



# **VILLA ESTHER**

casa di cura

**MODELLO ORGANIZZATIVO DELLA CASA**

**DI CURA PRIVATA VILLA ESTHER S.R.L.**

**ai sensi dell'art. 6, comma 3, del d.lgs. 231/2001**

## Sommario

<b>INTRODUZIONE.....</b>	<b>4</b>
IL DECRETO LEGISLATIVO N. 231/2001.....	4
<b>PARTE GENERALE.....</b>	<b>5</b>
SEZIONE I - PRINCIPI GENERALI .....	5
ART. 1 - DEFINIZIONI.....	5
ART. 2 - OGGETTO E STRUTTURA DELLA SOCIETÀ .....	6
ART. 3 - DESCRIZIONE DEL SISTEMA DI DELEGHE .....	7
ART. 4 - SCOPO E AMBITO DI APPLICAZIONE DEL MODELLO: CONDIZIONI E LIMITI DELLA RESPONSABILITÀ DELLA SOCIETÀ .....	8
ART. 5 - PRESUPPOSTI PER L'ESENZIONE DI RESPONSABILITÀ .....	8
ART. 6 - SISTEMA INTERNO PER SEGNALARE LE IRREGOLARITÀ (WHISTLEBLOWING) .....	9
ART. 7 - SOGGETTI OBBLIGATI .....	9
ART. 8 - PRINCIPIO GENERALE DI CORRETTEZZA E CODICE ETICO .....	10
ART. 9 - PRINCIPI GENERALI DEI SISTEMI DI PREVENZIONE E CONTROLLO .....	10
ART. 10 - ORGANISMO DI VIGILANZA .....	11
ART. 11 - REQUISITI DELL'ORGANISMO DI VIGILANZA.....	11
ART. 12 - COMPITI E POTERI DELL'ORGANISMO DI VIGILANZA .....	11
ART. 13 - COMPENSO E DOTAZIONE PATRIMONIALE.....	12
ART. 14 - RIUNIONI .....	13
ART. 15 - INFORMATIVA RESA ALL'OdV .....	13
ART. 16 - INFORMATIVA RESA DALL'OdV.....	14
ART. 17 - RIESAME E AGGIORNAMENTO DEL MODELLO .....	14
SEZIONE II - SISTEMA DISCIPLINARE .....	15
ART. 18 - FUNZIONE DEL SISTEMA DISCIPLINARE .....	15
ART. 19 - COMPORTAMENTI RILEVANTI .....	16
ART. 20 - CRITERI DI IRROGAZIONE DELLE SANZIONI .....	16
ART. 21 - SANZIONI NEI CONFRONTI DELL'AMMINISTRATORE.....	16
ART. 22 - SANZIONI NEI CONFRONTI DEI DIRIGENTI APICALI E DEGLI ALTRI SOGGETTI APICALI .....	17
ART. 23 - SANZIONI NEI CONFRONTI DEI DIPENDENTI .....	17
ART. 24 - SANZIONI NEI CONFRONTI DEI TERZI DESTINATARI.....	18
ART. 25 - RUOLO DELL'OdV IN RELAZIONE AI PROCEDIMENTI DI IRROGAZIONE DI SANZIONI.....	18
ART. 26 - PROCEDIMENTO DI IRROGAZIONE DI SANZIONI NEI CONFRONTI DELL'AMMINISTRATORE .....	19
ART. 27 - PROCEDIMENTO NEI CONFRONTI DEI DIRIGENTI APICALI .....	19
ART. 28 - PROCEDIMENTO NEI CONFRONTI DEGLI ALTRI SOGGETTI APICALI.....	20
ART. 29 - PROCEDIMENTO NEI CONFRONTI DEI DIPENDENTI .....	20
ART. 30 - PROCEDIMENTO NEI CONFRONTI DI TERZI.....	20
ART. 31 - PROCEDIMENTO DI IRROGAZIONE DI SANZIONI IN CASO DI VIOLAZIONE DELLA NORMATIVA WHISTLEBLOWING .....	21
<b>PARTE SPECIALE .....</b>	<b>22</b>
SEZIONE I - STRUTTURA DELLA PARTE SPECIALE E ORGANIZZAZIONE INTERNA DELLA SOCIETÀ .....	22
ART. 32 - STRUTTURA DELLA PARTE SPECIALE .....	22
ART. 33 - ORGANIZZAZIONE INTERNA DELLA SOCIETÀ.....	22
PROCESSI AZIENDALI RILEVANTI .....	23
ART. 34 - DESCRIZIONE E GESTIONE DEI FLUSSI FINANZIARI .....	23
ART. 35 - GESTIONE DEL PROCESSO DI APPROVVIGIONAMENTO.....	23
ART. 36 - TRATTAMENTO DEI DATI PERSONALI .....	24
ART. 37 - GESTIONE DEL SISTEMA INFORMATIVO .....	24
SEZIONE II - REATI-PRESUPPOSTO, VALUTAZIONE DEI RISCHI E MISURE DI PREVENZIONE .....	31
INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO, DI UN ENTE PUBBLICO O DELL'UNIONE EUROPEA O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE, FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO E FRODE NELLE PUBBLICHE FORNITURE .....	31
ART. 38 - REATI-PRESUPPOSTO DI CUI ALL'ART. 24 DEL DECRETO 231.....	31
ART. 39 - MISURE DI PREVENZIONE .....	31

PECULATO, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ, CORRUZIONE E ABUSO D'UFFICIO.....	35
ART. 40 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25 DEL DECRETO 231 .....	35
ART. 41 - MISURE DI PREVENZIONE .....	35
FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO; DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO .....	37
ART. 42 - REATI-PRESUPPOSTO DI CUI AGLI ARTT. 25-BIS E 25-BIS.1 DEL DECRETO 231 .....	37
ART. 43 - MISURE DI PREVENZIONE .....	38
ART. 44 - DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI.....	39
REATI SOCIETARI .....	40
ART. 45 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-TER DEL DECRETO 231 .....	40
ART. 46 - MISURE DI PREVENZIONE .....	40
REATI TRIBUTARI .....	42
ART. 47 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUINQUESDECIES DEL DECRETO 231 .....	42
ART. 48 -MISURE DI PREVENZIONE .....	42
DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO.....	44
ART. 49 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUATER DEL DECRETO 231 .....	44
ART. 50 - MISURE DI PREVENZIONE .....	44
DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE .....	45
ART. 51 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUINQUES DEL DECRETO 231 .....	45
ART. 52 - MISURE DI PREVENZIONE .....	45
ABUSI DI MERCATO.....	46
ART. 53 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-SEXIES DEL DECRETO 231.....	46
ART. 54 - MISURE DI PREVENZIONE .....	46
PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI .....	47
ART. 55 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUATER.1 DEL DECRETO 231 .....	47
ART. 56 - MISURE DI PREVENZIONE .....	47
OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO.....	48
ART. 57 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-SEPTIES DEL DECRETO 231 .....	48
ART. 58 - MISURE DI PREVENZIONE .....	48
RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO .....	51
ART. 59 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-OCTIES DEL DECRETO 231 .....	51
ART. 60 - MISURE DI PREVENZIONE .....	51
REATI AMBIENTALI .....	53
ART. 61 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-UNDECIES DEL DECRETO 231 .....	53
ART. 62 - MISURE DI PREVENZIONE .....	54
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI.....	54
ART. 63 - REATI-PRESUPPOSTO DI CUI ALL'ART. 24-BIS DEL DECRETO 231.....	54
ART. 64 - MISURE DI PREVENZIONE .....	55
IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE.....	57
ART. 65 - REATI PRESUPPOSTO DI CUI ALL'ART. 25-DUODECIES DEL DECRETO 231 .....	57
ART. 66 - MISURE DI PREVENZIONE .....	57
TUTELA DEL DIRITTO D'AUTORE.....	58
ART. 67 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-NOVIES DEL DECRETO 231 .....	58
ART. 68 - MISURE DI PREVENZIONE .....	58
DELITTI DI CRIMINALITÀ ORGANIZZATA .....	59
ART. 69 - REATI-PRESUPPOSTO DI CUI ALL'ART. 24-TER DEL DECRETO 231 .....	59
ART. 70 - MISURE DI PREVENZIONE .....	59
INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA .....	60
ART. 71 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-DECIES DEL DECRETO 231 .....	60
ART. 72 - MISURE DI PREVENZIONE .....	60
SEZIONE III .....	61
TABELLA RIASSUNTIVA RISK ASSESSMENT: MAPPATURA DELLE ATTIVITÀ SENSIBILI E DEI PROCESSI A RISCHIO REATO, VALUTAZIONE DEI RISCHI E MISURE DI PREVENZIONE E DI CONTROLLO ADOTTATE .....	61

## INTRODUZIONE

### IL DECRETO LEGISLATIVO N. 231/2001

Il d.lgs. 8 giugno 2001 n. 231, recante *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”*, ha introdotto nell’ordinamento giuridico italiano un sistema di responsabilità amministrativa a carico degli enti collettivi (società, persone giuridiche, enti collettivi non riconosciuti, associazioni, consorzi) per alcuni reati, tassativamente elencati (c.d. reati presupposto), ove commessi nel loro interesse o vantaggio:

- da persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale;
- da persone fisiche che esercitano, anche di fatto, la gestione e il controllo degli enti medesimi (c.d. soggetti apicali);
- da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali, se la commissione del reato sia stata possibile dall’omissione di vigilanza di questi ultimi.

Il d. lgs. n. 231/2001 stabilisce che l’ente non risponde del reato commesso nel suo interesse o a suo vantaggio nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi, il c.d. Modello 231.

## PARTE GENERALE

### SEZIONE I - PRINCIPI GENERALI

#### ART. 1 - DEFINIZIONI

Ai fini del presente Modello Organizzativo si intendono per:

- **AIOP:** Associazione Italiana Ospedalità Privata, alla quale aderisce la Società come di seguito definita;
- **Società o Casa di Cura:** la CASA DI CURA PRIVATA VILLA ESTHER S.R.L., società a responsabilità limitata con sede legale in Bojano (CB), Via Gino Di Biase n.18, iscritta al Registro delle Imprese del Molise al n.01706190707;
- **Decreto 231:** il decreto legislativo 8 giugno 2001, n. 231, come successivamente modificato e integrato, recante *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”*;
- **Organismo di Vigilanza o OdV:** l’Organismo di Vigilanza previsto dall’articolo 6 del Decreto 231;
- **Amministratore:** l’organo amministrativo della Società, ossia l’Amministratore Unico;
- **Sindaco:** l’organo di controllo della Società, vale a dire il sindaco unico ai sensi della legge n. 183/2011;
- **Modello:** il presente modello organizzativo, adottato dall’Amministratore Unico in attuazione degli articoli 6 e 7 del Decreto 231;
- **Statuto:** lo statuto della Società, nella versione di tempo in tempo aggiornata.

## ART. 2 - OGGETTO E STRUTTURA DELLA SOCIETÀ

La Società ha per oggetto l'esercizio delle seguenti attività: casa di cura privata con ricovero ordinario e diurno nelle discipline mediche, chirurgiche e riabilitative (riabilitazione post acuzie e lungodegenza post acuzie); day service medico e chirurgico; poliambulatorio nelle discipline mediche, chirurgiche e riabilitative; laboratorio di analisi cliniche; servizio di radiodiagnostica; residenza sanitaria assistita (RSA); presidio e/o struttura di riabilitazione extra ospedaliera *ex art. 26 legge n. 833/78*; casa di riposo. Tutte le attività elencate potranno essere esercitate anche in associazione temporanea di impresa.

Alla Società resta interdetto l'esercizio in proprio delle attività professionali medico-chirurgica ed infermieristica e di qualsiasi altra attività comunque riferibile all'esecuzione delle prestazioni medico-sanitaria, medico-assistenziale e paramedica, che si intendono riservate e che, pertanto, potranno e dovranno essere personalmente svolte da coloro che, a norma delle vigenti leggi, siano legalmente abilitati ed iscritti negli appositi albi professionali.

La Società può altresì compiere tutte le altre operazioni commerciali, industriali, mobiliari, immobiliari, finanziarie, bancarie, attive e passive, ritenute necessarie, opportune e utili per il miglior raggiungimento dell'oggetto sociale, purché tali attività vengano svolte in misura non prevalente rispetto a quelle che costituiscono l'oggetto sociale e non nei confronti del pubblico; la Società potrà accedere a finanziamenti pubblici e privati; contrarre prestiti e mutui, anche ipotecari; stipulare contratti di sovvenzione, anticipazione e conto corrente con facoltà di fido, nonché emettere, scontare, girare o far protestare assegni e cambiali; rilasciare garanzie reali a favore di terzi, nonché fidejussioni a favore di soci o di società appartenenti al gruppo.

La Società può infine procedere all'acquisto, alla vendita, alla locazione e all'affitto di beni mobili e immobili, aziende e rami di azienda, assumere interessenze e partecipazioni in altre società, consorzi e imprese di qualunque natura, sia direttamente sia indirettamente in Italia e all'estero, nei limiti consentiti dalla legge e comunque non a scopo di collocamento.

Tutte le attività dovranno essere svolte nei limiti e nel rispetto delle norme che ne disciplinano l'esercizio.

Viene espressamente esclusa ogni attività finanziaria vietata dalle norme tempo per tempo vigenti in materia; in particolare è vietata la raccolta del risparmio tra il pubblico, la locazione finanziaria attiva, la concessione di finanziamenti sotto qualsiasi forma, la prestazione di servizi di pagamento e di intermediazione in cambi e la gestione fiduciaria.

La Società svolge le attività incluse nel proprio oggetto sociale, con un numero di dipendenti complessivamente pari a 69.

Le modalità di nomina degli organi sociali sono quelli disciplinati nello Statuto della Società.

## **Poteri da statuto**

Qualunque sia il sistema di amministrazione, l'organo amministrativo ha tutti i poteri di ordinaria e straordinaria amministrazione, esclusi quelli che la legge o lo statuto riservano espressamente ai soci.

Il consiglio di amministrazione, nei limiti previsti dall'art. 2381 c.c., può delegare le proprie attribuzioni in materia gestionale in tutto o in parte ad uno o più singoli amministratori.

Quando l'amministrazione è affidata a più persone che non costituiscono consiglio, i poteri di amministrazione, in occasione della nomina, potranno essere attribuiti agli stessi sia in via congiunta sia in via disgiunta, ovvero taluni poteri di amministrazione potranno essere attribuiti in via disgiunta e gli altri in via congiunta. In mancanza di qualsiasi precisazione nell'atto di nomina in ordine alle modalità di esercizio dei poteri di amministrazione, detti poteri si intenderanno attribuiti agli amministratori in via disgiunta.

Quando l'amministrazione è affidata disgiuntamente a più persone ciascun amministratore ha diritto di opporsi all'esecuzione da parte di altri amministratori di atti di gestione, prima che siano compiuti. In tal caso la decisione è rimessa all'assemblea dei soci.

La rappresentanza della Società di fronte ai terzi e in giudizio compete:

all'Amministratore unico;

al Presidente del Consiglio di amministrazione, senza limitazioni ed agli amministratori delegati, se nominati, nei limiti delle deleghe;

a ciascuno degli amministratori, in caso di amministrazione affidata a più persone che non costituiscono il consiglio, con firma congiunta o disgiunta, come risulta dalla deliberazione di nomina; in caso di omessa determinazione, l'esercizio del potere di rappresentanza si intende disgiuntivo.

Gli amministratori possono nominare institori o procuratori per singoli e per determinati atti o categorie di atti.

In ogni caso quando la rappresentanza della Società è conferita ad un soggetto che non sia amministratore, l'attribuzione del potere di rappresentanza è regolata dalle norme in tema di procura.

### **ART. 3 - DESCRIZIONE DEL SISTEMA DI DELEGHE**

I poteri nella Casa di cura Villa Esther s.r.l. sono assegnati secondo logiche definite. Un sistema dei poteri aziendali coerente è uno strumento fondamentale per ottenere il rispetto delle procedure, funzionale al raggiungimento di un buon livello di efficienza aziendale.

Le deleghe concesse alle funzioni aziendali di primo livello vengono normalmente attribuite dall'Amministratore Unico, con delibera che definisce in modo chiaro poteri e responsabilità.

Quando la delega comporta anche la rappresentanza della Società, deve essere attribuita una procura speciale predisposta con atto notarile.

La Società è amministrata da un Amministratore Unico, a cui spetta la gestione ordinaria e straordinaria della Società, fatti salvi i poteri riservati dalla legge o dallo Statuto ai soci, e altresì i poteri di rappresentanza generale della Società nei confronti dei terzi e in giudizio.

Il Sindaco unico vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e, in particolare, sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile della Società e sul suo concreto funzionamento.

Attualmente non sono previste deleghe.

#### **ART. 4 - SCOPO E AMBITO DI APPLICAZIONE DEL MODELLO: CONDIZIONI E LIMITI DELLA RESPONSABILITÀ DELLA SOCIETÀ**

Il presente Modello persegue lo scopo di adempiere a quanto previsto dall'art. 6, co. 3, del Decreto 231. Esso disciplina, pertanto, i presidi e le misure organizzative funzionali a prevenire il compimento, nell'interesse o a vantaggio della Società, dei reati, elencati tassativamente nel Decreto 231, da parte dei soggetti rientranti in una delle categorie di cui all'art. 5 del Decreto 231, ossia delle persone fisiche che:

- rivestano funzioni di rappresentanza, amministrazione o direzione della Società, nonché da parte delle persone fisiche che esercitino, anche di fatto, la gestione e il controllo della Società;
- siano sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati al punto che precede, se la commissione del reato è stata resa possibile dall'omissione di vigilanza.

Il Modello è stato redatto in conformità delle Linee Guida elaborate dall'AIOP nella versione di tempo in tempo aggiornata ed è costantemente allineato a queste Linee Guida.

La responsabilità della Società si aggiunge a quella della persona fisica che ha commesso materialmente il reato. La Società può essere dichiarata responsabile anche se la persona fisica che ha commesso il reato non è imputabile ovvero non è stata individuata.

La Società è consapevole del fatto che solo l'adozione e l'efficace attuazione del Modello, nonché l'idoneità dello stesso a prevenire le tipologie di reato-presupposto individuate nel Decreto 231, così come pure la nomina e l'effettivo e corretto funzionamento dell'Organismo di Vigilanza, possono avere effetti per essa scriminanti là dove un reato-presupposto sia integrato.

#### **ART. 5 - PRESUPPOSTI PER L'ESENZIONE DI RESPONSABILITÀ**

La Società non risponde del compimento dei reati-presupposto quando:

- a. volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento rilevanti in relazione a uno o più reati-presupposto; nonché quando, congiuntamente ricorrono le condizioni sotto indicate da b) ad e);

- b. l'Amministratore ha in effetti adottato ed efficacemente attuato, prima della commissione del fatto, il Modello e questo sia stato considerato in giudizio, in concreto, idoneo a prevenire reati della specie di quello verificatosi;
- c. il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il relativo aggiornamento è stato in effetti affidato all'OdV;
- d. le persone hanno commesso il reato eludendo fraudolentemente il Modello;
- e. l'OdV ha adeguatamente assolto ai propri compiti di vigilanza.

A prescindere dalla sussistenza delle condizioni per una eventuale esenzione di responsabilità, è comunque disposta la confisca del profitto che la Società avesse tratto dal reato, anche nella forma per equivalente.

#### **ART. 6 - SISTEMA INTERNO PER SEGNALARE LE IRREGOLARITÀ (WHISTLEBLOWING)**

La Società, in conformità all'art.6 co. 2 *bis*, introdotto dall'art. 2 della legge n. 179/2017 prevede:

- a) l'attivazione di uno o più canali che consentano ai soggetti indicati nell'art. 5, co. 1, lettere *a)* e *b)* della predetta legge, di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati alla segnalazione;
- d) nel sistema disciplinare adottato ai sensi del co. 2, lettera *e)*, sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Tutti i soggetti apicali e i sottoposti sono tenuti al rispetto della procedura di whistleblowing allegata, adottata in conformità della normativa sopra indicata.

#### **ART. 7 - SOGGETTI OBBLIGATI**

I soggetti obbligati al rispetto delle disposizioni contenute nel Modello includono:

- le persone che ricoprono una posizione apicale e, nello specifico, esercitano funzioni di amministrazione, direzione o rappresentanza ovvero hanno, anche di fatto, la gestione o il controllo della Società;
- le persone che, in forza di rapporti di subordinazione gerarchica rispetto a quelle di cui al punto che precede, dipendono dal loro potere di direzione o controllo;
- i collaboratori e i consulenti che – pur non essendo legati alla Società da rapporti del genere di cui sopra – si trovino ad avere conferiti incarichi professionali dai sopra citati soggetti.

I soggetti indicati devono astenersi dal porre in essere comportamenti contrari ai doveri d'ufficio o alle norme imperative di legge e, qualora vengano a conoscenza di comportamenti di questo genere, devono darne notizia prontamente all'Organismo di Vigilanza.

#### **ART. 8 - PRINCIPIO GENERALE DI CORRETTEZZA E CODICE ETICO**

La Società ha adottato e applica un principio generale di correttezza nonché specifici obblighi comportamentali contenuti nel Codice Etico al cui rispetto sono tenuti tutti coloro che, a vario titolo, operano per la Società (Amministratore e Sindaco unico, dipendenti, consulenti, collaboratori), allegato al presente Modello.

Conformemente al Codice Etico, la Società ispira la propria attività a principi di rispetto sostanziale e formale della vigente normativa disciplinante le attività che essa svolge, di regolarità nella gestione e di chiarezza nell'informazione.

Essa promuove la formazione etica dei propri dipendenti, stabilendo appositi canali informativi e progetti di formazione e aggiornamento al proprio interno. Essa cura altresì, all'atto dell'instaurazione di qualsiasi rapporto professionale con soggetti e consulenti esterni, che costoro ricevano adeguata informativa e conoscenza dell'impostazione etica seguita dalla Società.

La Società richiede inoltre ai propri dipendenti, nonché ai collaboratori e consulenti esterni, il rispetto continuo dell'impegno etico assunto, il quale elemento viene a tutti gli effetti considerato requisito indispensabile per la costituzione o il mantenimento di qualsiasi rapporto.

Si intendono parti integranti del Modello, oltre al principio etico di carattere generale, tutti i principi e le norme dettagliati all'interno del Codice Etico della Società.

#### **ART. 9 - PRINCIPI GENERALI DEI SISTEMI DI PREVENZIONE E CONTROLLO**

Per controllare l'effettiva attuazione dei principi etici e del Codice Etico adottato e per garantire comportamenti informati alla massima liceità, trasparenza e correttezza, la Società prevede appositi sistemi di registrazione, autorizzazione e verifica dei processi decisionali e ne cura il corretto funzionamento e l'aggiornamento, quando necessario. In ogni caso, i sistemi di prevenzione e controllo nonché gli specifici processi decisionali adottati dalla Società sono strutturati in modo tale da non potere essere aggirati se non con l'uso volontario di mezzi fraudolenti.

La Società prevede altresì specifiche procedure di vigilanza al fine del controllo delle operazioni e dei rapporti direttamente o indirettamente riconducibili ai soggetti obbligati. Il controllo si esplica nei limiti delle informazioni conosciute e ricevute dai soggetti medesimi e solamente sui rapporti e sulle operazioni compiute che abbiano un impatto sul rispetto dei principi etici e del Codice Etico adottato.

La Società assicura un'adeguata diffusione, una corretta conoscenza e una compiuta spiegazione delle prescrizioni normative e del Modello (compreso il Codice Etico) fra il personale, compreso quello direttivo, e i collaboratori, anche per il tramite di appositi corsi e seminari, differenziati in ragione dei soggetti cui è rivolta la formazione, delle aree in cui essi operano e delle mansioni loro assegnate, affinché tutti coloro che, a

vario titolo, operano per la Società abbiano piena conoscenza degli obblighi per essi derivanti dall'effettiva applicazione del Modello (compreso il Codice Etico). Rientra nell'ambito delle responsabilità dell'Organismo di Vigilanza il controllo circa l'effettiva attuazione dei presidi appena indicati. Questi seminari e corsi di formazione potranno essere organizzati anche mediante l'utilizzo di strumenti di e-learning.

I soggetti obbligati al rispetto del Modello assumono - all'atto dello stabilimento del rapporto di impiego o del conferimento dell'incarico o della consulenza - l'obbligo di denuncia, preventivo e a livello generale, delle aree e delle operazioni a rischio o particolarmente sensibili che potranno riguardare sé o i soggetti a sé collegati.

In ogni caso, l'adozione del Modello sarà comunicata a tutte le risorse presenti in azienda al momento della definitiva formalizzazione dello stesso tramite apposita comunicazione; ogni soggetto (dipendente o dirigente) darà atto - con modalità consone - di averne preso opportuna visione e conoscenza.

#### **ART. 10 - ORGANISMO DI VIGILANZA**

L'Organismo di Vigilanza è nominato dall'Amministratore. Esso è incardinato nella figura di un componente esterno, che è in grado di esercitare i compiti e le funzioni di componente dell'OdV in linea con il principio di continuità di azione.

L'OdV vigila sul funzionamento e sull'osservanza del Modello, definisce tempi e modalità del suo aggiornamento, sanziona le irregolarità riscontrate e svolge gli ulteriori compiti meglio dettagliati nel prosieguo della presente Parte Generale del Modello.

Ai fini dell'assolvimento delle proprie funzioni, l'Organismo di Vigilanza è dotato di poteri autonomi di iniziativa e controllo dell'attività amministrativa e gestionale della Società, come meglio dettagliati in seguito.

#### **ART. 11 - REQUISITI DELL'ORGANISMO DI VIGILANZA**

La sussistenza dei requisiti di indipendenza e professionalità del soggetto appartenente all'Organismo di Vigilanza è autocertificata dal medesimo. L'autocertificazione è acquisita all'atto dell'attribuzione del ruolo di componente dell'OdV.

L'OdV mantiene la facoltà di farsi assistere, in relazione a uno o più dei compiti a esso attribuiti ai sensi del Modello, da professionisti esterni alla Società, dotati di specifica esperienza in materia legale, contabile o in altro settore tecnico nonché di un idoneo livello di indipendenza e libertà d'azione e di giudizio.

L'OdV decade dalla carica ove violi i doveri su di lui incombenti. In caso di decadenza, questi è sostituito dall'Amministratore, secondo le regole ordinarie di funzionamento di tale organo.

#### **ART. 12 - COMPITI E POTERI DELL'ORGANISMO DI VIGILANZA**

All'Organismo di Vigilanza è affidato il compito di vigilare: sull'effettività e sull'osservanza del Modello da parte dei soggetti obbligati; sull'efficacia e adeguatezza

del Modello, in relazione all'articolazione della Società e alla concreta capacità di prevenire la commissione dei reati presupposto di cui al Decreto 231; sull'opportunità di procedere a un aggiornamento del Modello al ricorrere delle condizioni rilevanti.

Nel rispetto del principio secondo il quale all'OdV deve essere garantita la massima libertà di iniziativa al fine di incoraggiare il rispetto del Modello e, più in generale, della legalità, l'Organismo di Vigilanza è tenuto ad assolvere ai seguenti compiti:

- controllare che la conoscenza del Modello e delle misure in esso previste o richiamate sia adeguatamente diffusa tra tutti i soggetti obbligati al presente Modello;
- supervisionare i sistemi di prevenzione e di controllo previsti dal Modello o in esso richiamati;
- accertare l'effettiva e corretta applicazione del Modello, attraverso - a titolo esemplificativo e non esaustivo - l'analisi di un significativo campione di documenti attinenti alle aree a rischio di reato; l'audizione del personale e/o dei collaboratori rilevanti; il compimento di ricognizioni sulla mappatura dei processi sensibili rilevanti nell'attività della Società; l'effettuazione di verifiche periodiche su specifiche operazioni o specifici atti;
- ogni volta che lo ritenga opportuno, richiedere informazioni a chiunque operi a qualsiasi titolo nella Società;
- dare immediata notizia all'Amministratore dell'eventuale accertamento di violazioni che possano determinare la commissione di reati di cui alla Parte Speciale del Modello, affinché sia impedito il compito dell'azione o sia evitata la verifica dell'evento;
- redigere e trasmettere all'Amministratore relazioni delle attività di verifica periodica effettuata su specifiche operazioni o specifici atti;
- redigere e trasmettere all'Amministratore, con cadenza almeno annuale, una relazione circa l'attività svolta nel corso dell'esercizio precedente;
- redigere e conservare verbali delle proprie adunanze;
- monitorare l'adeguatezza del sistema disciplinare di cui al presente Modello.

Qualora lo ritenga opportuno al fine del più regolare svolgimento dei propri compiti, l'Organismo di Vigilanza può: nominare un consulente esterno con l'incarico di coadiuvare l'OdV; emanare dei protocolli operativi miranti a disciplinare in linea generale le proprie modalità di funzionamento e d'azione, anche in sede ispettiva, nonché le modalità di richiesta delle informazioni all'Amministratore, ai dipendenti e ai collaboratori della Società. Tali protocolli hanno, previa approvazione dell'Amministratore, valore vincolante per ogni dipendente o collaboratore.

Al fine di consentire all'OdV di svolgere adeguatamente i propri compiti, sono messi a sua disposizione mezzi tecnici adeguati, compresa la creazione di un'apposita casella di posta elettronica, con accesso riservato in via esclusiva ai componenti dell'OdV, [odv@villaesther.it](mailto:odv@villaesther.it).

### **ART. 13 - COMPENSO E DOTAZIONE PATRIMONIALE**

L'OdV può percepire un compenso deliberato dall'Amministratore.

La dotazione patrimoniale adeguata a consentire il corretto svolgimento dei compiti dell'OdV è assegnata in via previsionale all'inizio di ogni esercizio da parte dell'Amministratore. Ogni diminuzione degli stanziamenti a favore dell'Organismo di Vigilanza è portata a sua conoscenza. Qualora si dovesse rendere necessaria per consentire il corretto svolgimento dei compiti dell'OdV un'integrazione dei mezzi patrimoniali in dotazione, l'Amministratore vi provvede di propria iniziativa ovvero se interessato dall'OdV.

Le spese aventi carattere straordinario, eventualmente necessarie ed eccedenti la dotazione patrimoniale assegnata, potranno essere autorizzate all'Amministratore dietro richiesta motivata dell'Organismo di Vigilanza.

#### **ART. 14 - RIUNIONI**

L'Organismo di Vigilanza si riunisce con frequenza almeno quadrimestrale. Delle riunioni dell'OdV è redatto verbale, copia del quale viene trasmessa all'Amministratore. Alle riunioni può partecipare un professionista esterno alla Società esperto in materie legali inerenti alle tematiche oggetto del presente Modello.

Alle riunioni partecipa sempre il referente dell'OdV nominato dalla Società.

#### **ART. 15 - INFORMATIVA RESA ALL'ODV**

L'Organismo assume informazioni direttamente, anche mediante ispezioni o richieste a dipendenti e collaboratori, anche esterni, della Società, con la periodicità che esso ritenga più adeguata al corretto assolvimento delle proprie funzioni. Al fine di assicurare un ordinato svolgimento dell'operatività aziendale, l'Organismo di Vigilanza informa preventivamente il responsabile dell'ufficio interessato dell'esigenza di chiedere la collaborazione del personale addetto a quel determinato ufficio; quando la richiesta di collaborazione riguarda i soggetti di vertice, l'OdV ne informa preventivamente l'Amministratore.

L'Organismo di Vigilanza può chiedere all'Amministratore, con motivazione, l'esibizione dei libri sociali o l'estrazione di copia dagli stessi, per fini di controllo su questioni o affari determinati.

L'Organismo di Vigilanza è tenuto al più stretto riserbo e segreto professionale relativamente alle informazioni di cui venga a conoscenza nell'espletamento dell'incarico e agisce con il massimo grado di diligenza per evitare qualsiasi fuga di notizie o informazioni riservate. Le informazioni ricevute nell'esercizio delle funzioni dell'OdV sono adeguatamente protocollate e conservate a cura dello stesso Organismo di Vigilanza.

L'Amministratore può decidere di dotare l'OdV di una apposita casella di posta elettronica funzionale a consentire a chiunque operi per la Società di segnalare all'OdV stesso, nel rispetto del principio della massima riservatezza, possibili violazioni del Modello. È altresì prevista la facoltà dell'Amministratore di far predisporre ulteriori o alternativi mezzi fisici (ad esempio cassetta postale per segnalazioni cartacee) con la medesima finalità.

#### **ART. 16 - INFORMATIVA RESA DALL'ODV**

L'OdV è tenuto a riferire relativamente alla conduzione e all'esito delle verifiche effettuate in veste di OdV, direttamente all'Amministratore ogni volta che lo ritenga opportuno, se del caso anche mediante uno specifico rapporto sugli interventi di maggiore rilievo svolti o in corso di svolgimento nel quadrimestre di riferimento.

In ogni caso, l'OdV trasmette all'Amministratore relazioni dell'attività di verifica periodica effettuata su specifiche operazioni o specifici atti.

Con cadenza annuale, l'OdV dà notizia all'Amministratore dell'attività svolta, tramite apposita relazione riferita all'esercizio precedente.

#### **ART. 17 - RIESAME E AGGIORNAMENTO DEL MODELLO**

L'OdV, anche per il tramite dei professionisti di cui decida di avvalersi, effettua un riesame del Modello con periodicità almeno annuale e, se del caso, provvede alla modifica o integrazione del Modello all'esito del riesame. Al fine di effettuare un efficace riesame, l'OdV sente il personale o i collaboratori rilevanti per acquisire eventuali proposte operative inerenti all'applicazione del Modello.

Nel caso intervengano variazioni, anche di carattere normativo, che rendano necessario un aggiornamento del Modello, totale o parziale, l'OdV vi provvede entro un breve lasso temporale, anche per il tramite dei professionisti di cui decida di avvalersi, a prescindere dall'avvenuto riesame.

Qualsiasi modifica del Modello è portata a conoscenza di tutti gli interessati in modo tempestivo e completo.

## SEZIONE II - SISTEMA DISCIPLINARE

### ART. 18 - FUNZIONE DEL SISTEMA DISCIPLINARE

In conformità dell'art. 6, co. 1, lett. e), del Decreto 231, ai sensi del quale la prova dell'avvenuta introduzione di *“un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”* costituisce uno degli elementi essenziali per l'esimente della responsabilità della Società, la Società ha definito e applica un sistema disciplinare che individua le sanzioni – commisurate alla violazione e con valore di deterrente – previste in caso di violazione delle procedure indicate nel Modello da parte di componenti degli organi sociali, dirigenti, dipendenti e collaboratori.

Il sistema disciplinare della Società rispetta i limiti connessi al potere sanzionatorio imposti dall'art. 7 della l. n. 300/1970 (c.d. *“Statuto dei lavoratori”*) e dalla contrattualizzazione collettiva di settore e aziendale, sia per quanto riguarda le sanzioni irrogabili (che risultano *“tipizzate”* in relazione al collegamento con specificati indebiti disciplinari) sia per quanto riguarda la forma di esercizio di tale potere. Le sanzioni irrogabili sono adottate e applicate nel rispetto delle procedure previste dalle normative collettive nazionali ed aziendali applicabili al rapporto di lavoro. In caso di violazioni commesse da parte dei dirigenti, l'assunzione dei provvedimenti ritenuti idonei tiene conto della specifica qualifica dirigenziale e, dunque, del particolare vincolo fiduciario sottostante al rapporto di lavoro con la Società.

Il sistema disciplinare è altresì funzionale a rendere maggiormente efficiente l'azione di controllo dell'Organismo di Vigilanza e a garantirne l'effettività.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto 231.

In particolare, la violazione dei principi generali e/o delle procedure disciplinate o richiamate dal Modello così come la violazione delle regole di comportamento imposte dal Codice etico, dal Sistema disciplinare e dalle procedure aziendali, ad opera di lavoratori dipendenti della Società, costituiranno inadempimento alle obbligazioni derivanti da rapporto di lavoro e illecito disciplinare.

Fermo restando il principio di collegamento tra i provvedimenti disciplinari irrogabili e le fattispecie in relazione alle quali gli stessi possono essere assunti, nell'irrogazione della sanzione disciplinare dovrà necessariamente essere rispettato il principio della proporzionalità tra infrazione e sanzione.

Le violazioni della normativa vigente, del Modello o del Codice etico commesse dagli altri soggetti con cui la Società entra in contatto nello svolgimento di relazioni d'affari, sono sanzionate secondo i meccanismi contrattuali pattuiti o, in mancanza di essi, secondo le regole generali del Codice civile.

## **ART. 19 - COMPORTAMENTI RILEVANTI**

Ai fini del presente sistema disciplinare e nel rispetto della contrattazione collettiva applicabile alla Società, costituiscono violazione del Modello o delle misure e procedure in esso disciplinate o richiamate, tutte le condotte, commissive o omissive (anche colpose), che siano idonee a ledere l'efficacia del Modello quale strumento di prevenzione del rischio di commissione dei reati-presupposto rilevanti ai fini del Decreto 231.

L'Ufficio del Personale valuta le sanzioni irrogabili nel rispetto del principio di proporzionalità e tenuto conto di tutti gli elementi e/o delle circostanze rilevanti, secondo un ordine crescente di gravità da valutarsi ad opera dell'OdV.

## **ART. 20 - CRITERI DI IRROGAZIONE DELLE SANZIONI**

In caso di accertamento delle violazioni del Modello, le sanzioni verranno applicate nel rispetto delle disposizioni contenute nel presente Modello, nella contrattazione collettiva tempo per tempo vigente e nel codice disciplinare adottato in azienda. In ogni caso, l'individuazione e l'irrogazione delle sanzioni previste dal sistema disciplinare deve tenere conto dei principi di proporzionalità e adeguatezza delle stesse rispetto alla violazione contestata. Nello specifico, gli elementi da tenere in considerazione sono:

- gravità della condotta o dell'evento che quest'ultima ha determinato;
- tipologia di violazione compiuta;
- circostanze nel cui ambito si è sviluppata la condotta;
- le modalità della condotta.

La sanzione è aggravata nei seguenti casi:

- commissione di più violazioni nell'ambito della medesima condotta; in questo caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
- concorso di più soggetti nella commissione della violazione;
- recidiva dell'autore della condotta.

## **ART. 21 - SANZIONI NEI CONFRONTI DELL'AMMINISTRATORE**

In caso di commissione da parte dell'Amministratore di una delle condotte rilevanti ai fini dell'irrogazione di una sanzione, le sanzioni applicabili sono:

- rimprovero scritto;
- diffida al puntuale rispetto del Modello;
- decurtazione degli emolumenti o del corrispettivo se previsto, fino a un ammontare massimo del 60%;

- revoca dell'incarico;

ferma restando la possibilità per la Società di agire per il maggior danno.

#### **ART. 22 - SANZIONI NEI CONFRONTI DEI DIRIGENTI APICALI E DEGLI ALTRI SOGGETTI APICALI**

In caso di commissione da parte di un dirigente apicale di una delle condotte rilevanti ai fini dell'irrogazione di una sanzione, tenuto conto anche della contrattazione collettiva tempo per tempo vigente e del codice disciplinare adottato in azienda, le sanzioni applicabili, sono:

- rimprovero verbale;
- rimprovero scritto;
- sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni;
- licenziamento per giustificato motivo;
- licenziamento per giusta causa.

In caso di commissione da parte di un altro soggetto apicale di una delle condotte rilevanti ai fini dell'irrogazione di una sanzione, le sanzioni applicabili sono quelle previste per l'Amministratore.

#### **ART. 23 - SANZIONI NEI CONFRONTI DEI DIPENDENTI**

In caso di commissione da parte di un dipendente di una delle condotte rilevanti ai fini dell'irrogazione di una sanzione, le sanzioni applicabili, tenuto conto anche della contrattazione collettiva tempo per tempo vigente, sono:

- rimprovero verbale;
- rimprovero scritto;
- sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni;
- licenziamento per giustificato motivo;
- licenziamento per giusta causa.

Per i dirigenti non apicali, sono fatte salve le disposizioni applicabili previste dalla contrattazione collettiva rilevante nel caso concreto.

Quando sia richiesto dalla natura della condotta posta in essere o dalla necessità di svolgere accertamenti ulteriori rispetto al mero riscontro della medesima, la Società – nel lasso temporale necessario per deliberare il provvedimento disciplinare definitivo – può disporre l'allontanamento temporaneo del dipendente dal servizio.

#### **ART. 24 - SANZIONI NEI CONFRONTI DEI TERZI DESTINATARI**

In caso di commissione da parte di un terzo (consulente o collaboratore esterno) di una delle condotte rilevanti ai fini dell'irrogazione di una sanzione, le sanzioni applicabili sono:

- diffida al puntuale rispetto del Modello pena l'applicazione della penale di seguito indicata ovvero la risoluzione del rapporto negoziale intercorrente con la Società;
- applicazione di una penale, convenzionalmente prevista tra il 10% ed il 30% del fatturato totale lordo annuo;
- risoluzione immediata del rapporto negoziale intercorrente con la Società.

Nell'ambito dei rapporti con i terzi, la Società inserisce nelle lettere d'incarico e negli accordi negoziali, apposite clausole volte a prevedere l'applicazione delle sanzioni previste dal presente sistema disciplinare in caso di violazione del Modello.

#### **ART. 25 - RUOLO DELL'ODV IN RELAZIONE AI PROCEDIMENTI DI IRROGAZIONE DI SANZIONI**

Quando, nell'ambito delle verifiche condotte autonomamente nell'esercizio della sua attività di monitoraggio sull'applicazione del Modello ovvero sulla base di segnalazioni ricevute anche in forma anonima, l'OdV riscontra il pericolo di violazione del Modello, esso ha l'obbligo di attivarsi al fine di espletare gli accertamenti e i controlli opportuni, avvalendosi di ogni mezzo e potere rientrante nella sua disponibilità ai sensi del presente Modello.

Dopo aver esaustivamente portato a termine l'attività di ricerca, verifica e controllo, l'OdV valuta, sulla base degli elementi in proprio possesso, se è stata realmente integrata un'ipotesi di violazione del Modello soggetta a sanzione e:

- in caso positivo, procede quindi alla redazione di apposita relazione da trasmettere ai diversi organi competenti, a seconda del soggetto che è incorso nella violazione;
- in caso negativo, segnala per iscritto l'accaduto all'Amministratore e al responsabile dell'Ufficio del Personale affinché questi soggetti svolgano eventuali valutazioni circa la rilevanza della condotta rispetto alla legge e ai regolamenti applicabili.

Qualora i soggetti di cui sopra rilevino che la violazione del Modello riscontrata dall'OdV concreti anche una o più violazioni delle previsioni dei regolamenti aziendali e/o della contrattazione collettiva, all'esito del procedimento prescritto, possono irrogare anche sanzioni ulteriori o più gravi rispetto a quelle proposte dall'OdV, sempreché queste siano in concreto applicabili.

## **ART. 26 - PROCEDIMENTO DI IRROGAZIONE DI SANZIONI NEI CONFRONTI DELL'AMMINISTRATORE**

In caso di violazioni commesse ad opera dell'Amministratore, l'OdV trasmette al Sindaco della società una relazione contenente: i dati identificativi dell'Amministratore; la descrizione della condotta contestata; l'indicazione delle previsioni del Modello che risultano essere state violate; gli eventuali documenti ed elementi a supporto della contestazione; una proposta di applicazione della sanzione.

Entro dieci giorni dall'acquisizione della relazione, il Sindaco convoca l'Amministratore mediante una comunicazione scritta, contenente: l'indicazione della condotta contestata; le previsioni del Modello oggetto di violazione; l'indicazione della data dell'adunanza e della facoltà dell'interessato di formulare, anche in quella sede, eventuali rilievi e/o deduzioni, sia scritte che verbali. partecipa l'OdV.

A seguito dell'audizione dell'interessato, il Sindaco assume provvedimenti in merito all'irrogazione della sanzione, determinandone l'entità. Il Sindaco deve motivare l'eventuale dissenso rispetto alla proposta formulata dall'OdV circa la sanzione da irrogare.

Il provvedimento di irrogazione della sanzione è comunicato in forma scritta all'interessato e all'OdV, entro dieci giorni dall'invio della contestazione.

Il Sindaco e l'ODV verificano l'effettiva applicazione della sanzione irrogata.

Tale procedimento trova applicazione anche qualora sia riscontrata la violazione del Modello ad opera dell'organo di controllo monocratico.

## **ART. 27 - PROCEDIMENTO NEI CONFRONTI DEI DIRIGENTI APICALI**

Quando, nell'esercizio dell'attività di monitoraggio sull'applicazione del Modello da parte dell'OdV, questi riscontri una la violazione del Modello da parte di un dirigente apicale, la procedura di accertamento dell'illecito e di irrogazione della sanzione avviene nel rispetto delle disposizioni della contrattazione collettiva tempo per tempo vigente e del codice disciplinare adottato in azienda.

In particolare, l'OdV trasmette all'Amministratore e al responsabile dell'Ufficio del Personale una relazione contenente: i dati identificativi del soggetto responsabile della violazione; la descrizione della condotta contestata; l'indicazione delle previsioni del Modello che risultano essere state violate; gli eventuali documenti ed elementi a supporto della contestazione; una proposta di applicazione della sanzione.

Entro dieci giorni dall'acquisizione della relazione dell'OdV, l'Amministratore, di concerto con il responsabile dell'Ufficio del Personale contesta al dirigente apicale, mediante una comunicazione scritta, a firma congiunta dei predetti soggetti, contenente: la puntuale indicazione della condotta constatata; le previsioni del Modello oggetto di violazione; l'indicazione della data dell'adunanza dell'OdV e della facoltà dell'interessato di formulare eventuali rilievi e/o deduzioni scritte entro un termine non inferiore a 10 giorni dal ricevimento della comunicazione nonché di richiedere l'intervento del rappresentante dell'associazione sindacale cui il dirigente apicale aderisce o conferisce mandato.

A seguito delle eventuali controdeduzioni del dirigente apicale interessato, i soggetti competenti si pronunciano in ordine alla determinazione e all'applicazione della sanzione, motivando l'eventuale dissenso rispetto alla proposta formulata dall'OdV.

In ogni caso, i provvedimenti disciplinari non possono essere comminati prima che siano trascorsi 10 giorni dalla ricezione della contestazione da parte del dirigente apicale interessato.

Il responsabile dell'Ufficio del Personale cura l'effettiva applicazione della sanzione nel rispetto delle norme di legge e di regolamento nonché delle previsioni contenute nella contrattazione collettiva tempo per tempo vigente e nel codice disciplinare adottato in azienda.

L'OdV, al quale viene inviato per conoscenza il provvedimento di irrogazione della sanzione, verifica la sua applicazione.

Il dirigente può, nei venti giorni successivi alla ricezione del provvedimento, promuovere la costituzione di un collegio di conciliazione e arbitrato, secondo le previsioni del CCNL, restando in tal caso la sanzione sospesa fino alla relativa pronuncia. Rimane ferma la possibilità di adire l'Autorità Giudiziaria.

#### **ART. 28 - PROCEDIMENTO NEI CONFRONTI DEGLI ALTRI SOGGETTI APICALI**

Qualora sia riscontrata la violazione del Modello da parte di un altro soggetto apicale trovano applicazione, quanto al procedimento di contestazione e a quello di eventuale irrogazione della sanzione, le previsioni di cui all'articolo precedente nonché quelle contenute nella contrattazione collettiva tempo per tempo vigente e nel codice disciplinare adottato in azienda; in questo caso, le sanzioni sono individuate direttamente dell'Amministratore.

#### **ART. 29 - PROCEDIMENTO NEI CONFRONTI DEI DIPENDENTI**

Quando, nell'esercizio dell'attività di monitoraggio sull'applicazione del Modello l'OdV riscontra una violazione del Modello da parte di un dipendente, trovano applicazione, quanto al procedimento di contestazione e a quello di eventuale irrogazione della sanzione, le previsioni di cui all'articolo che precede, formulate con riguardo ai dirigenti apicali e agli altri soggetti apicali, compresa la facoltà per il dipendente di promuovere, nei venti giorni successivi la ricezione del provvedimento, la costituzione di un collegio di conciliazione e arbitrato; qualora il dipendente si avvalga di questa facoltà, la sanzione resta sospesa fino alla relativa pronuncia. Rimane ferma la possibilità di adire l'Autorità Giudiziaria.

#### **ART. 30 - PROCEDIMENTO NEI CONFRONTI DI TERZI**

Quando, nell'esercizio dell'attività di monitoraggio sull'applicazione del Modello, l'OdV riscontra una violazione del Modello da parte di un terzo (collaboratore o consulente), l'OdV trasmette all'Amministratore e alla persona responsabile del rapporto contrattuale una relazione contenente: i dati identificativi del soggetto responsabile della violazione; la descrizione della condotta contestata; l'indicazione

delle previsioni del Modello che risultano essere state violate; gli eventuali documenti ed elementi a supporto della contestazione; una proposta di applicazione della sanzione opportuna rispetto al caso concreto.

Entro dieci giorni dalla ricezione della relazione, la persona responsabile del rapporto contrattuale rilevante formula una proposta in merito alla medesima relazione, motivando l'eventuale scostamento rispetto alla proposta di sanzione formulata dall'OdV.

Una volta definita la sanzione, la persona responsabile del rapporto contrattuale rilevante invia all'interessato una comunicazione scritta contenente l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione.

Il provvedimento di applicazione della sanzione è comunicato per iscritto all'interessato a cura della persona responsabile del rapporto contrattuale rilevante, che provvede anche all'effettiva applicazione della sanzione, sotto il controllo dell'OdV.

#### **ART. 31 - PROCEDIMENTO DI IRROGAZIONE DI SANZIONI IN CASO DI VIOLAZIONE DELLA NORMATIVA WHISTLEBLOWING**

Quando, nell'esercizio dell'attività di monitoraggio sull'applicazione della normativa relativa alla procedura di segnalazione illeciti ed irregolarità (whistleblowing), l'OdV riscontri una violazione da parte dei soggetti destinatari, si segue il procedimento di contestazione ed eventuale irrogazione della sanzione, ferma restando la possibilità di adire l'Autorità Giudiziaria.

In particolare, l'OdV trasmette all'Amministratore una relazione contenente: i dati identificativi del soggetto responsabile della violazione; la descrizione della condotta contestata; l'indicazione delle previsioni del Modello che risultano essere state violate; gli eventuali documenti a supporto della contestazione; una proposta di applicazione della sanzione.

Nel caso in cui siano state tenute condotte vessatorie o siano state adottate misure ritorsive nei confronti del soggetto segnalante trovano applicazione per l'ente le sanzioni pecuniarie ed interdittive di cui ai precedenti articoli.

## PARTE SPECIALE

### SEZIONE I - STRUTTURA DELLA PARTE SPECIALE E ORGANIZZAZIONE INTERNA DELLA SOCIETÀ

#### ART. 32 - STRUTTURA DELLA PARTE SPECIALE

La Parte Speciale del Modello descrive, nell'Allegato I, le condizioni al ricorrere delle quali ciascuno dei reati-presupposto previsti dal Decreto 231 può ritenersi integrato, nonché le rispettive sanzioni. Queste sanzioni, pecuniarie e interdittive, sono ridotte da un terzo alla metà in relazione alla commissione di questi reati-presupposto nelle forme del tentativo.

La Parte Speciale del Modello individua inoltre, per ciascun reato-presupposto, i seguenti elementi:

- **area o aree e/o attività** in relazione alle quali sussiste un rischio di commissione dei reati-presupposto;
- **livello di rischio** di commissione dei reati-presupposto, anche in considerazione della classificazione di questi reati come: "reati peculiari", vale a dire reati suscettibili di venire tipicamente in considerazione, stante la natura dell'attività prestata; "reati atipici", vale a dire reati che di norma, sempre in ragione della natura dell'attività prestata, non sono tipicamente suscettibili di venire in considerazione; e "reati comuni", vale a dire reati che possono venire in considerazione a prescindere dalla specifica attività prestata;
- le misure e i sistemi di controllo adottati per la **prevenzione** dei reati-presupposto.

#### ART. 33 - ORGANIZZAZIONE INTERNA DELLA SOCIETÀ

La Società è un'istituzione sanitaria, che eroga prestazioni di diagnosi e cura per il Servizio Sanitario Nazionale in regime di degenza ospedaliera e prestazioni, diagnostiche e terapeutiche, di tipo ambulatoriale. Essa è dotata di 74 posti letto accreditati suddivisi in tre unità operative: Chirurgia generale, Medicina generale e Recupero e Riabilitazione funzionale. Nell'unità operativa di Chirurgia generale sono presenti moduli di Ortopedia, Oculistica e Urologia.

La Casa di Cura è dotata, inoltre, di servizi di diagnostica per immagini e laboratorio di analisi; è inoltre operante un poliambulatorio con specialità mediche e chirurgiche, tra cui Cardiologia, Fisiopatologia respiratoria, Ortopedia, Chirurgia generale, Endoscopia, Urologia, Oculistica.

Sotto il profilo organizzativo, la Società è suddivisa nelle seguenti aree aziendali:

- Amministratore Unico;
- Direzione Sanitaria;

- Reparto di Chirurgia generale, a sua volta articolato nei moduli di Ortopedia, Oculistica e Chirurgia urologica;
- Reparto di Medicina generale;
- Reparto di Recupero e Riabilitazione Funzionale;
- Area Amministrativa, che comprende i seguenti uffici: personale, contabilità, accettazione e ricoveri, acquisti;
- Servizio di radiologia
- Servizio di anestesia;
- Servizio di laboratorio analisi;
- Area Poliambulatori.

È stato nominato un Rspg e un responsabile dei Sistemi Informativi.

È stato nominato un responsabile del trattamento dati.

## **PROCESSI AZIENDALI RILEVANTI**

### **ART. 34 – DESCRIZIONE E GESTIONE DEI FLUSSI FINANZIARI**

Il sistema di controllo di gestione della Società prevede meccanismi di verifica della gestione delle risorse che devono garantire, oltre alla verificabilità e tracciabilità delle spese, l'efficienza e l'economicità delle attività aziendali, mirando ai seguenti obiettivi:

- definire in maniera chiara, sistematica e conoscibile le risorse a disposizione delle singole Direzioni e degli Uffici e il perimetro nell'ambito del quale tali risorse possono essere impiegate, attraverso la programmazione e la definizione del budget.
- Rilevare gli eventuali scostamenti rispetto a quanto predefinito in sede di budget, analizzarne le cause e riferire i risultati delle valutazioni agli appropriati livelli gerarchici per gli opportuni interventi di adeguamento.
- Predisporre situazioni periodiche di aggiornamento in cui la programmazione iniziale definita nel budget viene rivista sulla base degli scostamenti rilevati.
- La Casa di cura è tenuta a rispettare i limiti di finanziamento erogati dalla regione e di conseguenza il contratto di budget stipulato con l'ASL di appartenenza.

### **ART. 35 - GESTIONE DEL PROCESSO DI APPROVVIGIONAMENTO**

La procedura relativa alla gestione degli acquisti regola tutte le attività relative agli acquisti di farmaci, presidi, apparecchiature biomediche, materiale di consumo e servizi, al fine di garantire che gli stessi siano conformi alle specifiche richieste nonché tutte le attività relative all'accertamento della conformità dei prodotti ricevuti dall'esterno.

Obiettivo della Casa di Cura è quello di ottimizzare gli approvvigionamenti al fine di ridurre gli sprechi, sovraccarico di magazzino, fermi di erogazione del servizio e la valutazione delle prestazioni dei fornitori.

Sono previste le seguenti fasi: Rilevazione fabbisogno; Richiesta preventivo; Emissione degli ordini di acquisto; Controllo degli acquisti; Gestione delle non conformità.

#### **ART. 36 - TRATTAMENTO DEI DATI PERSONALI**

Le procedure seguite nella Società in materia di trattamento e protezione dei dati personali, sensibili e non, di pazienti e di lavoratori, sono conformi al Regolamento UE 679/16. La Società ha provveduto alla nomina di un Responsabile della protezione dati (DPO), nonché alla valutazione dei rischi connessi al trattamento stesso.

Il DPO svolge le proprie attività in conformità del GDPR n. 679/16, effettua verifiche periodiche e gestisce il Registro dei trattamenti, svolge corsi di formazione in materia di trattamento dei dati sanitari.

#### **ART. 37 - GESTIONE DEL SISTEMA INFORMATIVO**

I principali sistemi di gestione delle aree dell'amministrazione, contabilità, controllo di gestione, personale, acquisti, logistica sono supportati da applicativi informatici di buon livello qualitativo che assicurano altresì un buon livello di standardizzazione e di compliance; i processi sono infatti gestiti da tali applicativi validati a monte del rilascio del software.

La gestione dei sistemi informativi, utilizzando procedure che sono volte a garantire la sicurezza fisica e logica dei sistemi e dei dati in essi contenuti, è orientata ad assicurare:

- il principio di separazione dei compiti mediante la contrapposizione delle funzioni;
- la tracciabilità delle operazioni e la evidenza documentale dei controlli.

La Casa di Cura Villa Esther, nell'utilizzo dei sistemi informativi, poggia sull'architettura posta a protezione e prevenzione di possibili intrusioni, manomissioni di apparati o uso improprio della strumentazione aziendale.

Nell'architettura di rete le funzioni di sicurezza sono implementate a diversi livelli:

- protocolli di trasferimento;
- apparati specifici o condivisi;
- server;
- postazioni degli utenti interni;
- postazioni degli utenti esterni.

Il concetto base del sistema di sicurezza verte sul fatto che la comunità degli utenti di Villa Esther non possa accedere direttamente ad internet se non attraverso Firewall, il quale, verificando una definita catena di regole, autorizza o rifiuta l'instradamento verso la rete, consentendo o meno l'uso di porte e protocolli considerati pericolosi o insicuri.

Firewall, Proxy Server, File Server, DHCP server, DNS server, Application Server e Server Web sono collocati in un apposito locale tecnico, il cui accesso è inibito al personale non autorizzato.

Tutti i Server aziendali sono accedibili solo attraverso credenziali digitali e sono configurati per registrare nei files di Log di ogni servizio qualunque evento si verifichi (es. login e logout verso una macchina o uno specifico servizio, tentativo di accesso eseguito con credenziali non corrette, etc.).

L'implementazione di LAN virtualmente dedicate assicura la confidenzialità del transito. Infatti, le Virtual LAN (VLAN) ripartiscono e segmentano il traffico, segregando il transito delle informazioni in differenti reti private virtuali, con un forte controllo (o divieto) di incrocio di traffico proveniente da altri segmenti di VLAN, funzione questa delegata ad apparati di routing opportunamente configurati.

Inoltre, per rafforzare ulteriormente il sistema di sicurezza, sono stati profilati differenti livelli di utenza. Il primo livello gestisce informazioni critiche o parzialmente critiche come, ad esempio, i servizi di amministrazione, quelli sanitari, etc. Gli utenti profilati a tale livello dispongono di personal computer compatibili esclusivamente dedicati, configurati con profili di accesso che permettono esclusivamente l'uso di applicazioni precedentemente istallate (Office, antivirus, utility di servizio) ed hanno spazi prestabiliti sui File Server aziendali. Ogni altro tipo di installazione di applicazioni è bloccata. Per accedere sono necessari nome utente e password personali.

Un secondo livello di utenza può utilizzare solo alcuni personal computer disponibili in azienda accedendo comunque con nome utente e password personali. Il Server restituisce il profilo utente autenticato, i suoi documenti di lavoro, i soli percorsi sui File Server ed i servizi verso i quali è autorizzato.

Il terzo livello di utenza utilizza notebook disponibili in azienda che sono dedicati all'utilizzo di software e apparecchiature specifiche e che non hanno collegamento fisico alla rete. Gli utenti sono configurati con profili di accesso generici che permettono esclusivamente l'uso di applicazioni precedentemente istallate (Office, antivirus, utility di servizio). In questo caso il sistema non dà accesso alla rete aziendale e, conseguentemente, nemmeno ad Internet e ai File Server. Tutte le altre operazioni non sono consentite. Si accede con nome utente e password comunque personali.

Infine, l'utenza che si collega attraverso tunnel criptati VPN (Virtual Private Networks) ai servizi aziendali dall'esterno della sede di appartenenza, è sottoposta a puntuali controlli di autenticazione attraverso certificati digitali che assicurano l'accesso solo ai servizi per i quali è attiva l'autorizzazione prevista dalle policy stabilite a livello individuale.

Qui di seguito **le specifiche misure e procedure di protezione** previste dal Responsabile dei sistemi informativi, alle quali tutti i soggetti coinvolti dalla normativa 231 devono attenersi:

1. Misure di protezione dei documenti elettronici (es. firma digitale);

Le misure di protezione dei documenti elettronici che l'azienda ha adottato sono:

- **Accesso limitato:** l'accesso ai documenti elettronici sensibili è limitato solo al personale autorizzato. L'azienda ha stabilito una policy di accesso e ha adottato misure di sicurezza, come l'autenticazione con l'utilizzo di password complesse, per garantire che solo i dipendenti autorizzati possano accedere ai documenti.
- **Crittografia:** i documenti elettronici sensibili sono conservati su storage criptati per proteggerli dall'accesso non autorizzato. L'azienda utilizza la crittografia a livello di disco, con algoritmi di crittografia avanzati come AES (Advanced Encryption Standard), per proteggere i documenti.
- **Backup e ripristino:** vengono regolarmente effettuati il backup dei documenti elettronici sensibili e le copie di backup sono mantenute in una posizione sicura, al fine di prevenire la perdita di dati in caso di malfunzionamenti dei dispositivi di archiviazione.
- **Protezione antivirus e antimalware:** l'azienda utilizza un software antivirus e antimalware per proteggere i suoi sistemi e documenti dalle minacce informatiche come virus, worm, trojan e malware in generale.
- **Controllo dei permessi:** sono stabiliti chiaramente i permessi per i documenti elettronici, come il controllo del livello di accesso, la modifica o la visualizzazione, e sono adottati strumenti di sicurezza in grado di monitorare questi permessi e rilevare eventuali attività sospette.

Oltre queste misure di protezione dei documenti elettronici l'azienda mantiene costantemente monitorati e aggiornati tutti i suoi strumenti di sicurezza per garantire la massima sicurezza dei propri supporti digitali.

2. Procedure di validazione delle credenziali dotate di un sufficiente livello di complessità, soggette a modifica periodica e che prevedono la rimozione dei diritti di accesso al termine del rapporto di lavoro;

Le credenziali sono un elemento fondamentale per garantire la sicurezza dei dati digitali, poiché consentono di accedere a sistemi, applicazioni e documenti riservati. Per garantire che le credenziali siano dotate di sufficiente livello di complessità e sicurezza, l'Azienda adotta le seguenti procedure di validazione:

- **Lunghezza:** le credenziali devono essere abbastanza lunghe da rendere difficile l'individuazione tramite attacchi di forza bruta. È obbligatorio quindi utilizzare password di almeno 8 caratteri.

- Complessità: le credenziali devono essere abbastanza complesse ed evitare l'utilizzo di parole facilmente indovinabili. E' obbligatorio utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli.
- Cambi frequenti: per ridurre il rischio di compromissione dei dati a seguito di furti o perdite di credenziali è obbligatorio il cambio periodico delle credenziali con tempi che vanno da 1 a 3 mesi.
- Utilizzo di soluzioni di autenticazione a più fattori (MFA): per alcuni sistemi di accesso (ad esempio quello degli amministratori) l'azienda utilizza soluzioni di autenticazione a più fattori, come l'invio di un codice di verifica sul telefono cellulare dell'utente, che rendono più difficile l'accesso non autorizzato alle credenziali.

L'amministratore di sistema si occupa, inoltre, della formazione al personale sui rischi associati alle credenziali non sicure per sensibilizzarli sulla necessità di adottare comportamenti corretti in materia di sicurezza informatica.

### 3. Aggiornamento regolare dei sistemi informatici in uso

Le procedure che Villa Esther ha adottato per garantire che i sistemi informatici siano sempre aggiornati:

- Pianificazione degli aggiornamenti: l'azienda pianifica gli aggiornamenti dei sistemi informatici con regolarità, e stabilisce un calendario che prevede anche eventuali interruzioni di servizio necessarie per l'installazione degli aggiornamenti dei sistemi. Ad ogni modo, per evitare disservizi, la maggior parte di essi vengono comunque effettuati nei giorni con poco carico di lavoro (es: festivi).
- Monitoraggio degli avvisi di sicurezza: l'azienda monitora regolarmente gli avvisi di sicurezza rilasciati dai produttori dei sistemi informatici e degli applicativi utilizzati, per identificare eventuali vulnerabilità e gli aggiornamenti necessari per correggerle.
- Utilizzo di strumenti di gestione degli aggiornamenti: l'azienda adotta strumenti di gestione degli aggiornamenti, come i servizi di aggiornamento automatico, per semplificare e automatizzare il processo di aggiornamento dei sistemi.
- Test degli aggiornamenti: se necessario, prima di implementare gli aggiornamenti sui sistemi in produzione, questi vengono testati in un ambiente di separato, per verificare che non abbiano impatti negativi sui sistemi e sulle applicazioni in uso.
- Backup dei dati: prima di implementare gli aggiornamenti, sono effettuati backup dei dati, in modo da poter ripristinare le informazioni in caso di problemi durante l'aggiornamento.
- Formazione del personale: il personale dell'azienda viene costantemente informato sull'importanza degli aggiornamenti e sui rischi legati all'utilizzo di sistemi non aggiornati o non protetti.

4. Procedure di autorizzazione per l'accesso ai sistemi informatici aziendali, che prevedono la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al rispettivo ruolo.

Le procedure di autorizzazione per l'accesso a sistemi informatici aziendali di Villa Esther sono basate sul principio del "minimo privilegio", ossia l'assegnazione di permessi di accesso solo a quelle risorse informatiche necessarie per lo svolgimento delle attività legate al ruolo dell'utente.

In breve, la l'autorizzazione prevede i seguenti passaggi:

- Identificazione del ruolo: l'azienda identifica il ruolo del proprio dipendente e definisce i relativi permessi di accesso ai sistemi informatici e alle risorse aziendali. Questo passaggio prevede anche la definizione dei livelli di autorizzazione per ogni ruolo, in modo da garantire che gli utenti possano accedere solo alle risorse strettamente necessarie per svolgere le proprie mansioni.
- Richiesta di accesso: quando un dipendente assume un nuovo ruolo o ha bisogno di maggiori permessi per svolgere le proprie attività, deve presentare una richiesta (anche verbale) di accesso al responsabile dell'IT o al gestore della sicurezza informatica dell'azienda. La richiesta è accompagnata da una giustificazione che spiega le ragioni per cui l'accesso è necessario.
- Valutazione della richiesta: il responsabile dell'IT o il gestore della sicurezza informatica valuta la richiesta di accesso in accordo con la direzione, in base al ruolo dell'utente, alle attività svolte e alle risorse a cui l'utente ha già accesso approva o diniega la richiesta.
- Creazione di un account: se l'accesso è stato approvato, il responsabile dell'IT o il gestore della sicurezza informatica crea un account per l'utente, definendo i permessi di accesso in base al ruolo assegnato. La consegna avviene tramite un modulo, sottoscritto, nella quale l'operatore viene contestualmente informato sulle modalità e sui rischi di utilizzo delle stesse.
- Revoca degli accessi: quando un dipendente cambia ruolo o lascia l'azienda, il responsabile dell'IT o il gestore della sicurezza informatica revoca gli accessi ai sistemi informatici e alle risorse aziendali relativi al vecchio ruolo dell'utente.

#### 5. Procedure di controllo degli accessi e loro tracciabilità

La Casa di Cura Villa Esther adotta una serie di misure specifiche per garantire che l'accesso ai sistemi informatici e alle risorse aziendali affinché questo sia limitato ai soli utenti autorizzati e che ogni accesso sia tracciato e monitorato.

La procedura di controllo degli accessi e tracciabilità include i seguenti passaggi:

- Identificazione dell'utente: ogni utente che accede ai sistemi informatici e alle risorse aziendali è identificato attraverso un account utente univoco, che

richiede l'autenticazione dell'utente (ad esempio, tramite nome utente e password).

- Autorizzazione dell'accesso: ogni utente ha accesso solo alle risorse informatiche necessarie per svolgere le proprie attività, in base al ruolo assegnato.
- Controllo degli accessi: è prevista la registrazione degli accessi, con il monitoraggio di ogni attività svolta dall'utente e il rilevamento di eventuali accessi non autorizzati o attività sospette.
- Tracciabilità: sono registrati e conservati nei log degli accessi e le attività svolte dagli utenti, in modo da garantire la tracciabilità di ogni attività eseguita sui sistemi informatici e sulle risorse aziendali.
- Revisione dei log: i log degli accessi e delle attività svolte dagli utenti sono regolarmente monitorati e revisionati, al fine di individuare eventuali anomalie o attività sospette.

La procedura di controllo degli accessi e loro tracciabilità sono parte integrante della politica di sicurezza informatica dell'azienda, condivisa con tutti i dipendenti e regolarmente aggiornata per rispondere alle evoluzioni del rischio e delle minacce.

6. Misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse.

Le aree di accesso sono chiuse a chiave.

7. Procedure per la gestione e manutenzione dei sistemi utilizzati presso la Società; procedure per i controlli sulla rete aziendale e sulle informazioni che vi transitano, sull'instradamento (*routing*) della rete (funzionale ad assicurare che non vengano violate le politiche di sicurezza), sull'installazione di software sui sistemi operativi;

Villa Esther adotta e utilizza specifiche procedure per il controllo della rete aziendale e delle informazioni che vi transitano al fine di garantire la sicurezza delle informazioni aziendali e la corretta gestione dei dati. Alcune delle metodologie che sono adottate includono:

- Monitoraggio della rete: per garantire la sicurezza della rete aziendale, sono in uso strumenti di monitoraggio della rete che consentano di individuare eventuali anomalie o traffico sospetto. I principali strumenti in uso sono: firewall, intrusion detection system (IDS) o intrusion prevention system (IPS), software anti-virus e anti-malware.
- Controllo dell'accesso alla rete: per limitare l'accesso alla rete aziendale solo agli utenti autorizzati, esistono misure di autenticazione forte e l'utilizzo di password robuste. Inoltre, per l'accesso remoto a società ed utenti, che per il loro ruolo debbano accedere ai sistemi aziendali dall'esterno, sono utilizzate

Virtual Private Network (VPN), che consentono di stabilire una connessione sicura e crittografata tra la rete aziendale e le postazioni remote.

- Installazione di software sui sistemi operativi: per garantire la sicurezza dei sistemi informatici aziendali, è vietata l'installazione di software al di fuori di quelli autorizzati dall'amministratore di sistema. Solo il reparto IT ha le chiavi di accesso necessarie per l'installazione di ulteriori software che devono essere comunque autorizzati dalla direzione.
- Controllo del traffico di rete: per sostenere la sicurezza delle informazioni che transitano sulla rete aziendale, la politica di controllo del traffico di rete prevede l'uso di protocolli di crittografia per proteggere le comunicazioni tra i sistemi, come SSL o TLS.
- Aggiornamenti di sicurezza: per mantenere la sicurezza della rete aziendale, sono adottate misure per garantire l'aggiornamento regolare di tutti i software e le applicazioni installate sui sistemi operativi. Gli aggiornamenti di sicurezza sono scaricati solo da fonti affidabili e installati solo dopo una rigorosa valutazione.
- Utilizzo di VLAN: le VLAN e il routing strutturato sono strumenti utili per garantire la sicurezza informatica all'interno dell'organizzazione. In azienda sono utilizzate per consentire una suddivisione della rete in segmenti logici separati, limitare l'accesso alle risorse solo a determinati utenti o gruppi, impedire l'accesso ai dispositivi non autorizzati o limitare l'accesso alla rete solo a determinati dispositivi

## SEZIONE II - REATI-PRESUPPOSTO, VALUTAZIONE DEI RISCHI E MISURE DI PREVENZIONE

### INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO, DI UN ENTE PUBBLICO O DELL'UNIONE EUROPEA O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE, FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO E FRODE NELLE PUBBLICHE FORNITURE

#### ART. 38 - REATI-PRESUPPOSTO DI CUI ALL'ART. 24 DEL DECRETO 231

I reati-presupposto di cui all'art. 24 del Decreto 231 sono:

- Malversazione di erogazioni pubbliche (art. 316 *bis* c.p.);
- indebita percezione di erogazioni pubbliche (art. 316 *ter* c.p.);
- truffa (art. 640, co. 2, n.1, c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.);
- frode informatica (art. 640 *ter* c.p.).

La descrizione dei reati elencati e l'indicazione delle sanzioni previste a carico della Società in caso di commissione di questi reati sono contenute nell'Allegato I al Modello.

#### ART. 39 - MISURE DI PREVENZIONE

I reati di cui all'art. 24 del Decreto 231 sono classificabili come **reati peculiari**.

I suddetti reati sono astrattamente suscettibili di verificarsi presso gli uffici incaricati di richiedere contributi e finanziamenti a soggetti pubblici (ad esempio, Unione Europea, Stato, Regioni, ASL), sia in relazione all'attività sanitaria tipica e principale (ad esempio budget; DRG) sia in relazione ad attività collaterali (ad esempio, ricerca e sviluppo; formazione del personale; consulenze specialistiche). A titolo esemplificativo, questi reati potrebbero tipicamente essere commessi attraverso una non corretta classificazione delle prestazioni sanitarie erogate a favore dei pazienti e rimborsate dal Servizio Sanitario Nazionale mediante indicazione, nelle cartelle cliniche, di un DRG (che costituisce l'elemento in relazione al quale le prestazioni erogate vengono pagate dal Servizio Sanitario Nazionale) non corrispondente alle prestazioni effettivamente erogate.

Le **aree/attività** rilevanti sono la Direzione Sanitaria, i Reparti, l'Ufficio Contabilità e l'Ufficio Acquisti.

Il **rischio** è **medio**.

Le **misure di prevenzione**:

è previsto l'obbligo dell'Amministratore Unico di osservare ogni più ampia diligenza professionale nell'adozione delle delibere di affidamento di deleghe a soggetti che possano, in forza dei poteri loro conferiti, correre il rischio di commissione di alcuno

dei suddetti reati, nonché nel verificare la legittimità e l'ampiezza di eventuali sub-deleghe.

L'Amministratore Unico ha inoltre la facoltà di acquisire le relazioni periodiche scritte, almeno annuali, da coloro che interagiscono con la Pubblica Amministrazione e altri pubblici e privati uffici. In particolare, queste relazioni devono specificare modi e tempi di eventuali richieste di finanziamenti; modi e tempi necessari al loro ottenimento; destinazione dei finanziamenti. In caso di operazioni straordinarie, le suddette relazioni sono redatte e fornite ad evento. Una volta acquisite le relazioni, l'Amministratore Unico effettuerà le proprie valutazioni e, se del caso, adotterà le misure conseguenti.

### **Protocollo per la richiesta di finanziamenti**

La Società applica il seguente protocollo per la disciplina del processo di formazione delle decisioni e delle responsabilità relative alle seguenti fasi:

- assunzione della decisione di formulare una richiesta di finanziamento: la decisione viene assunta dall'Amministratore Unico in base ai limiti di spesa;
- preparazione dei documenti e dei dati da presentare per la richiesta di finanziamenti: questa fase rientra nella competenza del personale impiegato presso l'Ufficio Contabilità;
- presentazione dei documenti e dei dati per la richiesta di finanziamenti, per finanziamenti tipo bonus sud, industria 4.0, beni materiali e immateriali, ci si avvale di consulenti esterni che istruiscono la pratica; quando necessario, la richiesta viene effettuata mediante accesso ad apposita piattaforma informatica; per finanziamenti di importi ordinari, questa fase rientra nella competenza del personale impiegato presso l'Ufficio Contabilità, sotto la supervisione dell'Amministratore Unico;
- monitoraggio della richiesta fino all'effettiva erogazione del finanziamento: questa fase rientra nella competenza del personale impiegato presso l'Ufficio Contabilità o dei consulenti esterni nei casi summenzionati, sotto la supervisione dell'Amministratore Unico;
- ricezione dei finanziamenti e loro corretta imputazione e utilizzo: la ricezione dei finanziamenti avviene sui conti correnti della Società; la responsabilità per la loro corretta imputazione è accentrata presso l'Amministratore Unico che ha accesso ai conti e ha il potere di effettuare i pagamenti conseguenti al corretto utilizzo dei finanziamenti ricevuti;
- adeguata e tempestiva rendicontazione all'ente finanziatore: questo obbligo di rendicontazione rientra nelle attribuzioni dell'Amministratore Unico, il quale deve adempiervi in forma scritta (anche via e-mail), e nelle forme stabilite dalla normativa di riferimento;
- tutta la documentazione relativa alle varie fasi sono verificate, a sua richiesta, dal Sindaco.

Tutti i soggetti dotati di poteri rilevanti con riguardo alle predette fasi sono tenuti a osservare le prescrizioni del protocollo.

È fatto obbligo a tutti coloro che, a qualunque titolo, svolgono la loro attività presso la Società e sono concretamente coinvolti nelle richieste di finanziamenti, di impegnarsi, nei limiti delle rispettive competenze, a operare affinché sia rispettato quanto previsto dalla normativa vigente in materia di finanziamento delle istituzioni sanitarie. A tal fine, questi soggetti sono tenuti anche a partecipare a ogni attività formativa in materia di gestione dei finanziamenti pubblici organizzata da, o per, la Società.

### **Procedura per la codificazione corretta delle prestazioni e gestione della cartella clinica.**

È fatto obbligo di rispettare le *“Linee guida sulla corretta gestione della cartella clinica”*. Inoltre, è vietato: erogare prestazioni non necessarie; fatturare prestazioni non effettivamente erogate; fatturare utilizzando un codice di DGR che prevede un livello di pagamento maggiore rispetto al codice di DRG corrispondente alla prestazione effettivamente erogata al paziente; duplicare la fatturazione per una medesima prestazione; effettuare ricoveri oltre la data in cui il budget è esaurito, salvo quelli necessari per adempiere agli obblighi di continuità assistenziale. In ogni caso, qualsiasi eventuale fatturazione per prestazioni eccedenti i limiti di cui al budget assegnato, all’esito dei controlli di appropriatezza, sarà oggetto di emissione di nota di credito in favore della P.A. Questi divieti devono essere osservati da coloro che sono impiegati o operano presso l’Ufficio Accettazione e Ricoveri e presso l’Ufficio Contabilità.

Al fine di evitare che nelle cartelle cliniche siano riportati codici di DRG che prevedono un livello di pagamento non corrispondente alle prestazioni effettivamente erogate ai pazienti, viene rispettata la seguente procedura: il medico del Reparto di volta in volta rilevante individua il corretto codice di DRG in base alla classificazione nazionale tempo per tempo vigente, la correttezza del codice di DRG viene controllata dal Direttore dell’Unità Operativa di volta in volta interessato nel momento in cui firma la cartella clinica, la correttezza del codice di DRG viene poi ulteriormente verificata dal Direttore Sanitario, che controfirma la cartella clinica, dopo la consegna della stessa cartella alla Direzione Sanitaria e prima che venga richiesto alla PA il pagamento della prestazione erogata.

In ogni caso, è fatto obbligo di coinvolgere il prima possibile il Direttore Sanitario nei casi in cui vi sia un dubbio da parte del medico del Reparto e/o del Direttore dell’Unità Operativa circa la classificazione di determinate prestazioni. Nel caso di persistente dubbio in merito all’esatta classificazione delle prestazioni effettuate, non risolvibile in base ad una ragionevole interpretazione della normativa vigente, il Direttore Sanitario richiede un parere alla Regione o alla ASL. Decorso 30 giorni dalla richiesta di parere senza che sia stata fornita risposta dagli enti pubblici coinvolti, il Direttore Sanitario provvede alla classificazione della prestazione effettuata in base a principi di buona fede e di ragionevole interpretazione della legge.

L’Ufficio Contabilità, che riceve la cartella clinica, deve quindi effettuare tutti i passaggi amministrativi – tra cui, fotocopia del frontespizio della cartella, inserimento

della fotocopia in un raccoglitore cartaceo, invio alla ASL di tutte le fotocopie delle fatture mensili - preordinati al suo pagamento da parte della PA, senza in alcun modo modificare o integrare il documento. L'Amministratore Unico (Il responsabile dell'Area Amministrativa) controlla a campione periodicamente il pieno rispetto della procedura descritta.

### **Procedura per evitare il rischio di frode informatica**

Coloro che sono incaricati di predisporre e inviare documenti e informazioni funzionali alla formulazione di richieste di finanziamenti o contributi a soggetti pubblici e che, nell'espletamento di questi compiti, hanno accesso alla rete informatica aziendale, nonché coloro che hanno accesso a reti informatiche di soggetti pubblici (ad esempio, per il caricamento di documenti su piattaforme informatiche messe a disposizione dalla Regione in relazione alla procedura di accreditamento) devono accedervi in conformità delle procedure *ad hoc* elaborate. Queste procedure prevedono l'uso di una doppia chiave asimmetrica, composta da una parte pubblica (c.d. *user ID*) e da una parte privata (c.d. *password*). Le persone interessate si impegnano a non comunicare a terzi la propria password e a farne un uso strettamente personale, essendo vietato che una medesima *password* venga utilizzata da più di una persona e, più in generale, a osservare la normativa in tema di protezione dei dati personali.

Con specifico riferimento alla richiesta di autorizzazioni e/o accreditamenti istituzionali in materia sanitaria (esercizio, realizzazione, trasferimento, rimodulazione di posti letto etc.), è fatto obbligo all'Amministratore Unico di far rispettare le linee guida regionali per l'accesso alle piattaforme informatiche eventualmente previste e, in ogni caso, le leggi e i regolamenti regionali che disciplinano la richiesta di autorizzazione e accreditamento. In particolare, la richiesta deve essere predisposta dall'Amministratore Unico con il coinvolgimento del Direttore Sanitario, del consulente legale e dell'ufficio tecnico. Deve essere garantita la separazione delle funzioni di redazione, approvazione e controllo.

**PECULATO, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ,  
CORRUZIONE E ABUSO D'UFFICIO**

**ART. 40 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25 DEL DECRETO 231**

I reati-presupposto di cui all'art. 25 del Decreto 231 sono:

- Peculato (art. 314, co. 1, c.p.);
- Peculato mediante profitto dell'errore altrui (art. 316 c.p.);
- Concussione (art. 317 c.p.);
- Corruzione per l'esercizio della funzione (art. 318 c.p.); Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.); Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.), ivi incluse le pene per il corruttore (art. 321 c.p.) e le circostanze aggravanti (art. 319 *bis* c.p.); Corruzione in atti giudiziari (art. 319 *ter* c.p.);
- Induzione indebita a dare o promettere utilità (art. 319 *quater* c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 *bis* c.p.);
- Abuso d'ufficio (art. 323 c.p.);
- Traffico di influenze illecite (art. 346 *bis* c.p.).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

**ART. 41 - MISURE DI PREVENZIONE**

I reati di cui all'art. 25 del Decreto 231 sono classificabili come **reati peculiari**.

I suddetti reati sono astrattamente suscettibili di verificarsi in relazione alle attività svolte dai soggetti apicali e dai loro delegati nonché da soggetti loro sottoposti, i quali potrebbero commettere atti di corruzione nell'interesse della Società, promettendo o offrendo denaro o altra utilità a pubblici ufficiali o incaricati di pubblico servizio, che siano dotati del potere di assumere decisioni o di svolgere attività rilevanti per la Società. Vengono in considerazione al riguardo, a titolo esemplificativo, le seguenti attività: autorizzazioni e accreditamento, accordi contrattuali, concessione di finanziamenti, verifiche, controlli e ispezioni.

Le **aree** rilevanti sono quelle presso le quali operano coloro che hanno la materiale possibilità di avere un contatto diretto con soggetti pubblici, vale a dire l'Amministratore, il Direttore Sanitario, l'Ufficio Contabilità, l'Ufficio Personale, l'Ufficio Acquisti nonché eventuali consulenti esterni incaricati di rappresentare la Società presso enti pubblici ovvero presso l'associazione di categoria e che, tramite quest'ultima, possono avere contatti diretti con soggetti pubblici.

**Il rischio è medio.**

**Le misure di prevenzione:**

è fatto obbligo a tutti i soggetti che operano presso la Società o per conto di essa di conformare la propria condotta ai principi di probità, correttezza e trasparenza nonché di osservare, in ogni rapporto con la Pubblica Amministrazione, le leggi, i regolamenti e ogni altra normativa, tra cui la legge n. 190/2012.

L'Amministratore, cui competono anche funzioni correlate alla movimentazione dei conti della Società, è tenuto ad adempiere ogni obbligo di legge in tema di tracciabilità dei flussi finanziari aziendali, in quanto unico soggetto autorizzato all'accesso alle risorse finanziarie e ai conti correnti (e/o a eventuali conti titoli) intestati alla Società, avendo delega esclusiva a operare su questi conti, fatta salva la facoltà di sub-delega a un soggetto individuato di volta in volta.

I soggetti sopra indicati devono altresì rispettare le norme di seguito formulate:

- l'Amministratore o le persone formalmente da questi delegate sono gli unici soggetti deputati a curare i rapporti con i funzionari dell'assessorato regionale alla sanità e con quelli della ASL, con le autorità e i funzionari comunali, provinciali e delle altre istituzioni pubbliche nazionali o comunitarie, ovvero con enti privati con i quali la Società venga in rapporto;
- in deroga a quanto previsto al punto che precede, il Direttore Sanitario è l'unico soggetto deputato a curare i rapporti con soggetti pubblici nelle materie riservate dalla legge alla sua esclusiva competenza;
- il Direttore Sanitario e gli eventuali soggetti formalmente delegati dall'Amministratore devono informare quest'ultimo o altra persona da questi formalmente delegata, in modo tempestivo e puntuale, circa l'andamento e l'esito di ogni pratica in essere con i soggetti pubblici da essi rispettivamente curata;
- eventuali soggetti esterni formalmente incaricati dall'Amministratore a curare rapporti con enti pubblici devono, previa accettazione del Modello e di ogni norma o protocollo in esso contenuti o richiamati, riferire all'Amministratore, in modo tempestivo e puntuale, circa l'andamento e l'esito di ogni pratica in essere con i soggetti pubblici da questi curata.

È vietato promettere, offrire o consegnare denaro, doni o altre utilità, anche per interposta persona, a dipendenti della pubblica amministrazione, dello Stato o delle Comunità europee, di ogni qualifica o livello, al loro coniuge e ai di lui parenti, ovvero ai loro ascendenti, discendenti, fratelli, sorelle, zii, nipoti, salvo che il fatto accada in occasione di festività in cui sia tradizione lo scambio di doni o, comunque, questi siano di tenue valore, in linea con quanto previsto dal codice di comportamento dei dipendenti pubblici di cui al decreto del Presidente della Repubblica n. 62/2013.

È vietato:

- a tutti coloro che svolgono la propria attività presso, o per, la Società ricevere danaro, doni o qualsiasi utilità, o accettarne la promessa, da chiunque sia, o intenda entrare, in rapporto con la stessa Società e voglia conseguire indebitamente un trattamento in violazione della normativa di legge;

- a chi agisce per conto della Società, nei rapporti con funzionari dell'assessorato regionale alla sanità, della ASL ovvero di qualsiasi altra pubblica amministrazione, dello Stato o delle Comunità europee, di determinarne le decisioni con violenza, minaccia o inganno;
- assumere alle dipendenze della Società ex impiegati della pubblica amministrazione, dello Stato o delle Comunità europee, nei tre anni successivi al compimento di un atto, di competenza di uno dei predetti soggetti ed espressione del suo potere discrezionale, da cui sia derivato un vantaggio per l'Istituzione sanitaria. Lo stesso divieto è previsto per i casi di omissione o ritardo di un atto svantaggioso per la Società;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- favorire, nei processi d'acquisto, fornitori eventualmente indicati da pubblici ufficiali o da incaricati di pubblico servizio in cambio di vantaggi per la Società;
- promettere o fornire a pubblici ufficiali o incaricati di pubblico servizio o ai loro parenti ed affini servizi di utilità personale.

**FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO; DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO**

**ART. 42 - REATI-PRESUPPOSTO DI CUI AGLI ARTT. 25-BIS E 25-BIS.1 DEL DECRETO 231**

I reati-presupposto previsti dagli artt. 25-bis e 25-bis.1 del Decreto 231 sono:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.);
- Contraffazione, alterazione o uso di marchio segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);

- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.);
- Turbata libertà dell'industria e del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

#### **ART. 43 - MISURE DI PREVENZIONE**

I reati di cui all'art. 25-*bis* e 25-*bis*.1 del Decreto 231 sono classificabili come **reati comuni**.

Le **aree** maggiormente coinvolte sono quelle incaricate della gestione della contabilità. Nello specifico: l'Amministratore unico, l'Ufficio Accettazione e Ricoveri, l'Ufficio Contabilità e l'Ufficio Acquisti in relazione ai pagamenti effettuati e agli incassi ricevuti da questi uffici.

Il **rischio** è basso.

Le **misure di prevenzione**:

l'Amministratore deve osservare ogni più ampia diligenza nell'adozione delle decisioni e nell'affidamento di deleghe a soggetti che possano, in forza dei poteri loro conferiti, correre il rischio di commissione di alcuno dei suddetti reati e deve controllarne l'operato mediante l'attenta analisi delle relazioni predisposte da questi soggetti, a rendiconto delle attività loro affidate in delega.

È prevista la seguente procedura per l'effettuazione dei pagamenti:

- le operazioni di pagamento vengono effettuate dall'Ufficio Contabilità, che riceve le fatture da pagare o i preavvisi di pagamento da parte dell'Ufficio Acquisti;
- l'Ufficio Contabilità confronta la somma indicata nella fattura o nel preavviso di pagamento con la documentazione che ne legittima la corresponsione (ad esempio, contratto di fornitura), per verificarne la congruità;
- una volta compiuta la suddetta verifica, l'Ufficio Contabilità sottopone i pagamenti all'attenzione dell'Amministratore, che conferisce l'autorizzazione al pagamento;
- ottenuta l'autorizzazione, l'Ufficio Contabilità predispone la lista dei pagamenti da effettuare, tenendo conto del relativo ordine di priorità;

- il pagamento viene effettuato prevalentemente mediante bonifico bancario, utilizzando i codici del dispositivo (chiavetta) per l'operatività on-line, che sono affidati al, e custoditi dall'Amministratore;
- eventuali pagamenti allo sportello devono sempre essere effettuati direttamente dall'Amministratore o da altro dipendente, sulla base di formale delega dell'Amministratore.

È prevista la seguente procedura per gli incassi:

le entrate avvengono mediante bonifici bancari o con strumenti tracciabili bancari (assegni) visionati e controllati dall'Amministratore. I pagamenti ricevuti direttamente dall'Ufficio Accettazione e Ricoveri sono eseguiti mediante pos (bancomat o carta di credito) o in contanti. In quest'ultimo caso, gli addetti all'Ufficio Accettazione e Ricoveri effettuano controlli con appositi lettori di banconote e monete.

#### **ART. 44 - DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI**

I reati-presupposto di cui all'art. 25-*octies* 1 del Decreto 231 sono:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (493 *ter* c.p.);
- detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (493 *quater* c.p.);
- frode informatica (640 *ter* c.p.).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

In ordine al rischio, alle aree/attività sensibili e alle misure di prevenzione si richiama quanto previsto per i reati di cui agli artt. 25-*bis* e 25-*bis*.1 del Decreto 231, sopra indicati.

## REATI SOCIETARI

### ART. 45 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-TER DEL DECRETO 231

I reati-presupposto previsti dall'art. 25-ter del Decreto 231 sono:

- False comunicazioni sociali (art. 2621 c.c.);
  - Fatti di lieve entità (art. 2621 *bis* c.c.);
  - False comunicazioni sociali delle società quotate (art. 2622 c.c.);
  - Falso in prospetto (2623 c.c.);
  - Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.);
  - Impedito controllo (art. 2625 c.c.);
  - Indebita restituzione dei conferimenti (art. 2626 c.c.);
  - Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
  - Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
  - Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
  - Omessa comunicazione del conflitto di interessi (2629 *bis* c.c.);
  - Formazione fittizia del capitale (art. 2632 c.c.);
  - Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
  - Corruzione tra privati (art. 2635 c.c.);
  - Istigazione alla corruzione tra privati (art. 2635 *bis* c.c.);
  - Illecita influenza sull'assemblea (art. 2636 c.c.);
  - Aggiotaggio (art. 2637 c.c.);
  - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).
- Il DECRETO LEGISLATIVO 2 marzo 2023, n. 19 (in G.U. 07/03/2023, n.56) ha disposto la modifica dell'art.25 ter comma 1; la modifica dell'art. 25 ter comma 1 lettera s-bis; l'introduzione della lettera s ter all'art.25 ter comma 1.

Per il delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della direttiva UE 2019/2121 del Parlamento europeo e del Consiglio del 27 novembre 2019, la sanzione pecuniaria è da centocinquanta a trecento quote.

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 46 - MISURE DI PREVENZIONE

I reati di cui all'art. 25-ter del Decreto 231 sono classificabili come **reati tipici**.

Le **aree/attività** rilevanti sono l'Amministratore, il Sindaco e l'Ufficio Contabilità.

Il **rischio** è **medio**.

Le  **misure di prevenzione**:

è fatto obbligo ai soggetti sopra individuati e a coloro che siano comunque coinvolti nelle attività di formazione del bilancio o di altri documenti similari di osservare rigorosamente i principi etici volti ad assicurare massima collaborazione; completezza e chiarezza delle informazioni fornite; accuratezza dei dati e delle elaborazioni; tempestiva segnalazione di eventuali conflitti di interesse. Il rispetto dei principi etici è altresì specificamente funzionale a evitare che sia integrato il reato di corruzione tra privati o di istigazione alla corruzione tra privati.

Posto che il bilancio della Società è assoggettato a revisione e certificazione, prima che l'Amministratore approvi il bilancio viene a questi consegnata una bozza del bilancio stesso e viene effettuata una riunione tra Amministratore, Sindaco e Revisore avente ad oggetto tale documento, di tale riunione viene redatto verbale.

Sono previste: attività di formazione di base verso tutti coloro che intervengano nella formazione di documenti funzionali alla redazione del bilancio affinché conoscano almeno le principali nozioni sul bilancio (norme di legge, sanzioni, principi contabili) nonché i dati e le notizie che devono essere forniti all'Area Amministrativa; programmi di informazione/formazione periodica dell'Amministratore, del management e dei dipendenti sulla normativa in tema di *corporate governance* e sui reati/illeciti amministrativi in materia societaria; obblighi di identificazione delle principali fattispecie di interessi dell'Amministratore e le procedure autorizzative per operazioni esposte a situazioni di conflitto di interesse; la disciplina delle operazioni di riduzione del capitale sociale, fusione e scissione.

Al fine di evitare la commissione dei reati societari non strettamente correlati alla predisposizione e alla formazione del bilancio, sono effettuate, periodicamente, riunioni del Sindaco finalizzate a verificare l'osservanza della normativa in tema di società, nonché il rispetto dei comportamenti conseguenti da parte degli amministratori, del management e dei dipendenti.

È previsto che, in relazione alla negoziazione e stipulazione di contratti attivi (ossia contratti che generino un ricavo per la Società): è obbligatorio seguire l'*iter* di definizione e attuazione delle politiche commerciali preventivamente individuato dall'Amministratore, in base al quale i parametri utilizzati per la determinazione del prezzo sono quelli usualmente praticati nel mercato, tenuto conto dell'oggetto del contratto; ogni contratto include previsioni standardizzate in relazione alla sua natura e tipologia, ivi incluse previsioni finalizzate all'osservanza di principi di controllo/regole etiche nella gestione delle attività da parte del terzo, e meccanismi rimediali (principalmente, di assegnazione di termini per l'adeguamento; risoluzione del contratto o recesso) in caso di eventuali scostamenti.

È fatto obbligo ai soggetti che a qualunque titolo intervengano nella gestione dei rapporti con professionisti e soggetti appartenenti a società terze che svolgano attività professionali e/o di impresa dal cui svolgimento o mancato svolgimento possa derivare un vantaggio per la Società o per le quali la stessa possa avere un interesse, di segnalare tempestivamente all'Amministratore Unico e all'OdV ogni richiesta di denaro o regalia non giustificata dai normali rapporti con questi soggetti nonché di conferire incarichi o consulenze a soggetti terzi, nel rispetto dei criteri di legalità, trasparenza, condivisione funzionale, inerenza e giustificabilità. Restano ferme le procedure per il controllo dei flussi finanziari e la tracciabilità dei pagamenti.

Qualunque operazione deve essere comunque preceduta da un'attenta verifica in ordine alla consistenza dello stato patrimoniale della Società e, in caso di operazioni di maggiore rilevanza (vale a dire, che comportino per la Società un esborso pari o superiore a 1 milione di euro), dal previo parere del Sindaco.

Sono osservati appositi protocolli riguardanti la gestione dei rapporti con i soci, il sindaco, il revisore, la convocazione, lo svolgimento e la verbalizzazione delle assemblee; la gestione dei conferimenti, degli utili e delle riserve, delle operazioni sulle partecipazioni e sul capitale; la gestione delle operazioni straordinarie e di quelle di acquisto/vendita di strumenti finanziari; la gestione delle comunicazioni nei confronti di enti pubblici.

## REATI TRIBUTARI

### ART. 47 – REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUINQUESDECIES DEL DECRETO 231

I reati di cui all'art. 25-*quinquiesdecies* sono:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 c. 1 e 2 *bis*, d. lgs. n. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (art. 3, d. lgs. n. 74/2000);
- dichiarazione infedele (art. 4, d. lgs. n. 74/2000);
- omessa dichiarazione (art. 5, d. lgs. n. 74/2000);
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8 c. 1 e 2 *bis*, d. lgs. n. 74/2000);
- occultamento o distruzione di documenti contabili (art. 10, d. lgs. n. 74/2000);
- indebita compensazione (art. 10 *quater*, d. lgs. n. 74/2000);
- sottrazione fraudolenta al pagamento di imposte (art. 11, d. lgs. n. 74/2000);

La descrizione di questi reati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 48 – MISURE DI PREVENZIONE

I reati di cui all'art. 25-*quinquiesdecies* del Decreto 231 sono classificabili come reati comuni.

Le **aree/attività** potenzialmente a rischio sono: attività di approvvigionamento di beni e servizi; aree/uffici abilitati ad acquistare beni e servizi da cui potrebbero trarre origine fatture false attive e passive; complesso di attività dichiarative volte alla

determinazione dei tributi; redazione del bilancio e dei documenti fiscali; (Ufficio acquisti, Ufficio contabilità).

**Il rischio è medio.**

**Le misure di prevenzione:**

formazione del personale apicale con riferimento all'analisi dei rischi correlati ai reati tributari;

adozione di un sistema amministrativo-contabile adeguato che preveda l'implementazione di un sistema di corretta tenuta della documentazione contabile affiancato da un sistema gestionale altrettanto efficace;

separazione delle fasi di approvvigionamento, affido delle stesse a responsabili differenti e relativi meccanismi di monitoraggio costante di professionalità e correttezza degli incaricati;

gestione del rapporto con clienti e fornitori con particolare riferimento al processo di selezione e identificazione dei partner commerciali con verifiche periodiche a campione sulla reale consistenza ed affidabilità degli stessi (ad es. mirate visure camerali);

riscontro periodico a campione svolto da funzioni di controllo interne su servizi acquistati così come previsti da fatture o altri documenti contabili;

monitoraggio dei prezzi di vendita e di acquisto;

ad ogni bolla di consegna deve corrispondere una effettiva uscita di merce o erogazione del servizio; la fattura deve evidenziare esattamente le quantità uscite o i servizi resi;

conservazione della documentazione a supporto delle operazioni economico-finanziarie;

definizione delle modalità di verifica della coerenza tra il soggetto che ha erogato la prestazione, il soggetto indicato nell'ordine/contratto ed il soggetto che ha emesso la fattura;

definizione delle modalità di verifica dei termini e delle condizioni contrattuali in relazione alle modalità di pagamento;

interlocuzione corretta e trasparente con l'Agenzia delle Entrate.

È, altresì, vietato:

utilizzare strumenti anonimi di pagamento per il compimento di operazioni di trasferimento di importi rilevanti;

effettuare qualunque tipo di pagamento nell'interesse della Società in mancanza di adeguata documentazione di supporto;

indicare elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture per operazioni inesistenti. A tal fine all'OdV viene garantito libero accesso a tutta la documentazione contabile e fiscale.

## DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

### ART. 49 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUATER DEL DECRETO 231

I delitti di cui all'art. 25-*quater* del Decreto 231 sono:

- Associazioni sovversive (art. 270 c.p.);
- Associazione con finalità di terrorismo anche internazionale o di everzione dell'ordine democratico (art. 270 *bis* c.p.);
- Assistenza agli associati (art. 270 *ter* c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 *quater* c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 *quinqüies* c.p.);
- Condotte con finalità di terrorismo (art. 270 *sexies* c.p.);
- Attentato per finalità terroristiche o di everzione (art. 280 c.p.);
- Atti di terrorismo con ordigni micidiali o esplosivi (art. 280 *bis* c.p.);
- Sequestro di persona a scopo di terrorismo o di everzione (art. 289 *bis* c.p.);
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.);
- Cospirazione politica mediante accordo (art. 304 c.p.);
- Cospirazione politica mediante associazione (art. 305 c.p.);
- Banda armata: formazione e partecipazione (art. 306 c.p.);
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.);
- Impossessamento, dirottamento e distruzione di un aereo (art. 1, l. 342/1976);
- Danneggiamento delle installazioni a terra (art. 2, l. 342/1976);
- Sanzioni (art. 3, l. 422/1989);
- Convenzione di New York 9 dicembre 1999 (art. 2).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 50 - MISURE DI PREVENZIONE

I reati di cui all'art. 25-*quater* del Decreto 231 sono classificabili come reati atipici.

Il **rischio** è **molto basso**.

Le **aree/attività** rilevanti sono l'Ufficio Personale e l'Ufficio Accettazione e Ricoveri.

Le  **misure di prevenzione**:

è previsto che l'Ufficio Accettazione e Ricoveri effettui una scrupolosa verifica dei documenti di identità dei pazienti; l'Ufficio Personale provvede all'invio giornaliero, alla questura, dell'elenco dei pazienti alloggiati presso la Casa di Cura.

L'Ufficio Personale pone particolare attenzione al rispetto di tutte le procedure connesse alle assunzioni dei dipendenti e al possesso in capo a costoro dei requisiti richiesti dalla normativa e dal CCNL vigenti per i dipendenti delle istituzioni sanitarie private.

L'Amministratore verifica a campione le attività di identificazione e controllo svolte dall'Ufficio Personale e dall'Ufficio Accettazione e Ricoveri.

È fatto obbligo a tutti coloro che operano presso la Società di rispettare le disposizioni in tema di correttezza e legalità dei comportamenti previste dal Codice Etico.

## DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE

### ART. 51 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUINQUIES DEL DECRETO 231

I delitti di cui all'art. 25-*quinquies* del Decreto 231 sono:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600 *bis* c.p.);
- Pornografia minorile (art. 600 *ter* c.p.);
- Detenzione di materiale pornografico (art. 600 *quater* c.p.);
- Pornografia virtuale (art. 600 *quater-1* c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 *quinquies* c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603 *bis* c.p.);
- Adescamento di minorenni (art. 609 *undecies* c.p.).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 52 - MISURE DI PREVENZIONE

I reati di cui all'art. 25-*quinquies* del Decreto 231 sono classificabili come **reati atipici**.

Il **rischio** è **basso**.

Le **attività** ritenute a rischio sono: accesso a siti e/o ricezione di materiale relativo alla pornografia minorile; assunzione del personale. Le aree maggiormente coinvolte sono l'area amministrativa, l'Ufficio Personale, la Direzione Sanitaria.

Le  **misure di prevenzione**:

è fatto obbligo a tutti coloro che operano per la Società di rispettare le disposizioni del Codice Etico che impongono uno specifico divieto in tema di pornografia minorile nonché l'impegno a rispettare, e a far rispettare ai propri fornitori, la normativa vigente

in materia di lavoro, con particolare attenzione al lavoro minorile e al tema della salute e della sicurezza.

Con riferimento agli strumenti informatici a disposizione di dipendenti e collaboratori, saranno installati blocchi non violabili dai singoli utenti, che impediscono l'accesso e/o la ricezione di materiale relativo alla pornografia minorile. Il Codice Etico contiene altresì richiami netti e inequivocabili a un corretto utilizzo degli strumenti informatici a disposizione dei dipendenti.

La Società non organizza direttamente, né consente ai propri dipendenti e collaboratori, la partecipazione a viaggi o periodi di permanenza in località estere con specifico riguardo a località note per il fenomeno del c.d. "turismo sessuale".

Particolare attenzione viene dedicata al rispetto di tutte le procedure connesse alla selezione e assunzione dei dipendenti, nonché al possesso in capo a costoro dei requisiti richiesti dalla normativa e dal CCNL vigenti.

Nell'ambito dei contratti stipulati con terzi fornitori sono inserite specifiche clausole che prevedono l'impegno di questi ultimi di rispettare gli obblighi di legge in tema di: tutela del lavoro minorile e delle donne, rispetto dei divieti in materia di intermediazione sul lavoro e sfruttamento illecito; condizioni igienico-sanitarie e di sicurezza; diritti sindacali o di associazione e rappresentanza nonché di fornire alla Società ogni documentazione utile a comprovare l'effettivo rispetto di questi obblighi; nei medesimi contratti è altresì previsto, in caso di eventuali violazioni, la risoluzione espressa del contratto stipulato.

## ABUSI DI MERCATO

### ART. 53 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-SEXIES DEL DECRETO 231

I delitti previsti dall'art. 25-*sexies* del Decreto 231 sono:

- Abuso di informazioni privilegiate (art. 184 TUF);
- Abuso di informazioni privilegiate (art. 187 *bis* TUF);
- Manipolazione del mercato (art. 185 TUF);
- Manipolazione del mercato (art. 187-*ter* TUF).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 54 - MISURE DI PREVENZIONE

I reati di cui all'art. 25-*sexies* del Decreto 231 sono classificabili come **reati atipici**.

Il **rischio** è **molto basso**.

Le **aree** coinvolte sono gli Uffici amministrativi.

Le **misure di prevenzione**:

è fatto obbligo a tutti coloro che operano presso la Società di rispettare le disposizioni del Codice Etico che impongono uno specifico divieto di commissione dei reati in questione.

## PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI

### ART. 55 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-QUATER.1 DEL DECRETO 231

Il reato di cui all'art. 25-*quater*.1 del Decreto 231 è quello di pratiche di mutilazione degli organi genitali femminili (art. 583 *bis* c.p.).

La descrizione di questo reato e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 56 - MISURE DI PREVENZIONE

Il reato di cui all'art. 25-*quater*.1 del Decreto 231 è classificabile come **reato atipico**.

Il **rischio** è **basso**.

Le **aree/attività** coinvolte sono quella sanitaria strettamente intesa, svolta da medici e paramedici.

Le **misure di prevenzione**:

il Direttore Sanitario è tenuto a illustrare al personale medico e parasanitario le caratteristiche tecniche della pratica di mutilazione degli organi genitali femminili, allo scopo di assicurare la più ampia possibilità che vengano a lui segnalate eventuali violazioni al divieto di queste pratiche. Inoltre, il personale adibito all'accettazione dei pazienti deve segnalare al Direttore Sanitario l'effettuazione di qualunque prestazione chirurgica, anche ambulatoriale, su donne o bambine di etnie a rischio. In questo caso, il Direttore Sanitario, con la collaborazione del Direttore dell'Unità Operativa di Chirurgia è tenuto a controllare la diagnosi di entrata della paziente e la coerenza della terapia praticata, al fine di poter dimostrare che la pratica di mutilazione vietata non sussiste o, comunque, non è avvenuta presso la Casa di Cura.

È vietato adibire la Casa di Cura allo svolgimento di qualunque attività che si traduca in pratiche di mutilazione degli organi genitali femminili. Di questo divieto è data massima pubblicità nella struttura e specifica menzione nel Codice Etico.

## OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

### ART. 57 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-SEPTIES DEL DECRETO 231

I delitti di cui all'art. 25-*septies* del Decreto 231 sono:

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590 c.p.);

commessi con violazione delle norme a tutela della salute e della sicurezza sul lavoro.

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 58 - MISURE DI PREVENZIONE

I reati di cui all'art. 25-*septies* del Decreto 231 sono classificabili come **reati comuni**.

Il sistema di gestione per la sicurezza e salute sul luogo di lavoro, definito ai sensi dell'art. 30 del D.lgs. n.81/2008 e del D.M. 13/02/2014, fornisce la base per l'elaborazione del presente modello organizzativo di prevenzione dei rischi reato di omicidio colposo e di lesioni gravi e gravissime commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Le **attività** sensibili sono:

Attività a rischio di infortunio e malattia professionale: per essa si fa riferimento al Documento di Valutazione dei rischi aziendali di cui all'art. 28 d. lgs 81/2008, redatto dal Datore di lavoro;

Attività a rischio reato: individuazione delle disposizioni normative applicabili, cui uniformarsi per il rispetto degli standard tecnico-strutturali; definizione delle risorse, dei ruoli e delle responsabilità per assicurare le attività finalizzate all'attuazione delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori; gestione delle emergenze, delle attività di prevenzione degli incendi e di primo soccorso; gestione degli appalti; attività di sorveglianza sanitaria; competenza, informazione e formazione del personale; controlli sugli acquisti; attività manutentive finalizzate al rispetto degli standard tecnici e di salute e sicurezza applicabili; gestione della documentazione e dei sistemi di registrazione al fine di garantire la tracciabilità delle attività.

Le **aree coinvolte** sono: Direzione Sanitaria, Amministratore unico, RSPP, Medico competente.

Il **rischio** è **medio**.

Le **misure di prevenzione**:

tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi ai principi contenuti nel Codice etico della società, nella normativa antinfortunistica e nelle specifiche misure di prevenzione stesse. Pertanto, costituiscono presupposto e parte integrante del Modello i principi di comportamento stabiliti nel Codice etico, la

documentazione relativa alla tutela e alla sicurezza dei luoghi di lavoro, quali il Documento di valutazione dei rischi e le procedure di gestione delle emergenze;

costituisce fondamentale protocollo di prevenzione generale il fatto che, per nessuna ragione, esigenze di celerità e di ottimizzazione della produzione possano condurre a violare le norme in materia antinfortunistica, comprese le attività di formazione del personale;

sono adottati atti formali per la nomina di un RSPP e per conferire a tutti i soggetti, a vario titolo coinvolti nella sicurezza, deleghe precise che dettaglino i rispettivi ruoli e responsabilità;

l'RSPP, il datore di lavoro, i rappresentanti per i lavoratori e il medico competente sono tenuti a rispettare tutti gli obblighi di cui al d.lgs. 81/2008 in materia di sicurezza sul lavoro.

L'RSPP, in attuazione del d.lgs. 81/2008, si occupa, in particolare, di:

- assicurare l'efficace funzionamento del sistema prevenzionistico aziendale, anche avvalendosi delle competenze specialistiche presenti in azienda, quali il Direttore Sanitario e il Medico Competente nonché di consulenti esterni, come esperti chimico-biologici, ingegneri per acustica, esperti per radiologia, società specializzate per la prevenzione del rischio incendi, esperti per il piano di emergenza;
- preparare e aggiornare l'analisi dei rischi e realizzare le misure correttive e preventive approvate;
- gestire le emergenze;
- informare e formare i lavoratori in materia di sicurezza;
- assicurare l'utilizzo in sicurezza di tutti gli impianti accessori alle attività di ricovero e ambulatoriali;
- assicurare l'utilizzo in sicurezza delle apparecchiature biomediche; attività svolta in condivisione con il primario di reparto;
- assicurare la sicurezza anti-incendio;
- verificare che i lavoratori rispettino gli obblighi ad essi imposti dall'art. 20 del d.lgs. n. 81/2008;
- attuare e assicurare il funzionamento del DVR. L'aggiornamento del DVR avviene ogni qualvolta intervengano modifiche organizzative rilevanti per la sicurezza e la salute dei lavoratori. L'approccio metodologico per la formazione del DVR è specificato all'interno del medesimo documento. Questa attività è svolta dall'RSPP con eventuali consulenti esterni; essa è altresì controllata dal Rappresentante dei Lavoratori per la Sicurezza e dal Medico Competente e approvata dal Datore di Lavoro.

Tutti i soggetti coinvolti nella prevenzione e protezione della sicurezza e della salute dei lavoratori e, quindi, l'RSPP, il Rappresentante dei Lavoratori per la Sicurezza, il Direttore Sanitario, il Medico Competente e il Datore di Lavoro devono relazionare all'OdV almeno una volta l'anno circa le attività svolte e, in ogni caso, comunicargli qualsiasi criticità rilevata nell'espletamento delle rispettive mansioni.

L'esercizio del controllo tecnico-operativo in materia di sicurezza rimane esclusivamente riservato all'RSPP, in quanto in possesso della competenza necessaria e della relativa responsabilità, mentre all'OdV compete il controllo sull'osservanza delle procedure e degli adempimenti indicati e richiamati nel Modello.

Il Datore di lavoro è tenuto a garantire periodicamente, e comunque sempre in occasione di modifiche normative, a tutti i soggetti destinatari di obblighi in materia di sicurezza, un'adeguata e specifica formazione, il cui espletamento deve essere documentato in forma scritta. La documentazione rilevante deve essere annualmente trasmessa all'OdV.

La Società ha implementato un sistema proattivo di gestione del rischio clinico. Ogni anno adotta il PARM (Piano Annuale di Rischio Clinico), strumento che descrive l'organizzazione e la strategia di gestione del rischio messa in atto dalla struttura. Più nello specifico la Casa di Cura definisce nel PARM lo scopo, i destinatari, gli obiettivi, le metodologie, gli indicatori che intendere adottare per la gestione del rischio in ottemperanza agli indirizzi strategici di rischio clinico indicati dalla Regione e in risposta a precisi obblighi formativi. Tale strumento privilegia la prevenzione, la comunicazione, la formazione e l'aggiornamento. L'ottica è quella di diminuire le potenzialità di errore attivo nella struttura nonché di contenere le richieste di risarcimenti danni. La Direzione Sanitaria garantisce la diffusione del PARM a tutto il personale sanitario e di supporto. Come da Legge 24/2017 sulla responsabilità professionale e la sicurezza delle cure, la Casa di Cura provvede a pubblicare sul sito web della struttura sanitaria la relazione annuale sugli eventi avversi verificatisi, sulle cause che hanno prodotto ogni evento avverso e sulle conseguenti iniziative messe in atto.

È fatto obbligo di curare l'aggiornamento del **Documento di Valutazione del Rischio Biologico** (ai sensi del titolo X del D.lgs. n.81/08).

La Casa di Cura Villa Esther ha posto in essere tutte le misure necessarie per contrastare la diffusione del virus **Covid-19**. Infatti:

-in data 20 marzo 2020 è stato istituito il Comitato per l'applicazione e la verifica delle regole del protocollo di regolamentazione come indicato dal Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro del 14 marzo 2020. Il comitato si riunisce a seconda delle necessità e vengono elaborati dei verbali.

- I dipendenti, su indicazione del medico competente, sono sottoposti al test sierologico rapido (come da verbale n. 2 del comitato del 17 aprile 2020).

- È presente una "Procedura Operativa per la gestione del caso sospetto" aggiornata il 29 maggio 2020. Tale procedura è redatta dal Direttore Sanitario con il supporto del Risk Manager.

- Sono diffuse le regole comportamentali dettate dall'ISS.

- Sono utilizzati DPI appropriati come indicati da tabella del Dvr-Rischio Covid.

- Sono presenti postazioni per la sanificazione delle mani con gel sanificante in punti strategici.

- Chiunque entri in struttura è sottoposto a triage (viene rilevata la temperatura corporea e link epidemiologico). L'utente che non soddisfa tali requisiti non accede in struttura ed è invitato a contattare il proprio medico.

-Sono state adottate le misure previste dal Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro del 24 aprile 2020.

-Tutto il personale dipendente e i collaboratori della Casa di cura svolgono formazione continua anche in modalità Fad. La formazione è verbalizzata su modulistica dedicata.

A seguito dell'Ordinanza del Presidente della Giunta Regionale n. 30 del 15.05.2020 – *Ulteriori misure per la prevenzione e gestione dell'emergenza epidemiologica da Covid-19, ordinanza ai sensi dell'art. 3, co. 2, d.l. n. 19/2020, Regione Molise - Indicazioni Regionali per la riattivazione dell'assistenza sanitaria per la "fase 2"*.

Il datore di lavoro ha redatto, come richiesto dall'ordinanza, un Piano Aziendale in cui sono illustrate le misure adottate dalla struttura per contrastare la diffusione Covid-19.

#### **RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO**

##### **ART. 59 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-OCTIES DEL DECRETO 231**

I reati-presupposto di cui all'art. 25-octies del Decreto 231 sono:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648 bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.);
- Autoriciclaggio (art. 648-ter.1 c.p.).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

##### **ART. 60 - MISURE DI PREVENZIONE**

I reati di cui all'art. 25-octies del Decreto 231 sono classificabili come **reati comuni**.

Il **rischio** è **basso**.

Le **aree/attività** presidiate sono quelle a diretto contatto con terzi, clienti, fornitori e consulenti e, in particolare, l'Ufficio Contabilità, l'Ufficio Acquisti e l'Ufficio Accettazione e Ricoveri. Le **attività sensibili** sono:

selezione, valutazione e gestione dei rapporti con i fornitori ai fini della stipula dei contratti di acquisto di beni;

gestione dei rapporti con partner commerciali;

gestione delle risorse finanziarie;

gestione del processo di sponsorizzazione e concessione di erogazioni liberali e donazioni;

gestione delle attività e degli adempimenti connessi alla fiscalità.

#### **Le misure di prevenzione:**

è vietato, soprattutto a tutti coloro che operino nelle aree a rischio sopra identificate, acquistare, ricevere, sostituire o trasferire beni o denaro per occultare o dissimulare la loro origine illecita quando si abbia motivo di ritenere che provengano da attività delittuose. Nello specifico, questi soggetti sono tenuti a seguire la procedura qui indicata ai fini dell'identificazione dei terzi, clienti fornitori e consulenti, con cui essi entrino in contatto e a conservare copia dei documenti di identità in corso di validità e dell'ulteriore documentazione acquisita ai fini dell'identificazione.

In particolare, i suddetti soggetti devono provvedere a:

- la preventiva acquisizione di informazioni circa l'attendibilità commerciale e professionale del fornitore sulla base di alcuni indicatori di anomalia previsti dall'art. 41, co. 2, del d.lgs. n. 231/2007 e individuati con successivi provvedimenti di attuazione (es. dati pregiudizievoli pubblici (protesti, procedure concorsuali) o acquisizione di informazioni commerciali sull'azienda, sui soci e sugli amministratori tramite società specializzate;

- valutare se sussiste il coinvolgimento di "*persone politicamente esposte*" (come definite all'art. 1 dell'Allegato tecnico del d.lgs., n. 231/2007);

- valutare l'entità del prezzo e le condizioni che il fornitore richiede per l'opera, il servizio o i beni offerti in relazione alle condizioni di norma praticate nel mercato;

- verificare la corrispondenza tra i destinatari dei pagamenti e i soggetti effettivamente coinvolti nella transazione commerciale, nel rispetto del principio generale secondo cui la Società non accetta pagamenti da parte di soggetti diversi dai soggetti obbligati, preventivamente identificati come tali (di norma, all'atto della conclusione dell'accordo).

Le medesime procedure sono applicate anche in caso di attività di investimento e sponsorizzazioni.

L'Amministratore riveste il ruolo di responsabile dell'esecuzione dei contratti e, in quanto tale, è comunque responsabile della corretta esecuzione di tutte le attività sopra elencate.

Il personale addetto alla contabilità nonché chiunque altro sia delegato a effettuare pagamenti o incassi devono rispettare gli obblighi di cui agli artt. 49 e 50 del d.lgs. n. 231/2007.

I soggetti interessati sono inoltre tenuti obbligatoriamente a partecipare ai corsi di formazione organizzati presso la Società ai fini dell'illustrazione della normativa applicabile nonché, in concreto, delle operazioni suscettibili di essere considerate a rischio di riciclaggio.

Ai contratti che regolano rapporti commerciali devono essere apposte clausole che richiamano gli adempimenti e le responsabilità derivanti dal Decreto 231 e dal rispetto

dei principi fondamentali del Modello e del Codice etico, che vengono comunicati a partner e fornitori e indichino chiari effetti contrattuali in merito al mancato rispetto di tali adempimenti.

In caso di violazione degli obblighi sopra riportati, trovano applicazione specifiche sanzioni disciplinari.

## REATI AMBIENTALI

### ART. 61 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-UNDECIES DEL DECRETO 231

I reati-presupposto di cui all'art. 25-*undecies* del Decreto 231 sono:

- Inquinamento ambientale (art. 452 *bis* c.p.);
- Disastro ambientale (art. 452 *quater* c.p.);
- Delitti colposi contro l'ambiente (art. 452 *quinquies* c.p.);
- Traffico e abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.);
- Circostanze aggravanti (art. 452 *octies* c.p.).
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 *bis* c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 *bis* c.p.);
- Scarico di acque reflue industriali (art. 137, d.lgs. n. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256, d.lgs. n. 152/2006);
- Combustione illecita di rifiuti (art. 256 *bis*, d.lgs. n. 152/2006);
- Bonifica dei siti (art. 257, d.lgs. n. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, co. 4, d.lgs. n. 152/2006);
- Traffico illecito di rifiuti (art. 259, co. 1, d.lgs. n. 152/2006);
- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 *bis* d.lgs. n. 152/2006);
- Superamento dei valori limite della qualità dell'aria (art. 279, co. 5, d.lgs. n. 152/2006);
- Art. 1, co. 1, l. n. 150/1992;
- Art. 2, co. 1 e 2, l. n. 150/1992;
- Art. 3-*bis*, co. 1, l. n. 150/1992;
- Art. 6, co. 4, l. n. 150/1992;
- Misure a tutela dell'ozono stratosferico e dell'ambiente - Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3, co. 6, l. n. 549/1993);
- Inquinamento doloso (art. 8 d.lgs. n. 202/2007);
- Inquinamento colposo (art. 9 d.lgs. n. 202/2007).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

## ART. 62 - MISURE DI PREVENZIONE

I reati ambientali di cui all'art. 25-*undecies* del Decreto 231 sono classificabili come **reati comuni**.

Le **aree/attività** potenzialmente a rischio sono tutte quelle che implicano la gestione di rifiuti e acque reflue.

Il **rischio** è **basso**. È peraltro **escluso** il rischio di verifica dei reati ambientali che implicano lo svolgimento di attività su navi o aeromobili, nonché di quelli consistenti nel traffico e abbandono di materiale ad alta radioattività. Il rischio è essenzialmente circoscritto ai reati connessi alla gestione dei rifiuti e alle acque reflue, anche in considerazione dell'assenza di laboratori analisi.

### Le **misure di prevenzione**:

al Direttore Sanitario compete la responsabilità della gestione dei rifiuti e del rispetto dell'ambiente. In particolare, il Direttore Sanitario deve assicurare il rispetto delle disposizioni di legge in materia di deposito temporaneo presso il luogo di produzione dei rifiuti sanitari sino al conferimento dei medesimi all'operatore autorizzato della ditta smaltitrice. Al Direttore Sanitario spetta altresì il controllo sulla corretta tenuta dei registri di carico e scarico dei rifiuti. Nell'espletamento di queste funzioni, il Direttore Sanitario, che resta comunque di esse responsabile per legge, può avvalersi della collaborazione di uno o più dipendenti della Società, dopo che abbia a costoro conferito specifico incarico e abbia provveduto alla loro formazione.

Ogni operatore si attiene alle istruzioni impartite dal Direttore Sanitario in materia di raccolta dei rifiuti, nel rispetto delle specifiche norme procedurali indicate nel "Manuale pratico della gestione dei rifiuti" adottato dalla Società e della classificazione, ivi contenuta, dei rifiuti come pericolosi e non pericolosi, a rischio infettivo e non a rischio infettivo e delle rispettive regole di smaltimento.

Il "Manuale pratico della gestione dei rifiuti" adottato dalla Società è sottoposto a revisione periodica; eventuali aggiornamenti sono comunicati a tutti gli interessati da parte del Direttore Sanitario.

La gestione amministrativa dei rifiuti è posta sotto la responsabilità dell'Amministrazione, che provvede alla tenuta dei registri di carico e scarico dei rifiuti, ai sensi del d.lgs. n. 152/2006.

L'Amministratore assicura che siano messe in atto tutte le attività necessarie alla gestione dei rifiuti nel rispetto della normativa vigente.

## DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

### ART. 63 - REATI-PRESUPPOSTO DI CUI ALL'ART. 24-BIS DEL DECRETO 231

I reati-presupposto di cui all'art. 24-*bis* del Decreto 231 sono:

- Documenti informatici (art. 491 *bis* c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.);

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.);
- reato di ostacolo o condizionamento dei procedimenti per la Sicurezza Cibernetica e delle relative attività ispettive e di vigilanza (art. 1, co. 11, d.l. 105/2019).

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

#### **ART. 64 - MISURE DI PREVENZIONE**

I reati di cui all'art. 24-*bis* del Decreto 231 sono classificabili come **reati comuni**.

Le **aree/attività** potenzialmente a rischio sono la Direzione Sanitaria, in relazione all'attività di predisposizione e gestione delle cartelle cliniche, l'Ufficio Accettazione e Ricoveri, in relazione alla gestione dei dati dei pazienti, l'Ufficio Contabilità, in relazione alla gestione della contabilità e l'Ufficio del Personale per quanto attiene rispettivamente ai dati dei fornitori e a quelli dei dipendenti.

**Il rischio è medio.**

**Le misure di prevenzione:**

sono previste precise regole riguardanti le modalità di predisposizione e gestione delle cartelle cliniche. Le cartelle cliniche sono predisposte dai medici dei reparti, sotto la responsabilità di ciascun Direttore di Unità Operativa e del Direttore Sanitario.

L'Amministratore deve nominare un'apposita commissione sanitaria, presieduta dal Direttore Sanitario e composta da ciascun Direttore di Unità Operativa e da altri due medici alla quale è affidato il compito di verificare periodicamente, almeno con cadenza trimestrale, un campione significativo di cartelle cliniche allo scopo di ricercare se sussistano eventuali incongruenze o errori. È compito di questa commissione redigere un verbale che certifichi quante e quali cartelle cliniche siano

state da essa analizzate e le risultanze delle analisi compiute, al fine di adottare eventuali misure correttive o intensificare i controlli incrociati in fase di predisposizione delle cartelle cliniche.

Al fine di prevenire la possibilità che vengano rilasciate false certificazioni da parte dei medici, il personale dell'Ufficio Accettazione e Ricoveri controlla la corrispondenza del contenuto delle certificazioni rispetto ai dati contenuti nella cartella clinica. Analogo controllo viene svolto per evitare che il Direttore Sanitario rilasci copia legale di cartella clinica contenente divergenze, anche solo parziali, rispetto al contenuto originale della cartella stessa. Il personale dell'Ufficio Accettazione e Ricoveri ha inoltre il compito di verificare periodicamente, almeno su base trimestrale, la corrispondenza dei dati contenuti nelle copie legali delle cartelle cliniche rilasciate con gli originali.

Il Responsabile dei Sistemi Informativi ha inoltre il compito di predisporre quanto necessario per la corretta e sicura gestione dei sistemi informatici in uso presso la Società; è tenuto poi a fornire periodicamente - e comunque almeno una volta l'anno - con relazione scritta informazioni all'Amministratore circa le attività compiute e le risultanze delle verifiche effettuate.

Nello specifico, il Responsabile dei Sistemi Informativi è incaricato di predisporre le misure e procedure di seguito indicate e di assicurarne il rispetto: misure di sicurezza per apparecchiature fuori sede; procedure per la gestione e manutenzione dei sistemi utilizzati presso la Società; procedure per i controlli sulla rete aziendale e sulle informazioni che vi transitano, sull'instradamento (*routing*) della rete (funzionale ad assicurare che non vengano violate le politiche di sicurezza), sull'installazione di software sui sistemi operativi; procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi informatici; controlli di individuazione, prevenzione e ripristino funzionali a proteggere da software dannosi (virus), nonché procedure per la sensibilizzazione degli utenti sul tema; misure per un'adeguata protezione delle apparecchiature incustodite; misure per la protezione dei documenti elettronici (es. firma digitale); procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali. Queste procedure sono descritte in apposito documento, disponibile presso la sede della Società e adeguatamente diffuso a tutti gli utenti.

I soggetti incaricati di trasmettere a terzi (ASL, Regione) dati e informazioni circa l'attività sanitaria svolta o i pazienti (come, ad esempio, le liste dei pazienti ricoverati e dimessi) assumono la diretta responsabilità in ordine alla veridicità dei dati e delle informazioni trasmessi.

La prevenzione dei reati informatici non specificamente connessi con la gestione delle cartelle cliniche è assicurata dal rispetto delle seguenti misure e procedure: misure di protezione dei documenti elettronici (es. firma digitale); procedure di validazione delle credenziali dotate di un sufficiente livello di complessità, soggette a modifica periodica e che prevedono la rimozione dei diritti di accesso al termine del rapporto di lavoro; aggiornamento regolare dei sistemi informatici in uso; procedure di autorizzazione per l'accesso ai sistemi informatici aziendali, che prevedono la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al rispettivo ruolo; procedure di controllo degli accessi e loro tracciabilità; inclusione negli accordi con

terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni; misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse.

Il funzionamento del sistema di gestione per la tutela della privacy è descritto nei documenti redatti in conformità al GDPR redatto in base alle disposizioni del Disciplinare tecnico in materia di misure minime di sicurezza del Codice in materia di protezione dei dati personali.

#### IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

##### ART. 65 - REATI PRESUPPOSTO DI CUI ALL'ART. 25-DUODECIIES DEL DECRETO 231

I reato-presupposto di cui all'art. 25-*duodecies* del Decreto 231 sono:

- art. 22, co. 12-*bis*, del d.lgs. 286/1998;
- art. 12, co. 3, 3-*bis*, 3-*ter* e 5 del d. lgs. 286/98.

La descrizione di questi reati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

##### ART. 66 - MISURE DI PREVENZIONE

Il reato di cui all'art. 25-*duodecies* del Decreto 231 è classificabile come **reato comune**.

L'**area** rilevante è quella dell'Ufficio del Personale.

Il **rischio** è **basso**.

Le **misure di prevenzione**:

è previsto l'obbligo dell'Amministratore nonché di tutti i soggetti che operano presso l'Ufficio del Personale e che sono incaricati di controllare la documentazione rilevante ai fini dell'assunzione di verificare – sia al momento dell'assunzione dei dipendenti sia durante lo svolgimento di tutto il rapporto lavorativo – che i lavoratori provenienti da paesi terzi siano in regola con il permesso di soggiorno e con i relativi rinnovi. In particolare, questa documentazione viene chiesta ai lavoratori provenienti da paesi terzi in aggiunta a quella di norma acquisita all'atto dell'assunzione e comprende quanto segue: carta di identità, codice fiscale, titolo di studio o professionale in relazione alla qualifica, certificato di residenza e di nascita, certificato del casellario giudiziale, certificato carichi pendenti.

Inoltre, nelle ipotesi di inserimento nell'organico di un lavoratore straniero, anche a tempo determinato, i predetti soggetti sono altresì tenuti, per quanto di propria competenza, a dichiarare in forma scritta all'Amministratore l'avvenuto rispetto delle prescrizioni e dei divieti contenuti nel d.lgs. n. 286/1998.

Se la Società si avvale di agenzie fornitrici di lavoro interinale o stipula contratti di somministrazione, appalto, contratti d'opera, essa si fa rilasciare una garanzia con la quale la società interessata dichiara, sotto la propria responsabilità, che essa stessa si

avvale esclusivamente di lavoratori in regola con la normativa in materia di permesso di soggiorno.

La Società acquisisce una garanzia analoga quando instaura rapporti di collaborazione, anche occasionale, con soggetti terzi che, a loro volta, si avvalgono di lavoratori provenienti da paesi terzi: anche questi soggetti dichiarano, sotto la propria responsabilità, che si avvalgono esclusivamente di soggetti in regola con la normativa in materia di permesso di soggiorno.

## TUTELA DEL DIRITTO D'AUTORE

### ART. 67 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-NOVIES DEL DECRETO 231

I reati-presupposto di cui all'art. 25-*novies* del Decreto 231 sono quelli di cui all'art. 171, co. 1, lett. a-*bis* e co. 3, all'art. 171-*bis*, all'art. 171-*ter*, all'art. 171-*septies* e all'art. 171-*octies*, della l. n. 633/1941.

La descrizione dei reati sopra richiamati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 68 - MISURE DI PREVENZIONE

I reati di cui all'art. 25-*novies* del Decreto 231 sono classificabili come **reati comuni**.

Il **rischio** è **molto basso**.

L'**area** potenzialmente a rischio è l'Ufficio Contabilità, l'Ufficio Accettazione e l'area amministrativa, in quanto ivi lavorano i dipendenti che hanno accesso ai sistemi informativi in uso. I processi aziendali a rischio sono tutte quelle attività connesse con l'utilizzo di software e banche dati.

Le **misure di prevenzione**:

il Responsabile dei Sistemi Informativi ha predisposto e cura l'applicazione di procedure finalizzate ad evitare fenomeni di: c.d. *file sharing* (vale a dire condivisione o scambio di file in violazione della normativa del diritto d'autore e, comunque, al di fuori degli ordinari e leciti circuiti commerciali dei beni oggetto di proprietà intellettuale); *upload/download* (vale a dire immissione o condivisione, senza averne diritto, di contenuti protetti da diritti d'autore in un sistema di reti telematiche); *underlicensing* (vale a dire violazioni delle condizioni di licenza di un software); *hard disk loading* (vale a dire vendita e acquisto per l'azienda di computer sui quali sono installati software piratati); utilizzazione non autorizzata di banche dati; distribuzione e installazione di dispositivi di decodificazione per l'accesso a un servizio criptato, senza pagamento del canone.

Il Responsabile dei Sistemi Informativi ha inoltre predisposto e cura l'applicazione di una procedura aziendale che obbliga a un utilizzo corretto e lecito dei software e delle banche dati in uso e che impone specifici divieti aventi ad oggetto: l'installazione di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano la licenza d'uso; la diffusione anche attraverso la gestione del sito internet aziendale, di immagini,

documenti o altro materiale tutelati dalla normativa in materia di diritto d'autore; l'utilizzazione di software e banche dati in assenza di valida licenza.

Il Responsabile dei Sistemi Informativi fornisce informazioni all'Amministratore periodicamente, e comunque almeno una volta l'anno con relazione scritta, circa le attività compiute e le risultanze delle verifiche effettuate con riferimento alle procedure e misure a tutela del diritto di autore.

## DELITTI DI CRIMINALITÀ ORGANIZZATA

### ART. 69 - REATI-PRESUPPOSTO DI CUI ALL'ART. 24-TER DEL DECRETO 231

I delitti previsti dall'art. 24-ter del Decreto 231 sono:

- Associazione per delinquere (art. 416 c.p.);
- Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.);
- Scambio elettorale politico-mafioso (art. 416 ter c.p.);
- Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);
- Traffico di organi prelevati da persona vivente (art. 601 bis c.p.);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. n. 309/1990);
- art. 407, co. 2, lettera a), numero 5), c.p.p.

La descrizione dei reati elencati e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

### ART. 70 - MISURE DI PREVENZIONE

I reati di cui all'art. 24-ter del Decreto 231 sono classificabili come **reati comuni**.

Il **rischio è basso**.

Le **aree/attività** potenzialmente a rischio sono quelle deputate alla selezione e assunzione del personale e alla selezione di fornitori di beni e servizi, quindi, l'Ufficio del Personale, l'Ufficio Acquisti e l'Amministratore Unico.

Le **misure di prevenzione**:

l'Amministratore e suoi delegati devono rispettare il principio di libera concorrenza e vietare di approfittare in qualunque forma di eventuali condizioni di assoggettamento ambientale che determinino situazioni di disparità nelle contrattazioni commerciali.

È prevista una **procedura per la selezione dei partner commerciali** in base alle quale questi soggetti devono: possedere una qualificazione etica (prevista dalla legge o da sistemi di autoregolamentazione), impegnarsi a produrre una dichiarazione sostitutiva attestante il rispetto delle norme contributive, fiscali, previdenziali e assicurative a favore dei propri dipendenti e collaboratori, degli obblighi di tracciabilità finanziaria, nonché l'assenza di provvedimenti a carico loro o dei loro soggetti apicali per reati della specie di quelli previsti dal Decreto 231, con particolare riferimento a quelli di cui all'art. 24-ter.

È obbligatorio che nei contratti con i fornitori siano previste: clausole risolutive espresse per il caso in cui l'impresa fornitrice, destinataria di una certificazione antimafia regolare, risulti destinataria di una sopraggiunta comunicazione ovvero informazione antimafia interdittiva, nonché per l'ipotesi di mancato rispetto delle norme richiamate sopra e dell'obbligo di denunciare i reati subiti direttamente o dai propri familiari e/o collaboratori; limitazione al tempo strettamente necessario del termine entro cui il fornitore destinatario di una sopraggiunta informazione antimafia interdittiva venga in concreto estromesso dal contratto.

Inoltre, per quanto concerne la gestione degli stupefacenti, il registro di carico e scarico degli stessi è affidato al Direttore Sanitario, il quale può delegare tale gestione solo a una persona; il registro viene sottoposto a periodici controlli sulla sua regolare tenuta, anche ad opera dell'Amministratore. In ogni caso, nessuno può accedere al luogo in cui sono conservati gli stupefacenti senza espressa autorizzazione scritta del Direttore Sanitario.

#### INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

##### ART. 71 - REATI-PRESUPPOSTO DI CUI ALL'ART. 25-DECIES DEL DECRETO 231

Il delitto di cui all'art. 25-*decies* è quello di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.).

La descrizione di questo reato e l'indicazione delle relative sanzioni sono contenute nell'Allegato I al Modello.

##### ART. 72 - MISURE DI PREVENZIONE

Il reato di cui all'art. 25-*decies* del Decreto 231 è classificabile come **reato comune**.

Il **rischio** è **molto basso**.

Non sussistono specifiche **aree/attività** potenzialmente a rischio; piuttosto, tutti i soggetti che operano presso la Società e che abbiano rapporti con altri soggetti coinvolti in procedimenti giudiziari e possano essere chiamati a rendere dichiarazioni in quel contesto sono potenzialmente a rischio.

Le **misure di prevenzione**:

obbligo di immediata comunicazione all'Amministratore di eventuali notizie o notifiche di indagini, nel rispetto dei principi etici di correttezza, volti a evitare il compimento del reato in questione.

### SEZIONE III

**TABELLA RIASSUNTIVA RISK ASSESSMENT: MAPPATURA DELLE ATTIVITÀ SENSIBILI E DEI PROCESSI A RISCHIO REATO, VALUTAZIONE DEI RISCHI E MISURE DI PREVENZIONE E DI CONTROLLO ADOTTATE**

Reati ex d.lgs. 231/2001	Aree coinvolte	Processi aziendali	Misure di prevenzione	Livello di rischio
<p><b>Reati contro la Pubblica Amministrazione -</b></p> <p><b>Indebita percezione di erogazioni, Truffa in danno dello Stato, di un Ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un Ente pubblico e frode nelle pubbliche forniture (art. 24 d.lgs. 231/2001)</b></p>	<p>Direzione Sanitaria;</p> <p>Reparti;</p> <p>Uff. Contabilità;</p> <p>Uff. Acquisti.</p>	<p>Classificazione delle prestazioni sanitarie rimborsate dal Servizio Sanitario Nazionale;</p> <p>gestione di contratti con la Pubblica Amm;</p> <p>acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti concessi da P.A;</p> <p>ottenimento di permessi, licenze, autorizzazioni;</p> <p>richiesta di autorizzazioni all'esercizio di attività sanitaria, accreditamenti, rimodulazione di posti letto.</p>	<p>Diligenza professionale nell'adozione delle delibere di affidamento di deleghe e verifica sulla legittimità e l'ampiezza di eventuali sub-deleghe;</p> <p>relazioni periodiche;</p> <p>protocollo specifico per la richiesta di finanziamenti;</p> <p>procedura per la corretta codificazione delle prestazioni e gestione della cartella clinica;</p> <p>procedura per evitare il rischio di frode informatica.</p>	<p><b>Medio</b></p>
<p><b>Reati P.A. -Peculato, concussione, induzione indebita a</b></p>	<p>Amministratore ;</p>		<p>Rispetto normativa anticorruzione;</p>	

<p><b>dare o promettere utilità, corruzione, abuso di ufficio</b></p> <p>(art. 25 d. lgs. 231/2001)</p>	<p>Uff. Contabilità; Uff. Personale; Direzione Sanitaria; Uff. Acquisti; eventuali consulenti esterni.</p>	<p>Selezione e gestione del personale; presa in carico dei pazienti e ospiti della struttura; gestione delle ispezioni amministrative, fiscali e previdenziali; gestione degli affari legali e di attività giudiziali e stragiudiziali; gestione di omaggi, pubblicità, sponsorizzazioni , autorizzazioni e accreditamento, accordi contrattuali, concessione di finanziamenti, verifiche, controlli e ispezioni; gestione dei flussi finanziari. relazioni istituzionali con autorità e p.a. Gestione degli acquisti di beni e servizi.</p>	<p>tracciabilità e verifica dei flussi finanziari; diligenza professionale nell'adozione delle delibere di affidamento di deleghe e verifica sulla legittimità e l'ampiezza di eventuali sub-deleghe; procedura per i rapporti con ASL e Regione; divieto di elargizione di denaro e/o doni a dipendenti della P.A.; ulteriori divieti e obblighi.</p>	<p><b>Medio</b></p>
<p><b>Falsità in monete, in carte di pubblico credito, in valori di</b></p>	<p>Uff. Accettazione;</p>		<p>Utilizzo del bonifico bancario quale</p>	

<p><b>bollo e in strumenti o segni di riconoscimento, delitti contro l'industria e il commercio (artt. 25 bis e 25 bis-1 d.lgs. 231/2001)</b></p>	<p>Uff. Contabilità; Uff. Acquisti; Amministratore</p>	<p>Pagamenti effettuati e incassi ricevuti.</p>	<p>mezzo prevalente di pagamento; diligenza nell'adozione delle delibere e nell'affidamento di deleghe; procedure per l'effettuazione dei pagamenti e degli incassi; tracciabilità degli strumenti di pagamento; controllo sui fornitori.</p>	<p><b>Basso</b></p>
<p><b>Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 octies-1 d.lgs. 231/2001)</b></p>	<p>Sono le medesime previste per i reati presupposto di cui agli artt. 25 bis e 25 bis-1 d.lgs. 231/2001.</p>	<p>Sono i medesimi previsti per i reati presupposto di cui agli artt. 25 bis e 25 bis-1 d.lgs. 231/2001.</p>	<p>Sono le medesime previste per i reati presupposto di cui agli artt. 25 bis e 25 bis-1 d.lgs. 231/2001.</p>	<p>È il medesimo previsto per i reati presupposto di cui agli artt. 25 bis e 25 bis-1 d.lgs. 231/2001</p>
<p><b>Reati societari (art. 25 ter, d. lgs. 231/2001)</b></p>	<p>Amministratore ; Sindaco; Liquidatori; Revisore.</p>	<p>Tenuta della contabilità; attività di predisposizione della documentazione funzionale alla formazione del bilancio;</p>	<p>Procedura di controllo della documentazione e riunioni periodiche; attività di formazione/informazione, verifiche e segnalazioni; attuazione di politiche commerciali</p>	<p><b>Medio</b></p>

		<p>gestione delle operazioni societarie;</p> <p>gestione dei rapporti con l'incaricato del controllo contabile, del collegio sindacale e degli altri organi societari.</p>	<p>preventivamente determinate;</p> <p>sottoscrizione di una dichiarazione di veridicità e completezza delle informazioni;</p> <p>rispetto del Codice etico.</p>	
<p><b>Reati tributari (art. 25 <i>quinquiesdecies</i> d. lgs. 231/2001)</b></p>	<p>Uff. Acquisti;</p> <p>Uff. Contabilità.</p>	<p>Attività di approvvigionamento di beni e servizi; aree abilitate ad acquistare beni e servizi da cui potrebbero trarre origine fatture false attive e passive;</p> <p>complesso di attività dichiarative volte alla determinazione dei tributi;</p> <p>redazione del bilancio e dei documenti fiscali.</p>	<p>Implementazione di un sistema di corretta tenuta della documentazione contabile;</p> <p>separazione delle fasi di approvvigionamento e affidamento delle stesse a responsabili differenti;</p> <p>gestione del rapporto con clienti e fornitori;</p> <p>riscontro periodico svolto da funzioni di controllo interne;</p> <p>monitoraggio dei prezzi di vendita e di acquisto;</p> <p>interlocuzione con l'agenzia delle Entrate.</p>	<p><b>Medio</b></p>
<p><b>Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (art.</b></p>	<p>Uff. Contabilità;</p> <p>Uff. Acquisti;</p> <p>Uff. Accettazione;</p>	<p>Selezione, valutazione e gestione dei rapporti con terzi, clienti,</p>	<p>Utilizzo di specifica procedura ai fini dell'identificazione dei terzi, clienti fornitori e consulenti;</p>	<p><b>Basso</b></p>

<p>25 <i>octies</i>, d. lgs. 231/2001)</p>	<p>Amministratore</p>	<p>fornitori e consulenti;</p> <p>gestione dei rapporti con partner commerciali;</p> <p>gestione delle risorse finanziarie;</p> <p>gestione del processo di sponsorizzazione e concessione di erogazioni liberali e donazioni;</p> <p>gestione delle attività e degli adempimenti connessi alla fiscalità.</p>	<p>rispetto d.l. n. 231/2007;</p> <p>formazione obbligatoria;</p> <p>inserimento di clausole che richiamano gli adempimenti e le responsabilità di cui al Decreto 231/2001 ed i principi di cui al Codice Etico nei contratti con i fornitori e partner commerciali.</p>	
<p><b>Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 <i>septies</i> d. lgs. 231/2001)</b></p>	<p>Direzione Sanitaria;</p> <p>Amministratore ;</p> <p>medico competente;</p> <p>RSPP.</p>	<p>Attività a rischio di infortunio e malattia professionale;</p> <p>attività a rischio di reato:</p> <p>individuazione delle disposizioni normative applicabili a cui uniformarsi per il rispetto degli standard tecnico-strutturali.</p> <p>definizione delle risorse, dei ruoli e delle responsabilità per assicurare le attività</p>	<p>Nomina di RSPP;</p> <p>rispetto del d.lgs. 81/2008;</p> <p>attività di istruzione e formazione del personale;</p> <p>controlli su tutti gli aspetti impiantistici;</p> <p>obbligo di relazione all’Odv da parte dei soggetti responsabili sulle attività svolte;</p> <p>misure di prevenzione e protezione per il contenimento da contagio Covid-19.</p>	<p><b>Medio</b></p>

		<p>finalizzate all'attuazione delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;</p> <p>gestione delle emergenze, delle attività di prevenzione degli incendi e di primo soccorso;</p> <p>gestione degli appalti;</p> <p>attività di sorveglianza sanitaria;</p> <p>formazione e informazione dei lavoratori;</p> <p>controllo sugli acquisti, acquisizione di documentazioni e certificazioni;</p> <p>attività manutentive finalizzate al rispetto degli standard tecnici e di salute e sicurezza applicabili;</p> <p>gestione della documentazione e dei sistemi di registrazione al fine di garantire la tracciabilità delle attività.</p>		

<b>Reati ambientali (art. 25 undecies d. lgs. 231/2001)</b>	Direzione Sanitaria.	Gestione dei rifiuti e delle acque reflue.	Rispetto della normativa e degli standard in materia;  procedura gestione dei rifiuti sanitari.	<b>Basso</b>
<b>Delitti informatici e trattamento illecito dei dati (art. 24 bis d. lgs. 231/2001)</b>	Direzione Sanitaria;  Uff. Contabilità;  Uff. Accettazione;  Ufficio del Personale;  Responsabile dei sistemi informatici.	Attività di predisposizione e gestione delle cartelle cliniche;  trasmissione a terzi (ASL, Regione, associazione di categoria) di dati e informazioni circa l'attività sanitaria svolta o i pazienti;  attività informatiche non specificamente connesse con la gestione delle cartelle cliniche.	Nomina di un Responsabile dei sistemi informatici incaricato di predisporre misure e procedure;  procedure di predisposizione e gestione delle cartelle cliniche.	<b>Medio</b>
<b>Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater d. lgs. 231/2001)</b>	Ufficio Personale;  Uff. Accettazione.	Procedure connesse  alle assunzioni dei dipendenti e al possesso in capo a costoro dei requisiti richiesti dalla normativa e dal CCNL.	Rispetto del Codice etico e della normativa vigente in materia.	<b>Molto basso</b>
<b>Delitti contro la personalità individuale (art. 25)</b>	Area amministrativa;  Uff. Personale;	Accesso a siti e/o ricezione di materiale relativo alla	Rispetto del codice etico e della normativa vigente in materia.	<b>Basso</b>

<i>quinquies</i> d. lgs. 231/2001)	Direzione Sanitaria.	pornografia minorile; assunzione del personale.		
<b>Abusi di mercato (art. 25 <i>sexies</i> d. lgs. 231/2001)</b>	Area amministrativa.		Rispetto del Codice etico.	<b>Molto Basso</b>
<b>Pratiche di mutilazione degli organi genitali femminili (Art. 25 <i>quater-1</i> d. lgs. 231/2001)</b>	Area strettamente sanitaria (medici e paramedici); Ufficio Accettazione.	Accettazione e presa in carico delle pazienti.	Rispetto del codice etico; formazione specifica sulla pratica di mutilazione al personale medico e parasanitario da parte del Medico Responsabile della struttura; attestazione circa le condizioni di entrata della paziente da parte del personale sanitario.	<b>Basso</b>
<b>Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 <i>duodecies</i> d. lgs. 231/2001)</b>	Ufficio del Personale; Amministratore	Assunzione di lavoratori	Controllo sui permessi di soggiorno; Procedure specifiche per l'assunzione del personale; Rispetto del d.lgs 286/1998.	<b>Basso</b>

<p><b>Tutela del diritto d'autore (art. 25 <i>novies</i> d. lgs. 231/2001)</b></p>	<p>Area amministrativa; Ufficio Accettazione.</p>	<p>Utilizzo di software e banche dati.</p>	<p>Applicazione di una procedura aziendale circa il corretto e lecito utilizzo dei software e delle banche dati; relazioni periodiche.</p>	<p><b>Basso</b></p>
<p><b>Delitti di criminalità organizzata (art. 24 <i>ter</i> d. lgs. 231/2001)</b></p>	<p>Ufficio del personale; Ufficio Acquisti.</p>	<p>Selezione e assunzione del personale; selezione fornitori beni e servizi.</p>	<p>Predisposizione di una procedura per la selezione dei partner commerciali; inserimento di clausole specifiche in materia.</p>	<p><b>Basso</b></p>
<p><b>Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25 <i>decies</i> d. lgs. 231/2001)</b></p>	<p>Tutti i soggetti che operano presso la sede legale e amministrativa della Società che abbiano rapporti con altri soggetti coinvolti in procedimenti giudiziari e possano essere chiamati a rendere dichiarazioni in quel contesto sono potenzialmente a rischio.</p>	<p>Dichiarazioni all'autorità giudiziaria.</p>	<p>Comunicazioni all'Amministratore di eventuali indagini.</p>	<p><b>Molto basso</b></p>

## **ALLEGATI**

- Allegato I - Reati presupposto e sanzioni
- Allegato II - Codice Etico
- Allegato III - procedura di whistleblowing