conseguenze negative in tema di salute e sicurezza; iii) modalità e responsabilità di gestione delle prove di emergenza, con particolare riguardo alla tipologia di emergenza (es. incendio, evacuazione, ecc.); iv) pianificazione ed esecuzione delle prove di emergenza per la verifica dell'efficacia dei piani di gestione delle emergenze; iv) individuazione, attraverso detti piani, dei percorsi di esodo e delle modalità di attuazione, da parte del personale, delle misure di segnalazione e di gestione delle emergenze; v) devono essere disponibili e mantenuti in efficienza idonei sistemi per la lotta agli incendi scelti per tipologia e numero in ragione della specifica valutazione del rischio di incendio ovvero delle indicazioni fornite dall'autorità competente; sono altresì presenti e mantenuti in efficienza idonei presidi sanitari; vi) deve essere assicurata all'interno degli spazi operativi un'adeguata organizzazione delle attività produttive al fine di consentire la corretta esecuzione delle procedure di emergenza; vii) ove applicabile, la Società provvede a ottenere il Certificato di Prevenzione Incendi (CPI) ai sensi del D.P.R 151/2011.

- Ruoli e responsabilità - Gestione delle emergenze

Ruoli e Responsabilità: devono essere individuate delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso.

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Procure e deleghe

Procure e deleghe: devono essere garantiti i seguenti principi in forza dei quali i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Tutte le attività devono essere svolte nel rispetto del sistema interno di procure e di attribuzione dei poteri di rappresentanza e firma sociale e dal sistema interno di deleghe allo svolgimento delle attività di competenza.

- Misure operative

- DL adotta e aggiorna piano di emergenza tenendo conto della non autosufficienza degli ospiti, dei turni notturni e delle interferenze.
- Sono designati e formati addetti in numero adeguato alle condizioni operative
- CS verifica copertura e comunica assenze o scoperture.
- Si effettuano prove, controlli dei presidi e riesame degli esiti secondo legge e piano
- emergenze e azioni correttive sono registrate.

**Evidenze e tracciabilità:**

Piano, nomine, registri di controllo, prove, rilievi e azioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Emergenze, carenze critiche, mancata copertura o prove obbligatorie omesse: tempestivo.

**10.4 Area di Rischio n. 27: Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la salute e sicurezza sul lavoro.**

Attività sensibili:

- gestione della sicurezza sul lavoro;

- redazione e aggiornamento DVR;

- appalti e subappalti.

**Funzioni coinvolte nelle attività sensibili:**

DL; RSPP; MC; RLS; preposti

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

La Società dispone del documento di valutazione dei rischi e della nomina del RSPP. Le misure previste in questa area si coordinano con la valutazione e con gli adempimenti di aggiornamento e attuazione richiesti dalla normativa.

- Conservazione del registro attività formative sulla sicurezza

Documentazione: deve essere conservato in archivio il registro delle attività formative svolte in ambito sicurezza e salute sul luogo del lavoro.

- Disponibilità documenti in adempimento Testo Unico Sicurezza

Documentazione: deve essere disponibile, in adempimento al Testo Unico Sicurezza, per ciascuna unità locale e attraverso il supporto del RSPP, il Piano Antincendio e d'Emergenza della Sede.

- Misure operative

- DL elabora e aggiorna DVR con RSPP e MC nei casi richiesti, previa consultazione del RLS
- gli obblighi indelegabili restano al datore.
- La valutazione considera movimentazione ospiti, agenti biologici e chimici, taglienti, stress, attrezzature, incendi e interferenze, secondo esposizioni effettive.
- Ogni misura ha responsabile, scadenza e risorse
- DL verifica attuazione e rivaluta a seguito di cambiamenti, infortuni o esigenze previste dalla legge.

**Evidenze e tracciabilità:**

DVR, valutazioni, verbali RLS, piani, disposizioni e riscontri.

**Flussi informativi verso l'Organismo di Vigilanza:**

Infortuni gravi, rischi non governati, modifiche e ritardi rilevanti: immediato; stato piano semestrale.

**10.5 Area di Rischio n. 28: Individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali.**

Attività sensibili:

- processi produttivi.

**Funzioni coinvolte nelle attività sensibili:**

DL; RSPP; DG; RQ; manutentori

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 - Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

- Procedure - Applicazione della normativa

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi:i) la conformità alle vigenti norme in materia (leggi, norme tecniche e regolamenti, ecc.) deve essere assicurata attraverso l'adozione di specifiche registrazioni allo scopo di porre sotto controllo l'identificazione delle leggi e delle normative applicabili alle attività e ai prodotti della Società; ii) il controllo periodico della conformità alla normativa applicabile;

- Ruoli e responsabilità - Applicazione di normative

Ruoli e Responsabilità: devono essere assegnati ruoli e responsabilità dei soggetti responsabili dell'identificazione e valutazione dell'applicabilità della normativa vigente e sono identificate le fonti di approfondimento normativo consultabili.

- Misure operative

- RQ e DL mantengono scadenzario di certificazioni e controlli applicabili, distinguendo obblighi del proprietario e del gestore secondo contratti e legge.
- Tecnici qualificati svolgono verifiche e manutenzioni
- gli esiti sono acquisiti e le non conformità classificate per gravità.
- DL dispone misure immediate per condizioni pericolose e monitora chiusura, risorse e comunicazioni agli enti ove dovute.

**Evidenze e tracciabilità:**

Certificazioni, verbali, contratti, controlli, piani e prova di chiusura.

**Flussi informativi verso l'Organismo di Vigilanza:**

Scadenze mancate, esiti negativi e pericoli: tempestivo; riepilogo semestrale.

### 10.6 Area di Rischio n. 29: Sorveglianza sanitaria

Attività sensibili:

- gestione della sicurezza sul lavoro.

**Funzioni coinvolte nelle attività sensibili:**

DL; MC; RSPP; AMM

Reati presupposto ex. D.Lgs. 231/2001 rilevanti per l'area di rischio

Codice Penale, art. 589 – Omicidio Colposo

Codice Penale, art. 590 c.3 - Lesioni personali colpose

Protocolli di prevenzione:

- Documentazione Sorveglianza Sanitaria

Documentazione: deve essere conservato in archivio il protocollo sanitario, la relazione annuale sullo stato di salute dei lavoratori, il verbale di sopralluogo del medico, fotocopia dei giudizi di idoneità.

- Procedure - Sorveglianza sanitaria

La Società disciplina l'attività sensibile mediante disposizioni e procedure adeguate, utilizzando e integrando ove necessario quelle esistenti, per assicurare i seguenti elementi: i) deve essere garantita la formazione dei lavoratori della Società e il presidio sanitario previsto per legge; deve essere mantenuto aggiornato – almeno ogni 2 mesi – l'elenco del personale di Sede/Società da sottoporre o sottoposto a sorveglianza sanitaria, presidiando le scadenze, i cambi mansioni, le nuove assunzioni, il rispetto delle prescrizioni impartite dal medico competente; ii) deve essere inviato, almeno ogni 2 mesi, al datore di lavooro o al suo delegato e al medico competente l'elenco complessivo e aggiornato dei lavoratori al fine di consentire l'aggiornamento dello stato di attuazione della sorveglianza sanitaria da parte deil medico competente; iii) il medico competente deve effettuare almeno un sopralluogo annuale – e all'occorrenza ogni qual volta richiesto - agli ambienti di lavoro rilasciando relativo verbale scritto; iv) deve essere assicurata l'attuazione della sorveglianza sanitaria; v) devono essere definite le modalità di

verifica dei requisiti per quanto riguarda gli aspetti sanitari, se riscontrati in sede di valutazione del rischio, da effettuare preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore.

- Segregazione dei compiti

Deve essere assicurata, ove concretamente praticabile, la separazione dei compiti fra le funzioni coinvolte nelle attività autorizzative, esecutive e di controllo. Quando ciò non sia concretamente praticabile, l'AU dispone verifiche compensative documentate, ferme le attribuzioni e i controlli inderogabili previsti dalla legge.

- Tracciabilità

Tracciabilità: devono essere garantiti i seguenti principi: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.

- Procure e deleghe

Procure e deleghe: devono essere garantiti i seguenti principi in forza dei quali i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Tutte le attività devono essere svolte nel rispetto del sistema interno di procure e di attribuzione dei poteri di rappresentanza e firma sociale e dal sistema interno di deleghe allo svolgimento delle attività di competenza.

- Ruoli e responsabilità - Attività sensibili

Deve essere garantita la formale identificazione di ruoli e responsabilità di coloro che sono coinvolti nell'attività sensibile

- Misure operative

- DL nomina MC nei casi previsti e gli fornisce informazioni sui rischi, cambi mansione e lavoratori esposti.
- AMM e MC gestiscono scadenze delle visite
- DL e preposti applicano limitazioni e prescrizioni del giudizio nel rispetto della riservatezza.
- Le cartelle sanitarie restano nella disponibilità del MC
- all'OdV sono trasmessi solo dati aggregati su coperture e anomalie, non diagnosi.

**Evidenze e tracciabilità:**

Nomina, scadenziario, giudizi nei limiti consentiti, dati aggregati e riscontri.

**Flussi informativi verso l'Organismo di Vigilanza:**

Visite scadute, idoneità incompatibili e carenze significative: tempestivo; dati aggregati semestrali.

## 11 Ambito: Ammissioni, assistenza e tutela degli ospiti

### 11.1 Area di Rischio n. 30: Ammissione, accesso e dimissione degli ospiti

**Attività sensibili:**

Domande private e convenzionate, valutazioni UVM, titoli, inserimento e dimissioni.

**Funzioni coinvolte nelle attività sensibili:**

DG; AS; UAC; RS; CS; AMM

**Reati presupposto e ambito:**

Reati contro la P.A. (artt. 24 e 25); reati contro la personalità individuale solo nelle fattispecie richiamate dall'art. 25-quinquies.

Protocolli di prevenzione:

- AS e UAC raccolgono domanda, documentazione, condizioni e titoli di accesso pertinenti, distinguendo regime privato e convenzionato.
- RS verifica appropriatezza, bisogni e capacità assistenziale
- DG valuta le domande e decide l'ammissione nei limiti dei propri poteri; la funzione amministrativa verifica, per quanto di competenza, disponibilità del posto e limiti contrattuali, senza considerare automaticamente attivi i posti soltanto autorizzati.
- Ammissioni, rinnovi, trasferimenti e dimissioni sono approvati secondo competenze, datati e comunicati agli enti quando dovuto
- non si accettano favori o pagamenti personali.

**Evidenze e tracciabilità:**

Fascicolo accesso, valutazioni UVM ove dovute, titoli, contratti, posto assegnato e comunicazioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Ammissioni senza titolo, limiti superati o richieste indebite: immediato; riepilogo trimestrale.

### 11.2 Area di Rischio n. 31: Presenze, rette e rendicontazione ASL

**Attività sensibili:**

Presenze, assenze, quote, fatture private e trasmissioni alla ASL.

**Funzioni coinvolte nelle attività sensibili:**

AMM; AS; UAC; RS; CS; AU

**Reati presupposto e ambito:**

Truffa o indebite erogazioni nei casi previsti dall'art. 24; corruzione e induzione indebita (art. 25); reati tributari ove pertinenti (art. 25-quinquiesdecies).

Protocolli di prevenzione:

- UAC registra giornalmente ingressi, uscite e assenze su evidenze
- CS verifica, per le attività assistenziali di competenza, la corrispondenza con i registri di reparto e il fascicolo; AS collabora per gli aspetti di propria competenza.
- AMM verifica mensilmente titoli, rinnovi, giornate, tariffe, quote, limiti di budget e contratti vigenti
- una persona diversa verifica il prospetto prima dell'invio e AU o soggetto munito di poteri autorizza; se la separazione non è praticabile, si applica il controllo compensativo documentato previsto al paragrafo 1.1.
- Correzioni riportano autore, data e motivo
- eventuali duplicazioni o eccedenze sono bloccate, rettificate e comunicate all'ente quando dovuto
- divieto di fatturare prestazioni non rese o quote duplicate.

Nella gestione delle presenze, delle rette e delle rendicontazioni verso l'ASL si osservano anche i principi previsti dal Codice Etico in materia di rapporti con la Pubblica Amministrazione, correttezza delle registrazioni e divieto di indebite utilità. È vietato rappresentare dati non veritieri sulle presenze o sulle prestazioni, richiedere o percepire corrispettivi non dovuti e offrire o promettere denaro, beni o altre utilità indebite a pubblici ufficiali o incaricati di pubblico servizio.

**Evidenze e tracciabilità:**

Titoli UVM, registri presenze, prospetti, controlli, fatture, ricevute e rettifiche.

**Flussi informativi verso l'Organismo di Vigilanza:**

Contestazioni ASL, differenze rilevanti, fatture irregolari o sforamenti: senza ritardo; riepilogo trimestrale.

### 11.3 Area di Rischio n. 32: Assistenza, PAI e documentazione clinica

**Attività sensibili:**

Valutazione multidimensionale, PAI, erogazione, registrazioni e passaggi di consegne.

**Funzioni coinvolte nelle attività sensibili:**

RS; CS; professionisti abilitati; AS

**Reati presupposto e ambito:**

Reati contro la P.A. (art. 24) se connessi a rendicontazioni false; reati contro la personalità individuale solo nei casi richiamati dall'art. 25-quinquies; sicurezza sul lavoro (art. 25-septies) nei relativi presupposti.

Protocolli di prevenzione:

L'organizzazione assistenziale considera la Carta dei servizi e i piani assistenziali individuali presenti nella documentazione aziendale. Le registrazioni e i controlli previsti dal presente Modello si coordinano con tali strumenti e con le attribuzioni dei professionisti coinvolti.

- RS coordina la valutazione e l'équipe definisce, attua e rivaluta il PAI con partecipazione dell'ospite e dei soggetti legittimati secondo legge.
- Ogni professionista registra in modo tempestivo attività realmente svolte, valutazioni e consegne
- CS controlla completezza, turni e coerenza con il PAI.
- Eventi avversi e omissioni sono comunicati a RS e gestiti immediatamente
- eventuali modifiche ai dati sono tracciate senza retrodatazioni o cancellazioni occulte.

**Evidenze e tracciabilità:**

PAI, valutazioni, cartelle, turni, consegne, audit e azioni correttive.

**Flussi informativi verso l'Organismo di Vigilanza:**

Eventi gravi, sistematiche omissioni o alterazioni: immediato; indicatori aggregati semestrali.

### 11.4 Area di Rischio n. 33: Tutela degli ospiti, incidenti e reclami

**Attività sensibili:**

Prevenzione di abusi, violenze, cadute, contenzioni e gestione reclami.

**Funzioni coinvolte nelle attività sensibili:**

RS; CS; AS; DG; professionisti

**Reati presupposto e ambito:**

Art. 25-quinquies esclusivamente per i delitti di personalità individuale espressamente richiamati; ulteriori rischi assistenziali e reati comuni sono presidiati anche a tutela degli ospiti senza affermarne automaticamente la rilevanza 231.

Protocolli di prevenzione:

- Operatori proteggono immediatamente l'ospite, attivano RS o i soccorsi e registrano incidenti o sospetti abusi
- AU valuta comunicazioni obbligatorie alle autorità e ai soggetti legittimati.
- Eventuali misure limitative sono gestite soltanto nei presupposti di legge e clinici, con valutazione, motivazione, monitoraggio, rivalutazione e documentazione
- sono vietate come punizione o sostituto dell'assistenza.
- AS raccoglie reclami di ospiti e familiari in canali accessibili, ne traccia presa in carico, risposta e rimedio
- i reclami restano distinti dai canali protetti dei segnalanti.

**Evidenze e tracciabilità:**

Registri incidenti, segnalazioni cliniche, valutazioni, reclami, riscontri e audit con accesso limitato.

**Flussi informativi verso l'Organismo di Vigilanza:**

Episodi gravi e anomalie sistematiche: senza ritardo con dati minimizzati; riepilogo semestrale.

### 11.5 Area di Rischio n. 34: Farmaci, dispositivi e approvvigionamenti sanitari

**Attività sensibili:**

Prescrizione, acquisto, ricezione, conservazione, somministrazione, scadenze e smaltimento.

**Funzioni coinvolte nelle attività sensibili:**

RS; professionisti abilitati; CS; AMM

**Reati presupposto e ambito:**

Reati contro la P.A. (art. 24) per false prestazioni; delitti contro l'industria e il commercio (art. 25-bis.1) ove ricorrano; ricettazione (art. 25-octies).

Protocolli di prevenzione:

La documentazione aziendale comprende una procedura di gestione dei farmaci, con indicazioni su prescrizione, somministrazione e conservazione. Le misure del Modello si coordinano con tale procedura e con le competenze dei professionisti abilitati.

- RS assicura che prescrizione e somministrazione siano svolte dai soggetti abilitati secondo prescrizioni e procedure
- la somministrazione è registrata dall'operatore autorizzato.
- Il referente del servizio verifica ricezione, integrità, scadenze, condizioni di conservazione, accessi e giacenze
- differenze e incidenti sono segnalati a RS.
- AMM e RS controllano fornitori e corrispondenza tra ordini, consegne e fatture
- medicinali scaduti e rifiuti sono separati e conferiti secondo le procedure applicabili.

**Evidenze e tracciabilità:**

Prescrizioni e registrazioni ad accesso riservato, ordini, lotti, scadenze, controlli e segnalazioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Ammancanze, errori gravi, farmaci scaduti o frodi: tempestivo; dati aggregati semestrali.

### 11.6 Area di Rischio n. 35: Gestione di denaro e beni degli ospiti

**Attività sensibili:**

Custodia volontaria, consegna, spese autorizzate e restituzione di valori degli ospiti.

**Funzioni coinvolte nelle attività sensibili:**

AU; AMM; AS; CS

**Reati presupposto e ambito:**

Ricettazione, riciclaggio e autoriciclaggio nei casi previsti dall'art. 25-octies; reati contro la P.A. ove pertinenti; ulteriori illeciti comuni sono disciplinati a tutela della persona.

Protocolli di prevenzione:

- La presa in consegna avviene solo con titolo, consenso o poteri di rappresentanza documentati e con inventario sottoscritto dai soggetti legittimati.
- Ogni movimentazione richiede causale, autorizzazione e giustificativo, con separazione fra custodia e riscontro o verifica compensativa documentata.
- AMM riconcilia almeno mensilmente il registro con i valori custoditi
- restituzione e anomalie sono verbalizzate e comunicate ad AU e alle persone legittimate.

**Evidenze e tracciabilità:**

Verbali di consegna, autorizzazioni, registro, giustificativi, riconciliazioni e restituzioni.

**Flussi informativi verso l'Organismo di Vigilanza:**

Ammanco, prelievo non autorizzato o sospetto abuso: immediato; riepilogo aggregato semestrale.

## 12 Ambito: Tutela ambientale e sicurezza alimentare

### 12.1 Area di Rischio n. 36: Rifiuti sanitari e tutela ambientale

**Attività sensibili:**

Classificazione, deposito, trasporto e smaltimento di rifiuti sanitari, farmaci scaduti e altri rifiuti.

**Funzioni coinvolte nelle attività sensibili:**

AU; RQ; RS; CS; referente rifiuti; fornitore autorizzato

**Reati presupposto e ambito:**

Reati ambientali (art. 25-undecies) limitatamente alle fattispecie e condizioni richiamate dalla legge.

Protocolli di prevenzione:

Per la gestione dei rifiuti la documentazione aziendale comprende un contratto con un operatore esterno. Si osservano le prescrizioni applicabili alla classificazione, al deposito, alla tracciabilità e al conferimento, con verifica dei titoli richiesti ai soggetti incaricati.

- Il referente classifica i rifiuti con supporto tecnico, identifica contenitori e aree di deposito e verifica condizioni e tempi applicabili.
- Prima dell'affidamento AU verifica autorizzazioni e iscrizioni di trasportatore e destinatario rispetto a codici e operazioni
- le scadenze sono controllate.
- RQ o referente verifica formulari e registrazioni con il sistema di tracciabilità vigente e il rientro delle evidenze di conferimento
- omissioni o anomalie comportano immediata attivazione del fornitore e misure correttive.

**Evidenze e tracciabilità:**

Contratti, autorizzazioni, classificazioni, formulari e registri applicabili, verifiche e scadenze.

**Flussi informativi verso l'Organismo di Vigilanza:**

Sversamenti, autorizzazioni scadute, mancato riscontro conferimento o contestazioni: tempestivo; riepilogo semestrale.

### 12.2 Area di Rischio n. 37: Cucina interna, alimenti e fornitori

**Attività sensibili:**

Acquisto, ricezione, conservazione, diete, preparazione e distribuzione dei pasti.

**Funzioni coinvolte nelle attività sensibili:**

RS; referente cucina; RQ; AMM; AU

**Reati presupposto e ambito:**

Delitti contro l'industria e il commercio (art. 25-bis.1) nei casi applicabili; reati contro la P.A. (art. 24) per eventuali prestazioni falsamente rendicontate; rischi igienico-sanitari ulteriori sono presidiati autonomamente.

Protocolli di prevenzione:

La Società dispone di un manuale di autocontrollo alimentare HACCP. Le misure del presente Modello si coordinano con il piano e con gli adempimenti di sicurezza alimentare applicabili alla cucina e alle forniture.

- Il referente cucina applica il piano HACCP, controlla fornitori, temperature, scadenze, allergeni, tracciabilità e conformità delle consegne.
- RS definisce diete e consistenze secondo prescrizioni e bisogni
- CS verifica che le indicazioni raggiungano il personale e che le variazioni siano registrate.

- Non conformità, sospette tossinfezioni o interruzioni sono gestite immediatamente con isolamento, assistenza, comunicazioni dovute e azioni correttive.

**Evidenze e tracciabilità:**

Piano HACCP, registri temperature, diete con accesso limitato, consegne, non conformità.

**Flussi informativi verso l'Organismo di Vigilanza:**

Eventi gravi, irregolarità ripetute o prescrizioni autorità: immediato; riepilogo semestrale.

## 13 Ambito: Segnalazioni e sicurezza informatica

### 13.1 Area di Rischio n. 38: Segnalazioni, tutela del segnalante e flussi informativi

**Attività sensibili:**

Canale protetto, ricezione, gestione, riservatezza, divieto di ritorsione e flussi ordinari.

**Funzioni coinvolte nelle attività sensibili:**

AU; soggetto o servizio incaricato della gestione delle segnalazioni; OdV dopo nomina; funzioni competenti

**Reati presupposto e ambito:**

Presidio organizzativo dell'art. 6, comma 2-bis, D.Lgs. 231/2001 e D.Lgs. 24/2023; eventuali fatti di reato sono valutati nelle rispettive aree.

Protocolli di prevenzione:

- AU attiva il canale interno scritto e orale, sentite le rappresentanze ove dovuto, e nomina un gestore autonomo e formato
- informazioni e recapiti effettivi sono resi accessibili agli aventi diritto.
- Il soggetto o servizio incaricato della gestione rilascia avviso entro sette giorni e riscontro entro tre mesi dall'avviso o dalla scadenza dei sette giorni
- cura diligente seguito, gestione dei conflitti e trasmissione entro sette giorni al competente se ricevuta fuori canale.
- Identità e atti sono protetti
- i flussi ordinari all'OdV non sostituiscono il canale protetto né comportano comunicazione automatica dell'identità
- ritorsioni sono vietate e conservazione limitata ai termini di legge.

**Evidenze e tracciabilità:**

Atto di nomina gestore, procedure, prova informazione, registri riservati e dati aggregati.

**Flussi informativi verso l'Organismo di Vigilanza:**

Il soggetto o servizio incaricato della gestione trasmette all'OdV, dopo la nomina e nel rispetto della riservatezza, soli dati aggregati e criticità rilevanti; ritorsioni e anomalie gravi senza ritardo.

### 13.2 Area di Rischio n. 39: Sistemi informativi sanitari, cybersicurezza e incidenti

**Attività sensibili:**

Cartelle elettroniche, portali ASL, backup, fornitori e incidenti.

**Funzioni coinvolte nelle attività sensibili:**

DG; AMM; RS; AU; soggetti esterni incaricati

**Reati presupposto e ambito:**

Delitti informatici (art. 24-bis) e reati contro la P.A. (art. 24) nei casi applicabili; obblighi privacy e cybersicurezza operano autonomamente.

Le attività di accesso ai sistemi informativi aziendali, alle cartelle elettroniche e alle banche dati contenenti dati personali e sanitari sono svolte nel rispetto dei principi del Codice Etico e delle disposizioni aziendali in materia di sicurezza informatica. Le abilitazioni, la gestione delle credenziali, la

registrazione degli accessi e i controlli sugli incidenti sono disciplinati dai protocolli indicati nella presente area e nelle aree informatiche della Parte Speciale.

Protocolli di prevenzione:

- La Direzione gestionale, con il supporto dei soggetti esterni incaricati, mantiene inventario e profili minimi, protegge gli accessi e verifica aggiornamenti, log, vulnerabilità e utenze privilegiate.
- La Direzione gestionale e RS, con il supporto dei soggetti esterni incaricati, pianificano backup e almeno una prova periodica di ripristino
- i piani di continuità prevedono modalità sicure di erogazione delle cure durante indisponibilità.
- Incidenti sono comunicati immediatamente alla Direzione gestionale e alla funzione amministrativa, che si avvalgono dei soggetti esterni incaricati
- le funzioni tecniche valutano, con AU e gli eventuali soggetti esterni incaricati secondo le rispettive competenze, eventuali obblighi e scadenze NIS2 e privacy, senza presumere automaticamente l'applicabilità. L'eventuale uso di sistemi di intelligenza artificiale è previamente valutato da AU e dalle funzioni interessate, anche con il supporto dei fornitori incaricati, tenendo conto della destinazione d'uso, dei dati trattati, delle autorizzazioni, delle misure di sicurezza e della supervisione umana. Sono vietati l'alterazione illecita dei sistemi e la diffusione illecita di contenuti generati o alterati; ogni evento rilevante è documentato e segnalato secondo le procedure applicabili. Il presidio considera i delitti di cui agli artt. 437-bis e 612-quater c.p., nei casi richiamati dall'art. 25-vicies del Decreto.

**Evidenze e tracciabilità:**

Inventario, log, test ripristino, piani, registro incidenti e notifiche se dovute.

**Flussi informativi verso l'Organismo di Vigilanza:**

Incidenti rilevanti, indisponibilità dei sistemi clinici o accessi abusivi: senza ritardo; sintesi semestrale.