

**CREDICI S.R.L. – AGENZIA PER IL LAVORO  
MODELLO DI ORGANIZZAZIONE E GESTIONE**

**Parte Speciale**

ai sensi del d.lgs. 231/2001

Emendato con Delibera del 15.11.2025

Indice

<b>INTRODUZIONE E MODALITÀ DI SEGNALAZIONE (WHISTLEBLOWING)</b> .....	<b>3</b>
1. Finalità della Parte Speciale.....	3
2. Aree organizzative rilevanti.....	4
3. Classificazione dei reati presupposto.....	4
4. Modalità di segnalazione (whistleblowing).....	5
4.1 Oggetto delle segnalazioni.....	5
4.2 Canale unico di segnalazione WB.....	6
4.3 Canali alternativi.....	7
4.4 Gestione delle segnalazioni.....	7
4.5 Divieto di ritorsione e tutela del Segnalante.....	8
<b>1 – SEZIONE A – REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 D.LGS. 231 DEL 2001)</b> .....	<b>8</b>
1. Le fattispecie di reato.....	8
2. Le attività a rischio.....	9
3. Regole di comportamento.....	9
4. I controlli dell’Organismo di Vigilanza.....	10
<b>2 – SEZIONE B – REATI SOCIETARI (ART. 25-TER D.LGS. 231 DEL 2001)</b> .....	<b>11</b>
1. Le fattispecie di reato.....	11
2. Le attività a rischio.....	11
3. Regole di comportamento.....	12
4. I controlli dell’Organismo di Vigilanza.....	13
<b>3 – SEZIONE C – REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (ART. 25-SEPTIES)</b> .....	<b>13</b>
1. Le fattispecie di reato.....	13
2. Le attività a rischio.....	13
3. Regole di comportamento.....	14

Approvato per emendamento al MOG 231 con Delibera del 15.11.2025

4. I controlli dell'Organismo di Vigilanza.....	14
<b>4 – SEZIONE D – REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24-BIS)</b> .....	<b>15</b>
1. Le fattispecie di reato.....	15
2. Le attività a rischio.....	15
3. Regole di comportamento.....	16
4. I controlli dell'Organismo di Vigilanza.....	16
<b>5 – SEZIONE E – REATI AMBIENTALI (ART. 25-UNDECIES)</b> .....	<b>17</b>
<b>6 – SEZIONE F – REATI CONTRO LA PERSONALITÀ INDIVIDUALE (ART. 25-QUINQUIES)</b> .....	<b>17</b>
<b>7 – SEZIONE G – RICETTAZIONE, RICICLAGGIO, AUTORICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 25-OCTIES)</b> .....	<b>18</b>
1. Le fattispecie di reato.....	18
2. Le attività a rischio.....	18
3. Regole di comportamento.....	19
<b>8 – SEZIONE H – REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES)</b> .....	<b>19</b>
<b>9 – SEZIONE I – REATI DI CRIMINALITÀ ORGANIZZATA (ART. 24-TER)</b> .....	<b>20</b>
<b>10 – SEZIONE L (1) – REATI DI FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO, VALORI DI BOLLO E STRUMENTI O SEGNI DI RICONOSCIMENTO (ART. 25-BIS)</b> .....	<b>20</b>
<b>11 – SEZIONE L (2) – REATI CONTRO L'INDUSTRIA E IL COMMERCIO (ART. 25-BIS.1)</b> .....	<b>20</b>
<b>12 – SEZIONE M – DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (ART. 25-QUATER)</b> .....	<b>21</b>
<b>13 – SEZIONE N – PRATICHE PER LA MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (ART. 25-QUATER.1)</b> .....	<b>21</b>
<b>14 – SEZIONE O – ABUSI DI MERCATO (ART. 25-SEXIES D.LGS. 231 DEL 2001)</b> .....	<b>22</b>
<b>15 – SEZIONE P – INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25-DECIES)</b> .....	<b>22</b>
1. Le fattispecie di reato.....	22
2. Le attività a rischio.....	22
3. Regole di comportamento.....	23
4. I controlli dell'Organismo di Vigilanza.....	23
<b>16 – SEZIONE Q – DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 25-OCTIES.1)</b> .....	<b>24</b>

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

1. Le fattispecie di reato.....	24
2. Le attività a rischio.....	24
3. Regole di comportamento.....	24
<b>17 – SEZIONE R – IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25-DUODECIES)</b> .....	<b>25</b>
1. Le fattispecie di reato.....	25
2. Le attività a rischio.....	25
3. Regole di comportamento.....	25
4. I controlli dell’Organismo di Vigilanza.....	26
<b>18 – SEZIONE S – RAZZISMO E XENOFOBIA (ART. 25-TERDECIES)</b> .....	<b>27</b>
<b>19 – SEZIONE T – FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O SCOMMESSA E GIOCHI D’AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI (ART. 25-QUATERDECIES)</b> .....	<b>27</b>
<b>20 – SEZIONE U – REATI TRIBUTARI (ART. 25-QUINQUESDECIES)</b> .....	<b>28</b>
1. Le fattispecie di reato.....	28
2. Le attività a rischio.....	28
3. Regole di comportamento.....	28
4. I controlli dell’Organismo di Vigilanza.....	29
<b>21 – SEZIONE V – CONTRABBANDO (ART. 25-SEXIESDECIES)</b> .....	<b>29</b>
<b>22 – SEZIONE Y – DELITTI CONTRO IL PATRIMONIO CULTURALE (ART. 25-SEPTIESDECIES)</b> .....	<b>29</b>
<b>23 – SEZIONE Z – DELITTI CONTRO GLI ANIMALI (ART. 25-UNDEVICIES)</b> .....	<b>30</b>
<b>RIFERIMENTI E COORDINAMENTO</b> .....	<b>30</b>

## **INTRODUZIONE E MODALITÀ DI SEGNALAZIONE (WHISTLEBLOWING)**

### **1. Finalità della Parte Speciale**

La presente Parte Speciale del Modello di organizzazione, gestione e controllo ex decreto legislativo 231 del 2001 di **CREDICI S.R.L.** (di seguito anche «Società») individua, per le diverse categorie di reati presupposto, le attività aziendali a rischio, i principi di comportamento e i presidi di controllo che completano:

- la Parte Generale del Modello 231 della Società;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- il Codice Etico;
- il Regolamento Whistleblowing di CREDICI (edizione 01/2025);
- il Regolamento dell'Organismo di Vigilanza;
- le ulteriori policy e procedure interne in materia di salute e sicurezza, privacy, gestione del personale, amministrazione e finanza.

La Parte Speciale ha lo scopo di:

- definire, per ciascuna categoria di reati presupposto, le **fattispecie rilevanti** per la Società;
- individuare le **attività a rischio** connesse all'oggetto sociale e al modello operativo di CREDICI;
- fissare **regole di comportamento vincolanti** per amministratori, organi sociali, dipendenti, collaboratori, consulenti e soggetti terzi che operano in nome o per conto della Società;
- individuare i **flussi informativi** verso l'Organismo di Vigilanza (OdV) e le modalità di coordinamento con il sistema di whistleblowing.

## **2. Aree organizzative rilevanti**

Ai fini dell'analisi dei rischi e dell'applicazione della presente Parte Speciale, la Società è articolata, in via funzionale, nelle seguenti macro-aree:

- **Formazione e politiche attive del lavoro;**
- **Ricerca bandi e gestione progettazione;**
- **Rapporti istituzionali e sviluppo commerciale;**
- **Amministrazione, finanza e contabilità.**

Per ciascuna sezione vengono richiamate, ove necessario, le aree maggiormente esposte al rischio di commissione dei reati presupposto.

## **3. Classificazione dei reati presupposto**

L'analisi dei rischi condotta dalla Società ha portato a distinguere, per ogni categoria di reato, tra:

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- **reati potenzialmente realizzabili**, in relazione alle attività effettivamente svolte e ai processi aziendali mappati;
- **reati la cui commissione è ritenuta di bassa probabilità**, pur astrattamente configurabili rispetto all'oggetto sociale;
- **reati non applicabili**, in quanto non compatibili con l'attività e la struttura di CREDICI.

Questa classificazione è richiamata, se del caso, all'interno delle singole sezioni.

#### **4. Modalità di segnalazione (whistleblowing)**

La Società ha adottato un sistema di segnalazione interna conforme al decreto legislativo 10 marzo 2023 numero 24 e disciplinato dal Regolamento Whistleblowing di CREDICI S.R.L., che costituisce parte integrante del Modello 231.

Ai fini del presente Modello:

- per Segnalante o Whistleblower si intende la persona fisica che, in qualità di lavoratore, collaboratore, fornitore, consulente, candidato o altro soggetto in rapporto con la Società, comunica informazioni su violazioni delle disposizioni normative, del Modello 231, del Codice Etico o delle procedure interne, secondo quanto previsto dal decreto legislativo 24 del 2023 e dal Regolamento Whistleblowing;
- per Segnalato si intende il soggetto cui sono riferiti i fatti descritti nella segnalazione.
- Le definizioni e le modalità operative di dettaglio sono quelle contenute nel Regolamento Whistleblowing di CREDICI; in caso di difformità, prevale quanto previsto nel Regolamento.

#### **4.1 Oggetto delle segnalazioni**

Sono oggetto di segnalazione, in coerenza con il quadro normativo e regolamentare vigente, in via esemplificativa:

- condotte, atti od omissioni che integrano o possono integrare reati presupposto ex decreto legislativo 231 del 2001;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- violazioni del Modello 231, del Codice Etico e delle procedure connesse (ad esempio, in materia di gestione dei bandi, rapporti con la Pubblica Amministrazione, trattamento dei dati personali, salute e sicurezza, gestione del personale, trasparenza amministrativo-contabile);
- violazioni del diritto dell'Unione europea o nazionale nei settori richiamati dal decreto legislativo 24 del 2023;
- condotte idonee a vanificare o aggirare il sistema di controllo interno e i presidi delineati dalla presente Parte Speciale.

Non rientrano, di norma, nell'ambito del whistleblowing le lamentele di carattere personale che non hanno rilevanza per l'interesse pubblico o per l'integrità della Società, salvo quanto previsto dal Regolamento Whistleblowing.

#### **4.2 Canale unico di segnalazione WB**

La Società utilizza un **canale unico di segnalazione** tramite piattaforma informatica dedicata (di seguito «piattaforma WB»), condiviso con le altre entità del network, che consente al Segnalante di:

- trasmettere segnalazioni in forma scritta, eventualmente allegando documenti a supporto;
- ricevere un numero di protocollo o codice identificativo della segnalazione;
- dialogare con il soggetto incaricato della gestione, anche in forma anonima, nei limiti consentiti dalla normativa;
- essere informato sugli esiti della segnalazione entro i termini previsti dal decreto legislativo 24 del 2023.

La piattaforma WB garantisce:

- la tutela della **riservatezza** dell'identità del Segnalante, del Segnalato e dei terzi comunque menzionati;
- la **sicurezza** delle informazioni e dei documenti trasmessi;
- la **tracciabilità** delle operazioni compiute nel sistema, nel rispetto della normativa in materia di protezione dei dati personali.

Approvato per emendamento al MOG 231 con Delibera del 15.11.2025

### 4.3 Canali alternativi

Oltre al canale informatico, il Regolamento Whistleblowing prevede canali alternativi, quali ad esempio:

- invio di segnalazione scritta in busta chiusa con dicitura riservata, indirizzata al Responsabile WB o all'OdV;
- segnalazione orale mediante incontro diretto, su richiesta del Segnalante, secondo le modalità stabilite dal Regolamento;
- altri canali che la Società ritenga di attivare, nel rispetto del quadro normativo.
- Il ricorso ai canali alternativi non può comunque pregiudicare le garanzie di riservatezza e protezione del Segnalante, come disciplinate dalla normativa e dal Regolamento Whistleblowing.

### 4.4 Gestione delle segnalazioni

La gestione delle segnalazioni è affidata al soggetto o ai soggetti individuati nel Regolamento Whistleblowing (Responsabile WB, OdV, eventuale Comitato WB), nel rispetto dei principi di imparzialità, indipendenza e autonomia.

In sintesi:

- la Società assicura la **presa in carico** della segnalazione e l'invio al Segnalante di un avviso di ricevimento entro i termini di legge;
- viene svolta un'**istruttoria** proporzionata alla natura e alla gravità dei fatti segnalati, anche mediante richieste di chiarimenti al Segnalante, audizioni, acquisizione di documenti o informazioni presso le funzioni coinvolte;
- il soggetto potenzialmente coinvolto o in conflitto di interessi è escluso da ogni fase dell'istruttoria;
- al termine dell'istruttoria viene comunicato al Segnalante un **riscontro** sintetico, nel rispetto dei limiti di legge e delle esigenze di riservatezza;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- qualora emergano elementi di possibile rilevanza ai fini del decreto legislativo 231 del 2001, l'OdV ne è informato e valuta gli impatti sul Modello 231, adottando le opportune iniziative.

#### **4.5 Divieto di ritorsione e tutela del Segnalante**

È fatto divieto di porre in essere, di minacciare o di tentare qualsiasi forma di **ritorsione** o comportamento discriminatorio nei confronti del Segnalante per motivi direttamente o indirettamente collegati alla segnalazione. La Società assicura inoltre:

- la tutela della riservatezza dell'identità del Segnalante, fatte salve le eccezioni di legge;
- la protezione dei dati personali trattati nell'ambito del processo di segnalazione;
- il raccordo fra il sistema di whistleblowing e i procedimenti disciplinari, nel rispetto del principio del contraddittorio e del diritto di difesa.

Per quanto non espressamente previsto nella presente Parte Speciale, si rinvia integralmente al **Regolamento Whistleblowing di CREDICI S.R.L. (edizione 01/2025)**, che in caso di contrasto prevale.

## **1 – SEZIONE A – REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 D.LGS. 231 DEL 2001)**

### **1. Le fattispecie di reato**

Rientrano in questa sezione, a titolo esemplificativo, i reati di:

- indebita percezione di erogazioni, malversazione a danno dello Stato o dell'Unione europea, truffa aggravata per il conseguimento di erogazioni pubbliche;
- corruzione propria e impropria, concussione, induzione indebita a dare o promettere utilità, istigazione alla corruzione;
- frode nelle pubbliche forniture, peculato e abuso d'ufficio;
- ogni altra fattispecie prevista dagli articoli 24 e 25 del decreto legislativo 231 del 2001 e successive modifiche.

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

Per la Società tali reati sono considerati **potenzialmente realizzabili** in relazione alla gestione di rapporti, convenzioni, bandi e finanziamenti con soggetti pubblici.

## **2. Le attività a rischio**

Costituiscono, in via non esaustiva, attività a rischio:

- la partecipazione a bandi, avvisi pubblici e procedure selettive promosse da amministrazioni statali, regionali, locali o da enti pubblici, per l'ottenimento di contributi, finanziamenti, accreditamenti o convenzioni in materia di formazione e politiche attive del lavoro;
- la gestione operativa, amministrativa e rendicontale dei progetti finanziati con risorse pubbliche o europee;
- i rapporti con centri per l'impiego, agenzie regionali, enti previdenziali e ispettivi, nonché con altri soggetti pubblici competenti in materia di lavoro e formazione;
- la negoziazione, stipula ed esecuzione di contratti, convenzioni o protocolli d'intesa con pubbliche amministrazioni;
- la gestione di ispezioni, verifiche, controlli o audit effettuati da autorità pubbliche o organismi di vigilanza esterni.

## **3. Regole di comportamento**

Nello svolgimento delle attività a rischio, è fatto obbligo a tutti i destinatari del Modello di:

- mantenere rapporti con la Pubblica Amministrazione nel rispetto dei principi di **legalità, trasparenza, correttezza e tracciabilità**;
- astenersi da qualsiasi promessa, offerta, dazione o richiesta di denaro, utilità o vantaggi di qualunque natura, anche per interposta persona, che possano essere interpretati come finalizzati a influenzare indebitamente le decisioni di soggetti pubblici;
- rifiutare e segnalare, tramite i canali WB o all'OdV, ogni richiesta o sollecitazione di vantaggi indebiti proveniente da pubblici ufficiali o incaricati di pubblico servizio;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- utilizzare esclusivamente canali formali e autorizzati per i rapporti con la Pubblica Amministrazione, nel rispetto delle deleghe, delle procure e delle procedure interne;
- assicurare la **completezza, chiarezza, accuratezza e veridicità** delle informazioni fornite in sede di presentazione di domande di finanziamento, rendicontazione, relazioni o report verso soggetti pubblici;
- conservare in modo ordinato e accessibile la documentazione a supporto dei rapporti con la Pubblica Amministrazione, secondo quanto previsto dalle procedure interne.

È vietato, in particolare:

- utilizzare fondi, contributi o finanziamenti pubblici per finalità diverse da quelle per cui sono stati concessi;
- alterare o falsificare documenti, dati o informazioni destinati a soggetti pubblici;
- porre in essere qualsiasi condotta, anche omissiva, idonea a trarre in inganno la Pubblica Amministrazione o a indurre in errore i suoi rappresentanti.

#### **4. I controlli dell'Organismo di Vigilanza**

L'OdV, anche tramite i flussi informativi provenienti dalle funzioni competenti, verifica periodicamente:

- l'esistenza e l'effettiva applicazione di procedure interne per la gestione dei bandi, dei finanziamenti pubblici e dei rapporti con la Pubblica Amministrazione;
- la tracciabilità delle decisioni e delle operazioni significative connesse all'ottenimento e alla gestione di risorse pubbliche;
- la presenza di adeguata documentazione a supporto delle domande, delle rendicontazioni e dei rapporti con gli enti pubblici;
- eventuali segnalazioni ricevute tramite il canale WB in materia di rapporti con la Pubblica Amministrazione;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- l'adeguatezza del sistema dei controlli interni e l'opportunità di proporre aggiornamenti del Modello.

**2 – SEZIONE B – REATI SOCIETARI (ART. 25-TER D.LGS. 231 DEL 2001)**

**1. Le fattispecie di reato**

In relazione alla natura di **società di capitali** di CREDICI S.R.L., rientrano in questa sezione, in via esemplificativa:

- le false comunicazioni sociali e le false comunicazioni sociali in danno della società, dei soci o dei creditori;
- le ipotesi di illecita ripartizione di utili o riserve, indebita restituzione dei conferimenti, formazione fittizia del capitale;
- le operazioni in pregiudizio dei creditori;
- l'impedito controllo da parte dei sindaci o del soggetto incaricato della revisione legale;
- le omesse comunicazioni o le comunicazioni mendaci agli organi di controllo e ai soci;
- gli altri reati societari richiamati dall'articolo 25-ter del decreto legislativo 231 del 2001, nei limiti della loro compatibilità con l'assetto di governance della Società.

Per CREDICI tali reati sono considerati **potenzialmente realizzabili** in relazione ai processi di formazione del bilancio, alla tenuta delle scritture contabili e alla gestione dei rapporti con i soci e gli organi di controllo.

**2. Le attività a rischio**

Sono considerate attività a rischio, in particolare:

- la predisposizione del bilancio di esercizio, delle situazioni infrannuali e della reportistica economico-finanziaria interna ed esterna;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- la tenuta delle scritture contabili obbligatorie e dei libri sociali, nonché la conservazione della relativa documentazione di supporto;
- la redazione di relazioni e comunicazioni indirizzate ai soci, agli organi di controllo, agli istituti di credito e ad altri stakeholder;
- la gestione di operazioni sul capitale sociale, distribuzione di utili o riserve, operazioni infragruppo e significative operazioni straordinarie;
- la gestione dei rapporti con il soggetto incaricato della revisione e con eventuali ulteriori organi di controllo.

### **3. Regole di comportamento**

Nello svolgimento delle attività a rischio, è fatto obbligo di:

- rappresentare in modo **veritiero, completo, corretto e trasparente** la situazione patrimoniale, economica e finanziaria della Società;
- registrare ogni operazione contabile in modo **tempestivo, accurato e documentato**, nel rispetto dei principi contabili applicabili e delle procedure interne;
- conservare la documentazione giustificativa delle operazioni in modo da consentire la ricostruzione del processo decisionale e autorizzativo;
- garantire il corretto flusso di informazioni verso gli organi di controllo, fornendo dati e notizie completi e non fuorvianti;
- astenersi dall'effettuare operazioni sul capitale o sulla composizione della compagine sociale che possano arrecare pregiudizio ai creditori o ai soci, in violazione della legge o dello statuto.

È vietato:

- esporre fatti non rispondenti al vero, ancorché oggetto di valutazione, ovvero omettere informazioni la cui comunicazione è imposta dalla legge, in modo idoneo a indurre in errore i destinatari delle comunicazioni sociali;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- porre in essere operazioni simulate o fittizie tali da alterare la rappresentazione della situazione economico-finanziaria della Società;
- ostacolare con qualsiasi mezzo l'attività degli organi di controllo o del soggetto incaricato della revisione legale.

#### **4. I controlli dell'Organismo di Vigilanza**

L'OdV:

- riceve, con cadenza almeno annuale, copia del bilancio di esercizio e di eventuali relazioni dell'organo di controllo e del revisore;
- può richiedere informazioni e documentazione alle funzioni amministrative in merito a specifiche operazioni o aree di rischio;
- valuta eventuali anomalie, rilievi o carenze segnalate dagli organi di controllo e propone, se necessario, misure correttive del sistema di controllo interno;
- monitora eventuali segnalazioni pervenute tramite il canale WB attinenti a irregolarità amministrativo-contabili.

### **3 – SEZIONE C – REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (ART. 25-SEPTIES)**

#### **1. Le fattispecie di reato**

La presente sezione riguarda i reati di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza nei luoghi di lavoro.

Per la Società tali reati sono considerati **potenzialmente realizzabili** in relazione alle attività svolte nei propri uffici e in eventuali sedi operative o presso terzi.

#### **2. Le attività a rischio**

Costituiscono attività a rischio, in via esemplificativa:

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- l'organizzazione e la gestione degli ambienti di lavoro (sedi, uffici, aule formative);
- l'utilizzo di attrezzature di lavoro, videoterminali, dispositivi elettronici e sistemi informatici;
- le attività svolte dal personale presso sedi di terzi, clienti o partner, in particolare in occasione di eventi formativi o incontri istituzionali;
- la gestione delle emergenze, degli infortuni e dei mancati infortuni.

### **3. Regole di comportamento**

La Società si impegna a garantire il rispetto delle disposizioni del decreto legislativo 81 del 2008 e successive modifiche, attraverso:

- l'adozione e l'aggiornamento periodico del Documento di Valutazione dei Rischi;
- la nomina del Responsabile del Servizio di Prevenzione e Protezione e delle altre figure previste dalla normativa;
- la formazione, informazione e addestramento dei lavoratori in materia di salute e sicurezza;
- la fornitura di attrezzature e dispositivi di lavoro idonei e conformi alla normativa.

Tutti i destinatari del Modello sono tenuti a:

- attenersi scrupolosamente alle procedure e alle istruzioni in materia di sicurezza sul lavoro;
- utilizzare correttamente le attrezzature e i dispositivi messi a disposizione;
- segnalare tempestivamente al proprio responsabile, al RSPP o tramite il canale WB situazioni di pericolo, infortuni o mancati infortuni di cui vengano a conoscenza;
- non rimuovere o modificare senza autorizzazione dispositivi di sicurezza o segnaletica di prevenzione.

### **4. I controlli dell'Organismo di Vigilanza**

L'OdV:

- riceve flussi informativi periodici in materia di infortuni, mancati infortuni, visite ispettive e sorveglianza sanitaria;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- può esaminare, anche a campione, il Documento di Valutazione dei Rischi e la documentazione relativa alla formazione dei lavoratori;
- valuta eventuali segnalazioni pervenute tramite il canale WB in materia di salute e sicurezza sul lavoro;
- coordina le proprie attività con il Datore di lavoro, il RSPP e le altre funzioni competenti.

#### **4 – SEZIONE D – REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24-BIS)**

##### **1. Le fattispecie di reato**

Sono ricompresi in questa sezione, a titolo esemplificativo:

- l'accesso abusivo a sistemi informatici o telematici;
- l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- il danneggiamento di dati, sistemi o programmi informatici;
- la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- le condotte di illecito trattamento di dati personali penalmente rilevanti.

Tali reati sono considerati **potenzialmente realizzabili** in relazione all'intenso utilizzo di strumenti informatici e al trattamento di dati personali e sensibili connessi alle attività di agenzia per il lavoro, formazione e gestione dei rapporti con candidati, lavoratori, clienti e partner.

##### **2. Le attività a rischio**

Sono considerate attività a rischio:

- la gestione delle infrastrutture informatiche e delle reti aziendali, incluse le credenziali di accesso e i profili autorizzativi;
- l'accesso ai database contenenti dati personali di candidati, lavoratori, clienti, fornitori e altri soggetti;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- l'utilizzo di strumenti informatici da parte del personale (postazioni di lavoro, dispositivi mobili, accessi da remoto);
- la gestione della posta elettronica e dei canali di comunicazione digitale;
- le attività di sviluppo, manutenzione o configurazione di applicativi, inclusi i sistemi utilizzati per il matching domanda-offerta di lavoro e per la gestione dei bandi.

### **3. Regole di comportamento**

In aggiunta a quanto previsto dalla normativa in materia di protezione dei dati personali e dalle policy aziendali, è fatto obbligo di:

- utilizzare le risorse informatiche esclusivamente per finalità connesse all'attività lavorativa;
- custodire con diligenza le proprie credenziali di accesso, evitando la loro condivisione con terzi;
- non accedere a sistemi, dati o risorse informatiche non pertinenti alle proprie mansioni o per le quali non si disponga di apposita autorizzazione;
- non installare software non autorizzati o provenienti da fonti non verificate;
  
- non alterare, cancellare o distruggere dati o informazioni senza idonea autorizzazione e adeguata motivazione;
- segnalare tempestivamente all'ufficio competente o tramite il canale WB eventuali violazioni di sicurezza, accessi sospetti o smarrimento di dispositivi.

### **4. I controlli dell'Organismo di Vigilanza**

L'OdV:

- coordina le proprie attività con le funzioni IT e, ove presente, con il Responsabile della protezione dei dati;
- valuta i flussi informativi relativi a incidenti di sicurezza, violazioni di dati personali e anomalie nell'utilizzo dei sistemi informativi;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- può richiedere analisi e verifiche a campione sull'osservanza delle policy informatiche e di sicurezza;
- esamina eventuali segnalazioni WB relative a violazioni in materia informatica o di protezione dei dati.

**5 – SEZIONE E – REATI AMBIENTALI (ART. 25-UNDECIES)**

Considerata la natura di CREDICI S.R.L., che opera prevalentemente in ambienti d'ufficio, la commissione di reati ambientali è ritenuta **di bassa probabilità**. Non sono individuate attività a rischio specifiche ulteriori rispetto a quelle ordinarie connesse alla gestione degli immobili, dei rifiuti e dei consumi energetici.

Resta fermo l'obbligo per tutti i destinatari del Modello di:

- rispettare la normativa ambientale applicabile e le eventuali procedure aziendali in materia;
  - utilizzare in modo corretto le risorse e le infrastrutture aziendali;
  - segnalare eventuali situazioni di potenziale impatto ambientale anomalo di cui vengano a conoscenza.
- 
- L'OdV tiene conto, nell'ambito della propria attività, di eventuali rilievi o sanzioni delle autorità competenti in materia ambientale.

**6 – SEZIONE F – REATI CONTRO LA PERSONALITÀ INDIVIDUALE (ART. 25-QUINQUIES)**

La presente sezione riguarda, fra gli altri, i delitti di riduzione o mantenimento in schiavitù o in servitù, tratta di persone, sfruttamento della prostituzione minorile, pornografia minorile e altre gravi violazioni della dignità e libertà della persona.

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

Nell'ambito delle attività di agenzia per il lavoro e formazione, la Società considera tali reati **di probabilità remota**, ma presta particolare attenzione al rispetto della dignità e dei diritti fondamentali di candidati, lavoratori e destinatari dei servizi.

Sono pertanto previste, in via generale, le seguenti regole di comportamento:

- è vietata qualsiasi forma di sfruttamento, discriminazione o abuso nei confronti di persone fisiche con cui la Società interagisce;
- i rapporti con candidati e lavoratori devono essere improntati al rispetto della dignità, della libertà personale, dell'uguaglianza e delle norme a tutela dei minori;
- eventuali comportamenti che possano integrare o agevolare reati contro la personalità individuale devono essere immediatamente segnalati tramite i canali WB.
- L'OdV valuta eventuali segnalazioni o rilievi provenienti da autorità competenti o da organizzazioni di tutela dei diritti fondamentali.

**7 – SEZIONE G – RICETTAZIONE, RICICLAGGIO, AUTORICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 25-OCTIES)**

**1. Le fattispecie di reato**

Sono compresi in questa sezione i reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

Per la Società il rischio di commissione di tali reati è considerato **di bassa probabilità**, ma non del tutto escluso in relazione alla gestione dei flussi finanziari con clienti, partner e fornitori.

**2. Le attività a rischio**

Sono considerate attività a rischio:

- l'incasso di corrispettivi per servizi resi, incluse eventuali anticipazioni o contributi da parte di enti pubblici o privati;
- i pagamenti verso fornitori, consulenti e collaboratori;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- l'eventuale gestione di anticipazioni, cauzioni o altre somme per conto terzi.

### **3. Regole di comportamento**

La Società adotta procedure amministrativo-contabili tali da garantire la tracciabilità dei flussi finanziari e l'individuazione dei soggetti coinvolti nelle operazioni di incasso e pagamento.

In particolare è fatto obbligo di:

- utilizzare, di regola, strumenti di pagamento tracciabili;
- verificare la coerenza fra il soggetto che effettua il pagamento e il soggetto con cui la Società intrattiene il rapporto contrattuale;
- segnalare tempestivamente eventuali operazioni sospette o anomale alle funzioni amministrative competenti o tramite il canale WB;
- non porre in essere operazioni prive di giustificazione economica o che presentino profili di anomalia rispetto alla normale operatività.
- L'OdV può richiedere analisi a campione sulle operazioni di incasso e pagamento e valuta eventuali segnalazioni pervenute tramite i canali WB.

## **8 – SEZIONE H – REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES)**

La Società utilizza materiali didattici, software e contenuti multimediali per lo svolgimento delle proprie attività formative e di comunicazione.

È fatto obbligo di:

- utilizzare software, banche dati e materiali protetti dal diritto d'autore nel rispetto delle relative licenze d'uso;
- citare le fonti e rispettare i diritti di proprietà intellettuale di terzi;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- non riprodurre, distribuire o comunicare al pubblico opere protette senza idonea autorizzazione.
- L'OdV tiene conto di eventuali segnalazioni WB o contestazioni formali in materia di violazione del diritto d'autore.

**9 – SEZIONE I – REATI DI CRIMINALITÀ ORGANIZZATA (ART. 24-TER)**

I delitti di associazione per delinquere di tipo mafioso o comunque riconducibili alla criminalità organizzata sono ritenuti, in relazione all'attività della Società, **di probabilità remota**.

La Società si impegna comunque a verificare, nei limiti consentiti dalla legge, l'affidabilità dei partner e dei principali fornitori e a evitare rapporti consapevoli con soggetti coinvolti in fenomeni di criminalità organizzata.

L'OdV valuta eventuali informazioni o segnalazioni provenienti da fonti qualificate o dal canale WB.

**10 – SEZIONE L (1) – REATI DI FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO, VALORI DI BOLLO E STRUMENTI O SEGNI DI RICONOSCIMENTO (ART. 25-BIS)**

Considerata la natura delle attività svolte, il rischio di commissione dei reati di cui alla presente sezione è valutato **remoto**. Non sono individuate attività a rischio specifiche oltre alla gestione ordinaria degli incassi e dei pagamenti.

Resta fermo l'obbligo di segnalare eventuali casi di sospetta falsificazione di mezzi di pagamento o valori di bollo di cui la Società venga a conoscenza.

**11 – SEZIONE L (2) – REATI CONTRO L'INDUSTRIA E IL COMMERCIO (ART. 25-BIS.1)**

I reati contro l'industria e il commercio (fra cui talune ipotesi di frode nelle relazioni commerciali) sono ritenuti **di bassa probabilità** in relazione all'attività di CREDICI.

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

Si applicano, in via generale, i principi di:

- correttezza e trasparenza nelle relazioni con clienti, fornitori e partner;
- veridicità delle informazioni commerciali e promozionali;
- rispetto delle condizioni contrattuali e delle normative a tutela del mercato.

L'OdV monitora eventuali segnalazioni e contenziosi che possano evidenziare rischi in quest'area.

## **12 – SEZIONE M – DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (ART. 25-QUATER)**

I delitti con finalità di terrorismo o eversione dell'ordine democratico sono ritenuti **non compatibili** con l'oggetto sociale e l'operatività ordinaria di CREDICI.

La Società si impegna comunque a:

- non instaurare rapporti consapevoli con soggetti o organizzazioni coinvolte in fenomeni di terrorismo;
- rispettare le normative vigenti in tema di misure di prevenzione e segnalazione di operazioni sospette, ove applicabili.

## **13 – SEZIONE N – PRATICHE PER LA MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (ART. 25-QUATER.1)**

La commissione di tali reati è ritenuta **non compatibile** con le attività della Società. Eventuali condotte, anche solo sospette, rilevate nell'ambito dei rapporti con utenti, candidati o lavoratori, devono essere immediatamente segnalate tramite i canali WB e, ove necessario, alle autorità competenti.

#### **14 – SEZIONE O – ABUSI DI MERCATO (ART. 25-SEXIES D.LGS. 231 DEL 2001)**

Considerata la natura di CREDICI S.R.L., che non è società emittente strumenti finanziari quotati né fa ricorso al mercato del capitale di rischio, i reati di abuso di mercato (abuso di informazioni privilegiate e manipolazione del mercato) sono ritenuti **non compatibili** con l'operatività ordinaria della Società.

Resta fermo l'obbligo per amministratori, soci e personale di:

- astenersi dal porre in essere condotte che, in qualunque forma, possano costituire violazione della normativa in materia di abusi di mercato, qualora venissero a conoscenza di informazioni privilegiate relative a soggetti terzi (clienti, partner, fornitori);
- rispettare le regole di riservatezza e correttezza nelle relazioni con soggetti che operano sui mercati finanziari.
- L'OdV prende atto dell'assenza di specifiche aree di rischio in capo alla Società e valuta eventuali segnalazioni che dovessero emergere tramite il canale WB.

#### **15 – SEZIONE P – INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25-DECIES)**

##### **1. Le fattispecie di reato**

Rientrano in questa sezione i delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, in occasione di procedimenti penali o civili.

Per la Società tali reati sono considerati **potenzialmente realizzabili** in relazione alla gestione di contenziosi e procedimenti nei quali CREDICI sia parte o comunque interessata.

##### **2. Le attività a rischio**

Sono considerate attività a rischio:

- la gestione dei rapporti con difensori, consulenti tecnici, testimoni e altri soggetti coinvolti in procedimenti giudiziari che riguardano la Società;
- la raccolta di dichiarazioni, informazioni e documenti da utilizzare in giudizio;

- i rapporti con autorità giudiziaria, forze di polizia giudiziaria e altre autorità competenti.

### **3. Regole di comportamento**

È fatto divieto a chiunque operi in nome o per conto della Società di:

- indurre, con qualsiasi mezzo, soggetti chiamati a rendere dichiarazioni davanti all'autorità giudiziaria a non dichiarare o a rendere dichiarazioni mendaci;
- prospettare o promettere vantaggi, o minacciare svantaggi, allo scopo di influenzare il contenuto delle dichiarazioni;
- predisporre documentazione, memorie o dichiarazioni contenenti fatti non corrispondenti al vero.

Tutti i destinatari del Modello sono tenuti a:

- collaborare con i legali incaricati e con le autorità competenti in maniera leale e trasparente;
- rappresentare fatti e circostanze di cui siano a conoscenza in modo completo e veritiero;
- segnalare all'OdV o tramite canale WB eventuali pressioni o comportamenti anomali riscontrati in occasione di procedimenti giudiziari.

### **4. I controlli dell'Organismo di Vigilanza**

L'OdV può:

- ricevere informazioni in merito a procedimenti giudiziari di particolare rilievo che coinvolgono la Società;
- valutare eventuali segnalazioni di condotte anomale nella gestione dei rapporti con testimoni o altri soggetti coinvolti in procedimenti;
- formulare proposte di aggiornamento del Modello e delle procedure interne se emergono criticità nei presidi di controllo.

## **16 – SEZIONE Q – DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 25-OCTIES.1)**

### **1. Le fattispecie di reato**

La presente sezione riguarda i reati in materia di strumenti di pagamento diversi dai contanti (es. carte di credito o di pagamento, strumenti di pagamento digitali), quali l'illecita detenzione e utilizzo, la contraffazione o l'alterazione degli stessi.

Per CREDICI tali reati sono considerati **di bassa probabilità**, ma non esclusi, in relazione alla gestione di incassi e pagamenti elettronici.

### **2. Le attività a rischio**

Sono considerate attività a rischio:

- l'utilizzo di carte di credito o altri strumenti di pagamento intestati alla Società;
- la gestione di incassi elettronici da parte di clienti o utenti dei servizi;
- la gestione di eventuali rimborsi tramite strumenti di pagamento elettronici.

### **3. Regole di comportamento**

È fatto obbligo di:

- utilizzare gli strumenti di pagamento intestati alla Società esclusivamente per finalità connesse all'attività aziendale e secondo le procedure interne;
- custodire con diligenza le carte e le credenziali collegate, segnalando immediatamente lo smarrimento o il furto;
- verificare, per quanto di competenza, la coerenza tra le operazioni effettuate e le attività aziendali sottostanti.

È vietato:

- utilizzare strumenti di pagamento di terzi senza idoneo titolo o autorizzazione;
- effettuare operazioni fittizie o prive di giustificazione economica;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- alterare o falsificare strumenti di pagamento o i relativi dati identificativi.

L'OdV può richiedere verifiche a campione sulle operazioni effettuate con strumenti di pagamento elettronici e valuta eventuali segnalazioni WB in materia.

## **17 – SEZIONE R – IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25-DUODECIES)**

### **1. Le fattispecie di reato**

Rientra in questa sezione il reato di impiego di cittadini di paesi terzi il cui soggiorno nel territorio dello Stato è irregolare.

Per la natura di agenzia per il lavoro e di soggetto operante nelle politiche attive, tale area è considerata **particolarmente rilevante** per CREDICI.

### **2. Le attività a rischio**

Sono considerate attività a rischio:

- la selezione, presa in carico e gestione di candidati cittadini di paesi terzi;
- la formalizzazione di rapporti di lavoro o di somministrazione che coinvolgono lavoratori stranieri;
- le attività di supporto amministrativo ai lavoratori stranieri in relazione ai titoli di soggiorno;
- i rapporti con aziende clienti che utilizzano lavoratori stranieri.

### **3. Regole di comportamento**

È fatto obbligo alle funzioni competenti (HR, selezione, amministrazione del personale, consulenti esterni) di:

- acquisire, prima dell'instaurazione del rapporto di lavoro o di collaborazione, copia del titolo di soggiorno del cittadino di paese terzo e verificarne la **validità, integrità e coerenza** con la tipologia di attività da svolgere;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- monitorare le scadenze dei titoli di soggiorno, richiedendo per tempo al lavoratore la documentazione aggiornata;
- non dare corso all'instaurazione o alla prosecuzione di rapporti di lavoro in assenza di titolo di soggiorno valido;
- in caso di appalto o somministrazione presso aziende clienti, informare i referenti aziendali circa gli obblighi in materia di impiego di cittadini di paesi terzi e, ove applicabile, acquisire idonee dichiarazioni e documentazione;
- segnalare tempestivamente, anche tramite canale WB, eventuali situazioni di dubbia regolarità della posizione di cittadini di paesi terzi di cui vengano a conoscenza.

È vietato, in particolare:

- assumere o utilizzare in qualunque forma lavoratori privi di titolo di soggiorno valido;
- tollerare consapevolmente situazioni di irregolarità del soggiorno in contesti lavorativi riconducibili alla Società.

#### **4. I controlli dell'Organismo di Vigilanza**

L'OdV:

- riceve flussi informativi periodici dalle funzioni HR o da eventuali consulenti del lavoro in merito alla gestione di lavoratori stranieri e alla presenza di eventuali criticità documentali;
- può disporre verifiche a campione sui fascicoli del personale straniero, nel rispetto della normativa sulla protezione dei dati personali;
- valuta eventuali segnalazioni WB relative a presunte irregolarità nell'impiego di cittadini di paesi terzi e propone, se necessario, il rafforzamento dei presidi organizzativi.

Approvato per emendamento al MOG 231 con Delibera del 15.11.2025

## **18 – SEZIONE S – RAZZISMO E XENOFobia (ART. 25-TERDECIES)**

I delitti di razzismo e xenofobia, così come definiti dalla normativa penale vigente, sono ritenuti **di probabilità remota** in relazione all'operatività di CREDICI.

La Società, anche in coerenza con il proprio Codice Etico, si impegna a:

- promuovere un ambiente di lavoro fondato sul rispetto della dignità della persona e sul rifiuto di ogni forma di discriminazione, in particolare per motivi di nazionalità, razza, etnia, religione o orientamento sessuale;
- vietare qualsiasi condotta, anche solo comunicativa o simbolica, riconducibile a propaganda, istigazione o commissione di atti discriminatori o violenti per motivi razzisti o xenofobi;
- prevedere, ove opportuno, iniziative di sensibilizzazione e formazione interna sui temi dell'inclusione e del contrasto alle discriminazioni.

Eventuali comportamenti di natura discriminatoria o comunque incompatibili con tali principi devono essere immediatamente segnalati tramite i canali WB o all'OdV.

## **19 – SEZIONE T – FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI (ART. 25-QUATERDECIES)**

CREDICI non opera nel settore delle competizioni sportive o del gioco/scommessa e non gestisce apparecchi da gioco. I reati di cui alla presente sezione sono pertanto ritenuti **non compatibili** con l'attività della Società.

Resta fermo l'obbligo, per i destinatari del Modello, di astenersi dall'utilizzare il nome o le risorse della Società per porre in essere condotte riconducibili ai reati in oggetto.

Approvato per emendamento al MOG 231 con Delibera del 15.11.2025

## 20 – SEZIONE U – REATI TRIBUTARI (ART. 25-QUINQUESDECIES)

### 1. Le fattispecie di reato

Rientrano nella presente sezione i reati tributari richiamati dall'articolo 25-quinquiesdecies del decreto legislativo 231 del 2001, fra cui, a titolo esemplificativo, la dichiarazione fraudolenta, l'emissione di fatture o altri documenti per operazioni inesistenti, l'occultamento o distruzione di documenti contabili, l'omesso versamento di imposte.

Per la Società questa area di rischio è considerata **rilevante**, in relazione ai processi amministrativo-contabili e di gestione degli adempimenti fiscali.

### 2. Le attività a rischio

Sono considerate attività a rischio:

- la tenuta delle scritture contabili e della documentazione fiscale;
- la predisposizione delle dichiarazioni fiscali e degli altri adempimenti tributari;
- la gestione dei rapporti con consulenti fiscali esterni;
- la gestione dei rapporti con l'Amministrazione finanziaria e gli altri enti impositori.

### 3. Regole di comportamento

È fatto obbligo di:

- registrare tutte le operazioni rilevanti ai fini fiscali in modo completo, veritiero e tempestivo;
- conservare la documentazione contabile e fiscale per i termini previsti dalla legge, in modo da consentire la ricostruzione di ogni operazione;
- fornire ai consulenti fiscali esterni informazioni e dati completi, accurati e non fuorvianti;
- gestire eventuali verifiche fiscali nel rispetto dei principi di collaborazione, trasparenza e correttezza, previa informazione agli organi competenti interni.

È vietato:

- emettere o utilizzare fatture o altri documenti per operazioni inesistenti o per importi non corrispondenti al vero;

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

- occultare o distruggere documenti contabili o fiscali al fine di evadere le imposte o di ostacolare l'attività di accertamento;
- porre in essere operazioni prive di giustificazione economica prevalente che abbiano come principale finalità un indebito risparmio d'imposta.

#### **4. I controlli dell'Organismo di Vigilanza**

L'OdV:

- può ricevere, almeno annualmente, un'informativa sintetica sugli adempimenti fiscali più rilevanti e su eventuali rilievi o contestazioni dell'Amministrazione finanziaria;
- valuta eventuali segnalazioni WB relative a irregolarità fiscali;
- propone, se necessario, interventi di rafforzamento dei controlli interni in materia tributaria.

#### **21 – SEZIONE V – CONTRABBANDO (ART. 25-SEXIESDECIES)**

CREDICI non svolge attività di importazione, esportazione o movimentazione di merci tali da comportare rischi in materia di contrabbando. I reati di cui alla presente sezione sono pertanto ritenuti **non applicabili** rispetto all'operatività della Società.

È comunque fatto divieto di utilizzare la struttura o il nome della Società per porre in essere, anche indirettamente, condotte riconducibili ai reati di contrabbando.

#### **22 – SEZIONE Y – DELITTI CONTRO IL PATRIMONIO CULTURALE (ART. 25-SEPTIESDECIES)**

I delitti contro il patrimonio culturale sono ritenuti **non compatibili** con l'oggetto sociale e l'attività ordinaria di CREDICI.

È fatto divieto ai destinatari del Modello di utilizzare il nome o le risorse della Società per porre in essere condotte riconducibili ai delitti contro il patrimonio culturale.

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

Eventuali situazioni anomale di cui i destinatari venissero a conoscenza devono essere segnalate tramite i canali WB.

**23 – SEZIONE Z – DELITTI CONTRO GLI ANIMALI (ART. 25-UNDEVICIES)**

I delitti contro gli animali sono ritenuti **non compatibili** con l'attività della Società, che non opera in settori direttamente collegati alla gestione o utilizzo di animali.

Resta fermo l'obbligo, per tutti i destinatari del Modello, di astenersi dal porre in essere, anche al di fuori dell'ambito lavorativo ma utilizzando il nome o le risorse della Società, condotte riconducibili ai reati in oggetto.

**RIFERIMENTI E COORDINAMENTO**

La presente Parte Speciale viene emendata con delibera di emendamento al MOG 231 di CREDICI S.R.L. del 15.11.2025 ed è immediatamente efficace e vincolante, inoltre, deve essere letta ed applicata in coordinamento con:

- la **Parte Generale** del Modello 231 di CREDICI S.R.L.;
- il **Codice Etico** della Società;
- il **Regolamento Whistleblowing di CREDICI S.R.L.**;
- Lo **statuto** ed il **Regolamento dell'Organismo di Vigilanza**;
- le ulteriori procedure, regolamenti e policy interne adottate dalla Società nei diversi ambiti (amministrazione e finanza, salute e sicurezza sul lavoro, privacy, gestione del personale, rapporti con la Pubblica Amministrazione, gestione dei bandi e dei progetti, IT e sicurezza informatica).

In caso di contrasto tra le previsioni della presente Parte Speciale e quelle di documenti successivamente approvati dalla Società, prevalgono le disposizioni più aggiornate, fermo restando l'obbligo di adeguare tempestivamente il Modello 231.

**Approvato per emendamento al MOG 231 con Delibera del 15.11.2025**

La presente Parte Speciale è soggetta a periodico aggiornamento, su proposta dell'OdV o delle funzioni competenti, in relazione a:

- modifiche normative, in particolare del decreto legislativo 231 del 2001 e delle discipline richiamate;
- variazioni dell'assetto organizzativo o delle attività della Società;
- esiti delle attività di controllo, delle segnalazioni e dei procedimenti disciplinari o giudiziari che evidenzino criticità nei presidi di prevenzione dei reati presupposto.