# CYBER EVOLUTION S.r.l.

# MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del D.Lgs. 8 giugno 2001, n. 231

Parte Generale - Parte Speciale - Risk Assessment - Sistema disciplinare - OdV

Versione 0.2 - 26 giugno 2026

Sede legale: Via Erasmo Mari 57/S/Q - 63100 Ascoli Piceno (AP)
P. IVA 02353440445

# Indice

# PARTE GENERALE

## 1. Finalità, destinatari e campo di applicazione

Il Modello è adottato con l'obiettivo di prevenire i reati dai quali possa derivare responsabilità amministrativa di Cyber Evolution S.r.l., promuovere una cultura aziendale improntata a legalità, correttezza, trasparenza, tracciabilità e responsabilità, nonché definire un sistema organico di controlli, responsabilità e flussi informativi.

### 1.1 Destinatari

- componenti dell'organo amministrativo e degli eventuali organi di controllo;
- dirigenti, responsabili di funzione e soggetti apicali di fatto;
- dipendenti, stagisti e collaboratori;
- consulenti, agenti, distributori, reseller, system integrator, fornitori, subfornitori e partner, nei limiti delle attività svolte per o con Cyber Evolution;
- soggetti che operano nell'ambito di PoC, installazioni, supporto tecnico, R&D, sviluppo software, servizi cloud o attività presso clienti.

### 1.2 Principio di prevalenza della sostanza

I controlli previsti dal Modello si applicano sulla base dell'attività concretamente svolta e non esclusivamente della qualifica formale del soggetto. Le funzioni indicate nel presente documento devono essere lette come funzioni organizzative o responsabilità equivalenti, da allineare all'organigramma aziendale vigente.

## 2. Quadro normativo D.Lgs. 231/2001

### 2.1 Presupposti della responsabilità dell'ente

La responsabilità dell'ente può sorgere quando uno dei reati presupposto è commesso, nell'interesse o a vantaggio dell'ente, da soggetti in posizione apicale oppure da persone sottoposte alla direzione o vigilanza di questi ultimi. La responsabilità dell'ente è distinta da quella personale dell'autore del reato.

### 2.2 Modello organizzativo ed esimente

Per i reati commessi da soggetti apicali, il sistema 231 attribuisce rilievo all'adozione e all'efficace attuazione, prima del fatto, di un modello idoneo a prevenire reati della specie verificatasi; alla presenza di un organismo dotato di autonomi poteri di iniziativa e controllo; all'elusione fraudolenta del modello; e all'assenza di omessa o insufficiente vigilanza. Per i soggetti sottoposti, assume rilievo l'adeguatezza del sistema di direzione e vigilanza.

### 2.3 Sanzioni

- sanzioni pecuniarie, determinate mediante il sistema delle quote;
- sanzioni interdittive, nei casi previsti dalla legge;
- confisca del prezzo o profitto del reato, anche per equivalente nei limiti consentiti;
- pubblicazione della sentenza nei casi previsti.

### 2.4 Catalogo dei reati presupposto

La società mantiene un elenco normativo aggiornato delle fattispecie rilevanti. Ai fini del presente risk assessment le famiglie sono valutate in rapporto ai processi aziendali e non vengono considerate tutte automaticamente “a rischio” allo stesso livello.

## 3. Profilo e sistema di governance di Cyber Evolution

### 3.1 Profilo operativo

Cyber Evolution S.r.l. sviluppa e commercializza tecnologia di cybersecurity proprietaria LECS. La società opera in un contesto ad alta intensità tecnologica, con attività di ricerca e sviluppo, produzione/assemblaggio o approvvigionamento di componenti hardware, sviluppo software e firmware, servizi e supporto tecnico, commercializzazione tramite canali diretti e indiretti, relazioni con clienti privati e pubblici e operatività internazionale.

### 3.2 Struttura di controllo da validare

| Area | Responsabilità di riferimento | Presidio minimo 231 |
|---|---|---|
| Governance | Organo amministrativo / CEO | Approvazioni, conflitti di interesse, procure, reporting OdV |
| Amministrazione e finanza | CEO / CFO / amministrazione | Pagamenti, incassi, fiscalità, contributi, segregazione e riconciliazioni |
| Commerciale e canale | Sales / Channel | Offerte, sconti, partner, PA, regali/ospitalità, due diligence |
| Procurement e supply chain | Acquisti / Operations | Vendor onboarding, import, origine merci, qualità, tracciabilità |
| R&D e sviluppo | CTO / R&D | Secure SDLC, licenze, IP, accessi, repository, componenti open source |
| IT e sicurezza | CISO/IT o equivalente | IAM, logging, segregazione privilegi, incident handling, asset management |
| HR | HR / amministrazione | Selezione, contratti, permessi, formazione, disciplina |
| HSE | Datore di lavoro/RSPP | DVR, formazione, DPI, appalti e sicurezza luoghi di lavoro |
| Privacy | DPO/privacy owner se nominato | GDPR, data governance, rapporti con clienti e fornitori |
| Legal/compliance | Legale/compliance o consulente | Contratti, contenzioso, export/sanzioni, aggiornamento normativo |

### 3.3 Principi di segregazione

- nessun soggetto dovrebbe poter avviare, approvare, eseguire e contabilizzare autonomamente la stessa operazione significativa;
- le deroghe per organizzazioni snelle devono essere compensate da controlli ex post documentati dell’organo amministrativo;
- le deleghe devono essere coerenti con le responsabilità, i poteri di spesa e le competenze;
- operazioni fuori standard, urgenti o ad alto rischio richiedono approvazione rafforzata e motivazione.

# 4. Metodologia di risk assessment

Il risk assessment 231 è organizzato per processi e per famiglie di reato. La valutazione preliminare considera: esposizione intrinseca del processo; possibilità che il reato sia commesso nell'interesse o vantaggio della società; frequenza delle operazioni; rilevanza economica; presenza di terze parti; componente internazionale; accesso a sistemi e dati; grado di discrezionalità; robustezza dei controlli esistenti.

## 4.1 Scala di valutazione

| Livello | Definizione | Trattamento |
|---|---|---|
| ALTO | Processo direttamente connesso a fattispecie 231 e/o caratterizzato da elevata discrezionalità, valore, esposizione PA/internazionale o accessi privilegiati. | Protocollo specifico, owner, evidenze, monitoraggio OdV periodico. |
| MEDIO | Rischio concretamente configurabile ma mitigabile con controlli standardizzati e segregazione. | Procedure documentate, controlli periodici e flussi per eccezioni. |
| BASSO | Rischio astratto o residuale rispetto all'attività corrente. | Principi generali, monitoraggio normativo e rivalutazione in caso di cambiamenti. |
| NON RILEVANTE / REMOTO | Nessun processo aziendale ordinario appare idoneo a realizzare il fatto nell'interesse/vantaggio dell'ente. | Nessun protocollo dedicato; resta applicabile il Codice Etico. |

## 4.2 Validazione del rischio

La matrice allegata è preliminare. La versione da sottoporre ad adozione deve essere validata tramite interviste ai process owner e campionamento di evidenze: contratti, ordini, fatture, workflow di approvazione, repository, ticket, registri accessi, documenti import/export, pratiche PA, bandi, gestione contributi, documenti HSE, procedure privacy e sicurezza.

# 5. Sistema dei controlli preventivi

### Tracciabilità

Ogni operazione sensibile deve essere documentata in modo da consentire ricostruzione di soggetti, autorizzazioni, motivazioni, importi e documenti di supporto.

### Segregazione

Separazione, ove possibile, tra chi richiede, autorizza, esegue e controlla. Nelle strutture snelle si adottano controlli compensativi.

### Poteri autorizzativi

Procure, deleghe e limiti di spesa devono essere coerenti, aggiornati e conoscibili.

### Controllo di terze parti

Onboarding proporzionato al rischio; verifica identità, titolarità, reputazione, conflitti, sanzioni, condizioni economiche e prestazioni effettive.

### Controlli finanziari

Pagamenti tracciabili, conti intestati alla controparte contrattuale, causali coerenti, divieto di fondi occulti o contabilità extracontabile.

### Controlli IT

Principio del minimo privilegio, MFA ove appropriata, logging, gestione credenziali, change management, backup, vulnerability management e segregazione ambienti.

### Gestione eccezioni

Eccezioni motivate, approvate da livello superiore e conservate per verifiche OdV.

## 6. Codice Etico e principi di comportamento

Il Codice Etico costituisce parte integrante del sistema 231 e deve essere coerente con il presente Modello. In coerenza con il Codice Etico, si applicano i seguenti principi minimi: legalità; integrità; trasparenza; correttezza nei rapporti con PA e privati; tutela di dati, sistemi e proprietà intellettuale; concorrenza leale; accuratezza di comunicazioni commerciali e tecniche; tutela della salute e sicurezza; rispetto dell'ambiente; non discriminazione; gestione dei conflitti; tracciabilità dei flussi finanziari; divieto di ritorsioni verso segnalanti.

### 6.1 Divieti specifici

- promettere o offrire utilità indebite a pubblici ufficiali, clienti, partner o altri soggetti per ottenere vantaggi impropri;
- alterare documenti, dati, log, certificazioni, report tecnici, dichiarazioni o evidenze di progetto;
- accedere a sistemi, reti, dati o credenziali oltre l'autorizzazione ricevuta, anche durante PoC o attività di supporto;
- utilizzare software, librerie, dataset, codice, brevetti, marchi o materiali in violazione di diritti di terzi o licenze;
- effettuare pagamenti a soggetti diversi dalla controparte senza valida motivazione e verifica;
- aggirare misure restrittive UE, controlli export, vincoli doganali o procedure di origine/etichettatura;
- occultare incidenti, non conformità o violazioni rilevanti ai fini del Modello.

## 7. Organismo di Vigilanza

### 7.1 Principi generali e requisiti

In attuazione di quanto previsto dall'art. 6 del Decreto Legislativo 8 giugno 2001, n. 231, Cyber Evolution S.r.l. istituisce un Organismo di Vigilanza, di seguito anche "OdV", cui è affidato il compito di vigilare sul funzionamento, sull'osservanza e sull'effettiva attuazione del presente Modello di Organizzazione, Gestione e Controllo, nonché di curarne l'aggiornamento mediante la formulazione di proposte e segnalazioni all'organo amministrativo.

L'OdV deve essere dotato, in relazione alle dimensioni, alla struttura organizzativa, alla natura delle attività e al profilo di rischio della Società, dei seguenti requisiti:

- **autonomia e indipendenza**, da intendersi quale assenza di condizionamenti gerarchici o operativi nell'esercizio delle funzioni di vigilanza e quale possibilità di riferire direttamente all'organo amministrativo;
- **professionalità**, intesa quale possesso di competenze adeguate in materia giuridica, societaria, organizzativa, amministrativa, di controllo interno, gestione dei rischi e, ove necessario, tecnica;
- **continuità d'azione**, assicurata attraverso una programmazione periodica delle attività di verifica, adeguati flussi informativi e la possibilità di accedere direttamente alle informazioni aziendali rilevanti;
- **onorabilità**, secondo criteri coerenti con la natura dell'incarico;
- **assenza di conflitti di interesse**, effettivi o potenziali, tali da compromettere l'obiettività e l'indipendenza dell'attività di vigilanza.

L'OdV opera in posizione di autonomia rispetto alle strutture operative della Società e non è titolare di poteri gestionali o decisionali relativi allo svolgimento delle attività aziendali sottoposte alla propria vigilanza.

L'OdV non sostituisce gli organi amministrativi, le funzioni aziendali o gli eventuali ulteriori soggetti cui la normativa attribuisce specifiche responsabilità di controllo, ma esercita una funzione autonoma di vigilanza sull'adeguatezza e sull'effettiva attuazione del Modello.

## 7.2 Composizione

Tenuto conto delle dimensioni e dell'assetto organizzativo di Cyber Evolution S.r.l., l'Organismo di Vigilanza può essere costituito in forma **monocratica** oppure, qualora l'evoluzione dimensionale, organizzativa o del profilo di rischio della Società lo renda opportuno, in forma **collegiale**.

La Società può affidare l'incarico a un professionista esterno in possesso dei necessari requisiti di autonomia, indipendenza, professionalità e onorabilità.

Può essere nominato quale componente dell'OdV anche un professionista che svolga ulteriori incarichi di controllo, verifica o revisione nei confronti della Società, purché tali incarichi siano compatibili con la funzione di Organismo di Vigilanza e non determinino situazioni di conflitto di interesse, autoriesame o compromissione dell'autonomia e dell'indipendenza richieste.

La sussistenza dei requisiti deve essere valutata all'atto della nomina e permanere per tutta la durata dell'incarico.

L'OdV può inoltre avvalersi, sotto la propria responsabilità e nell'ambito delle risorse attribuitegli, di consulenti o specialisti esterni per lo svolgimento di verifiche che richiedano competenze specifiche.

## 7.3 Nomina e accettazione dell'incarico

L'Organismo di Vigilanza è nominato dall'organo amministrativo mediante apposita deliberazione.

La deliberazione di nomina determina almeno:

- il soggetto o i soggetti nominati;
- la durata dell'incarico;
- il compenso, ove previsto;
- le risorse economiche attribuite all'OdV;
- i poteri di iniziativa, accesso e controllo;
- gli obblighi di reporting;
- le eventuali ulteriori condizioni per lo svolgimento dell'incarico.

Prima dell'accettazione dell'incarico, il soggetto individuato deve dichiarare l'assenza di cause di ineleggibilità, incompatibilità o conflitto di interesse rilevanti ai fini dello svolgimento della funzione.

Qualora il soggetto nominato ricopra già altri incarichi professionali nei confronti della Società, egli deve inoltre valutare e dichiarare la compatibilità di tali incarichi con la funzione di OdV e il permanere dei requisiti di autonomia e indipendenza richiesti.

L'avvenuta nomina dell'OdV e i relativi riferimenti devono essere portati a conoscenza del personale e dei soggetti interessati con modalità adeguate.

## 7.4 Durata dell'incarico

L'Organismo di Vigilanza resta in carica per il periodo stabilito dall'organo amministrativo nella deliberazione di nomina.

Salvo diversa determinazione motivata, la durata dell'incarico è stabilita in **tre esercizi**, con possibilità di rinnovo.

Alla scadenza, l'OdV continua a esercitare le proprie funzioni sino alla nomina del nuovo Organismo per il tempo strettamente necessario ad assicurare la continuità della funzione di vigilanza.

In caso di cessazione anticipata dall'incarico, l'organo amministrativo provvede alla sostituzione in tempi compatibili con l'esigenza di garantire la continuità dell'attività di vigilanza.

## 7.5 Cause di ineleggibilità, decadenza, rinuncia e revoca

Non possono essere nominati quali componenti dell'OdV, e decadono dall'incarico qualora la relativa circostanza sopravvenga, i soggetti che si trovino in condizioni tali da compromettere in maniera significativa i requisiti di onorabilità, autonomia e indipendenza richiesti dalla funzione.

Costituiscono, a titolo esemplificativo, circostanze da sottoporre a valutazione:

- la presenza di conflitti di interesse rilevanti e non eliminabili;

- l'assunzione di funzioni operative o gestionali incompatibili con il ruolo di vigilanza;
- la perdita dei requisiti di professionalità o indipendenza richiesti;
- gravi inadempimenti rispetto ai compiti attribuiti all'OdV;
- violazioni degli obblighi di riservatezza;
- impedimenti permanenti o comunque tali da rendere impossibile lo svolgimento effettivo dell'incarico.

La revoca dell'OdV prima della scadenza deve essere deliberata dall'organo amministrativo per **giusta causa** e adeguatamente motivata.

L'OdV può rinunciare all'incarico mediante comunicazione scritta all'organo amministrativo, assicurando, ove possibile, un congruo periodo di preavviso al fine di consentire la propria sostituzione.

## 7.6 Compiti dell'Organismo di Vigilanza

All'OdV sono affidati, in particolare, i seguenti compiti:

a) vigilare sull'effettiva applicazione e osservanza del Modello da parte dei suoi Destinatari;

b) verificare periodicamente l'adeguatezza del Modello rispetto alla struttura organizzativa e alle attività concretamente svolte dalla Società;

c) valutare l'effettiva capacità del Modello e dei relativi protocolli di prevenire o ridurre i rischi di commissione dei reati rilevanti ai sensi del D.Lgs. 231/2001;

d) predisporre e attuare un programma periodico delle attività di vigilanza, individuando le aree e i processi maggiormente rilevanti;

e) effettuare verifiche, anche a campione, sui processi sensibili e sulla corretta applicazione delle procedure e dei controlli previsti dal Modello;

f) acquisire e analizzare le informazioni e la documentazione necessarie allo svolgimento delle proprie funzioni;

g) verificare l'attuazione delle misure correttive individuate a seguito di anomalie, criticità o violazioni;

h) ricevere e valutare i flussi informativi previsti dal Modello;

i) coordinarsi, quando necessario, con le funzioni aziendali interessate, fermo restando il mantenimento della propria autonomia;

j) segnalare tempestivamente all'organo amministrativo eventuali violazioni rilevanti del Modello o situazioni che possano determinare significative esposizioni al rischio;

k) formulare proposte di aggiornamento o adeguamento del Modello in conseguenza di modifiche legislative, organizzative, societarie, operative o dell'emersione di nuovi rischi;

l) verificare, per quanto di propria competenza, che siano programmate adeguate attività di informazione e formazione in materia di D.Lgs. 231/2001 e sul contenuto del Modello;

m) documentare le attività di vigilanza svolte e conservarne adeguata evidenza.

L'OdV non assume responsabilità operative relativamente alla progettazione, esecuzione o gestione ordinaria dei processi aziendali sottoposti alla propria vigilanza.

## 7.7 Poteri e accesso alle informazioni

Per lo svolgimento dei propri compiti, l'OdV dispone di autonomi poteri di iniziativa, accesso e controllo.

In particolare, l'OdV può:

- accedere, senza necessità di preventiva autorizzazione delle singole funzioni interessate, alla documentazione e alle informazioni aziendali rilevanti ai fini dell'attività di vigilanza;
- richiedere informazioni, chiarimenti e documenti agli amministratori, ai dipendenti, ai collaboratori e, nei limiti contrattualmente previsti, ai consulenti e ai soggetti terzi che intrattengono rapporti con la Società;
- effettuare verifiche e approfondimenti sui processi e sulle operazioni aziendali;
- convocare o richiedere incontri con i responsabili delle diverse funzioni;
- richiedere l'adozione di azioni correttive, sottoponendo all'organo amministrativo le eventuali criticità non adeguatamente risolte;
- avvalersi di professionisti o specialisti esterni quando le verifiche richiedano competenze specifiche.

Tutte le funzioni e i destinatari del Modello sono tenuti a collaborare con l'OdV e a fornire tempestivamente le informazioni richieste, nel rispetto della normativa applicabile e degli obblighi di riservatezza.

L'OdV non può subire limitazioni ingiustificate nell'esercizio dei propri poteri di vigilanza.

## 7.8 Risorse e budget

L'organo amministrativo assicura all'OdV risorse economiche e organizzative adeguate allo svolgimento autonomo ed effettivo dei propri compiti.

A tal fine può essere attribuito all'OdV un **budget annuale di spesa**, determinato con la delibera di nomina o mediante successiva deliberazione dell'organo amministrativo.

L'OdV può utilizzare il budget assegnato, nei limiti stabiliti, senza necessità di preventiva autorizzazione per ogni singola spesa, fermo restando l'obbligo di rendicontazione.

Qualora, nel corso dell'attività di vigilanza, emergano esigenze straordinarie che richiedano risorse superiori al budget attribuito, l'OdV ne dà tempestiva comunicazione all'organo amministrativo.

Nei casi di particolare necessità e urgenza, deve essere assicurata all'OdV la possibilità di richiedere tempestivamente le ulteriori risorse necessarie allo svolgimento di verifiche o approfondimenti non differibili.

L'assenza o l'esiguità ingiustificata delle risorse economiche non deve costituire un limite all'effettivo esercizio delle funzioni dell'Organismo.

## 7.9 Flussi informativi verso l'Organismo di Vigilanza

L'efficacia dell'attività dell'OdV è assicurata mediante l'istituzione di adeguati flussi informativi, periodici e ad evento.

Devono essere trasmesse all'OdV, secondo modalità e periodicità definite dal Modello, dalle procedure aziendali o dall'OdV stesso, le informazioni rilevanti relative almeno a:

- modifiche significative della struttura societaria o organizzativa;
- modifiche delle deleghe, procure e responsabilità aziendali rilevanti;
- operazioni o attività caratterizzate da particolare rilevanza o anomalia rispetto ai processi sensibili;
- rapporti significativi con la Pubblica Amministrazione;
- partecipazione a gare, procedure di affidamento, finanziamenti, contributi o agevolazioni pubbliche, ove rilevanti;
- contestazioni, procedimenti o richieste provenienti da autorità pubbliche, giudiziarie, amministrative o di vigilanza che possano avere rilevanza ai fini del D.Lgs. 231/2001;
- violazioni accertate o sospette del Modello, del Codice Etico o delle procedure rilevanti ai fini 231;
- procedimenti disciplinari e relativi provvedimenti aventi rilievo rispetto al Modello;
- incidenti o eventi significativi in materia di salute e sicurezza sul lavoro;
- anomalie o criticità significative in materia fiscale, amministrativa e contabile;
- eventi significativi in materia ambientale, ove applicabili;
- esiti rilevanti di audit, verifiche, certificazioni e attività di controllo;
- modifiche sostanziali dei processi aziendali o introduzione di nuove attività potenzialmente rilevanti ai fini del Decreto;
- operazioni societarie straordinarie;
- ulteriori eventi individuati dall'OdV sulla base dell'evoluzione del profilo di rischio della Società.

L'OdV può definire mediante proprio regolamento, piano di vigilanza o specifiche comunicazioni il contenuto, la frequenza, i responsabili e le modalità di trasmissione dei flussi informativi.

I flussi devono essere sufficientemente documentati e conservati in modo tale da consentire la ricostruzione delle attività di vigilanza.

Le informazioni acquisite dall'OdV sono trattate nel rispetto dei principi di riservatezza e della normativa applicabile in materia di protezione dei dati personali.

## 7.10 Segnalazioni e coordinamento con il sistema di whistleblowing

L'Organismo di Vigilanza riceve le informazioni e le segnalazioni di propria competenza attraverso i canali individuati dalla Società.

Il sistema dei flussi informativi verso l'OdV deve essere coordinato con l'eventuale sistema interno di segnalazione delle violazioni adottato dalla Società ai sensi della normativa vigente in materia di whistleblowing.

Qualora la gestione del canale di segnalazione sia affidata a un soggetto diverso dall'OdV, devono essere definiti adeguati flussi informativi verso l'OdV con riferimento alle segnalazioni che presentino profili rilevanti ai fini del D.Lgs. 231/2001, nel rispetto degli obblighi di riservatezza e delle tutele previste dalla normativa applicabile.

L'OdV tratta le informazioni ricevute secondo criteri di riservatezza, imparzialità e tutela delle persone coinvolte.

## 7.11 Riunioni, attività e verbalizzazione

L'OdV svolge la propria attività con periodicità adeguata alle caratteristiche e al profilo di rischio della Società.

In caso di OdV monocratico, il componente documenta le proprie attività attraverso verbali, report, note di verifica o altra documentazione idonea a consentire la tracciabilità delle attività svolte.

L'OdV si riunisce o formalizza le proprie verifiche **almeno con cadenza trimestrale**, ferma restando la possibilità di intervenire in qualsiasi momento qualora emergano circostanze che richiedano un'immediata attività di vigilanza.

Le attività svolte devono risultare da apposita documentazione contenente, ove applicabile:

- data e oggetto della verifica;
- documentazione esaminata;
- soggetti coinvolti;
- attività effettuate;
- eventuali criticità riscontrate;
- azioni correttive richieste o raccomandate;
- termini e modalità di successivo follow-up.

La documentazione dell'OdV è conservata con modalità tali da garantirne integrità, disponibilità e riservatezza e con accesso limitato ai soggetti autorizzati.

L'OdV può dotarsi di un proprio regolamento interno volto a disciplinare nel dettaglio modalità operative, programmazione delle attività, verbalizzazione, gestione dei flussi e conservazione della documentazione.

## 7.12 Reporting all'organo amministrativo

L'Organismo di Vigilanza riferisce direttamente all'organo amministrativo della Società.

Con cadenza almeno **annuale**, l'OdV predispone una relazione sull'attività svolta contenente, almeno:

- le attività di vigilanza e le verifiche effettuate;
- lo stato di attuazione del programma di vigilanza;
- le principali evidenze emerse;
- le eventuali violazioni o criticità riscontrate;
- lo stato delle azioni correttive richieste;
- le eventuali proposte di aggiornamento del Modello;
- una valutazione dell'adeguatezza dei flussi informativi ricevuti;
- l'utilizzo delle risorse economiche attribuite, ove rilevante;
- il programma delle principali attività previste per il periodo successivo.

Ferma restando la rendicontazione periodica, l'OdV informa tempestivamente l'organo amministrativo qualora rilevi:

- violazioni significative del Modello;
- situazioni di particolare gravità o urgenza;
- ostacoli o limitazioni all'esercizio della propria attività;
- carenze significative dei controlli;
- mancata attuazione delle azioni correttive ritenute necessarie;
- circostanze che possano comportare un rilevante incremento del rischio di commissione di reati presupposto.

Qualora le circostanze oggetto della comunicazione coinvolgano direttamente uno o più componenti dell'organo amministrativo, l'OdV adotta modalità di comunicazione idonee a preservare l'autonomia, la riservatezza e l'efficacia dell'attività di vigilanza, informando i soggetti societari competenti secondo l'assetto di governance concretamente esistente.

## 7.13 Rapporti con le funzioni aziendali e aggiornamento del Modello

L'Organismo di Vigilanza mantiene rapporti con le funzioni aziendali interessate ai processi rilevanti ai fini del D.Lgs. 231/2001 e può richiedere la loro collaborazione nello svolgimento delle proprie attività.

La responsabilità dell'adozione e dell'aggiornamento del Modello rimane in capo all'organo amministrativo.

L'OdV, nell'ambito delle proprie funzioni, segnala all'organo amministrativo la necessità o l'opportunità di aggiornare il Modello quando rilevi, tra l'altro:

- modifiche della normativa rilevante;
- introduzione di nuovi reati presupposto;
- modifiche significative della struttura societaria o organizzativa;
- avvio di nuove attività o modifica sostanziale dei processi esistenti;
- violazioni significative o reiterate del Modello;
- carenze o inadeguatezze dei protocolli di prevenzione;
- evoluzioni del contesto di rischio della Società.

Spetta all'organo amministrativo valutare e approvare le modifiche del Modello, avvalendosi, ove necessario, delle competenti funzioni interne o di consulenti esterni.

### 7.14 Riservatezza

L'OdV è tenuto alla massima riservatezza in ordine alle informazioni acquisite nell'esercizio delle proprie funzioni.

Le informazioni e la documentazione acquisite possono essere utilizzate esclusivamente per le finalità connesse all'esercizio dei compiti attribuiti all'Organismo, fatti salvi gli obblighi previsti dalla legge.

Tale obbligo permane anche successivamente alla cessazione dell'incarico.

## 8. Flussi informativi e reporting verso l'OdV

Le funzioni trasmettono flussi periodici e ad evento. L'obiettivo non è sovraccaricare l'OdV, ma far emergere anomalie, operazioni sensibili e indicatori di rischio.

| Evento / flusso | Owner indicativo | Frequenza |
|---|---|---|
| Gare PA, affidamenti, contributi e finanziamenti pubblici | Sales/Finance/Legal | Trimestrale + evento significativo |
| Nuovi distributori/agenti in paesi esteri o ad alto rischio | Sales/Legal | Prima dell'onboarding + annuale |
| Operazioni doganali, contestazioni origine/etichettatura | Operations/Finance | Trimestrale + evento |
| Contenziosi, indagini, ispezioni, richieste autorità | Legal/CEO | Immediata |
| Violazioni cyber, accessi anomali o incidenti con profilo illecito | CISO/IT | Immediata |
| Violazioni IP/licenze o contestazioni copyright | R&D/Legal | Immediata |
| Scostamenti fiscali rilevanti, ravvedimenti, verifiche | Finance | Trimestrale + evento |

| | | |
|---|---|---|
| Infortuni e near miss significativi | HSE/RSPP | Immediata + semestrale |
| Whistleblowing rilevante 231 | Gestore WB | Secondo protocollo di raccordo |
| Violazioni del Modello e sanzioni disciplinari | HR/Legal | Semestrale + evento grave |

# 9. Whistleblowing

Il sistema interno di segnalazione deve essere coordinato con il D.Lgs. 24/2023 e con le linee guida ANAC applicabili. Il canale deve garantire riservatezza, tutela da ritorsioni, gestione diligente e tracciabile e accessibilità ai soggetti legittimati. Devono essere previste segnalazioni in forma scritta e orale secondo i requisiti applicabili.

## 9.1 Raccordo con l'OdV

Se il gestore del canale whistleblowing è diverso dall'OdV, la procedura definisce quali informazioni rilevanti ai fini 231 devono essere trasmesse all'OdV, con salvaguardia della riservatezza e dei principi di minimizzazione. Se l'OdV è gestore del canale, devono essere distinti i compiti di gestione della segnalazione e di vigilanza sul Modello.

## 9.2 Divieto di ritorsione

Sono vietati atti ritorsivi o discriminatori collegati, direttamente o indirettamente, a una segnalazione protetta. Le violazioni delle misure di tutela e gli abusi del canale sono soggetti al sistema disciplinare nei limiti di legge.

# 10. Formazione e comunicazione

| Destinatari | Contenuti minimi | Periodicità |
|---|---|---|
| Organo amministrativo e apicali | Responsabilità 231, deleghe, OdV, rischi PA/fiscali/corporate, sanzioni UE | All'adozione + annuale |
| Sales/Channel | PA, anticorruzione, partner, regali, sanzioni/export, dichiarazioni commerciali | Annuale |
| Finance/Admin | Fiscale, pagamenti, contributi, riciclaggio, contabilità e tracciabilità | Annuale |
| R&D/IT/Security | Cybercrime, accessi, IP, copyright, licenze, secure development e logging | Annuale |
| Operations/Procurement | Fornitori, import, dogane, origine, ambiente/RAEE, terze parti | Annuale |
| HR/HSE | Sicurezza lavoro, immigrazione, disciplina, whistleblowing | Annuale |
| Nuovi assunti | Codice Etico, Modello, canali di segnalazione | Onboarding |

# 11. Sistema disciplinare e sanzionatorio

La violazione del Modello, dei protocolli 231, del Codice Etico, degli obblighi di flusso verso l'OdV o delle regole whistleblowing costituisce illecito disciplinare o inadempimento contrattuale, indipendentemente dall'avvio o dall'esito di un procedimento penale. Le misure devono rispettare legge, CCNL applicabile, proporzionalità e diritto di difesa.

### 11.1 Criteri di graduazione

- intenzionalità o grado di colpa;
- rilevanza della regola violata e livello di responsabilità;
- esposizione della società a rischio 231 o danno;
- reiterazione;
- eventuale occultamento, falsificazione o ostacolo ai controlli;
- collaborazione nella ricostruzione e tempestiva segnalazione spontanea.

### 11.2 Categorie di destinatari

Per dipendenti si applicano le misure previste dal sistema disciplinare e dal CCNL. Per dirigenti e apicali sono previste misure coerenti con il rapporto. Per amministratori, sindaci o organi equivalenti, l'OdV segnala la violazione all'organo competente per i provvedimenti societari. Per terze parti si applicano clausole di sospensione, rimedio, risoluzione, manleva e/o audit in base a gravità e contratto.

## 12. Aggiornamento del Modello

Il Modello è riesaminato almeno annualmente e comunque in caso di: modifiche normative; nuovi reati presupposto; variazioni significative di business o governance; ingresso in nuovi paesi/mercati; acquisizioni; nuovi prodotti o servizi; incidenti o violazioni significative; rilievi OdV; mutamenti di processi, sistemi informativi o supply chain.

# PARTE SPECIALE

## 13. Mappa dei processi sensibili e sintesi dei rischi

| Processo | Famiglie 231 | Rischio prelim. | Razionale |
|---|---|---|---|
| Rapporti con PA, gare, bandi, contributi | Artt. 24, 25; reati contro PA | ALTO | Dichiarazioni, requisiti, spese rendicontate, contatti con funzionari, affidamenti, contributi R&D. |
| Sviluppo software, R&D, accesso a reti/sistemi | Art. 24-bis; art. 25-novies | ALTO | Accessi autorizzati, strumenti dual-use, credenziali, codice, malware/tooling, licenze e copyright. |
| Vendite e partner/distributori internazionali | Artt. 25, 24-ter, 25-octies, 25-octies.2 | ALTO | Due diligence, commissioni, paesi/controparti, sanzioni UE, intermediazione e pagamenti. |
| Fiscalità, bilancio e operazioni societarie | Artt. 25-ter, 25-quinquiesdecies | ALTO | Bilancio, imposte, fatture, crediti, operazioni sul capitale, documentazione. |
| Import/export hardware e supply chain | Artt. 25-bis.1, 25-sexiesdecies, 25-octies.2 | ALTO | Origine, etichettatura, dogane, classificazione, fornitori extra-UE, sanzioni. |
| Marketing, marchi, claim tecnici e Made in Italy | Artt. 25-bis, 25-bis.1 | MEDIO-ALTO | Veridicità, origine, marchi, concorrenza, caratteristiche di prodotto. |
| Pagamenti, tesoreria, strumenti digitali | Artt. 25-octies, 25-octies.1 | MEDIO | IBAN, beneficiari, tracciabilità, frodi, segregazione, riconciliazioni. |
| Salute e sicurezza | Art. 25-septies | MEDIO | Uffici/lab, attività tecniche, trasferte, installazioni presso clienti. |
| Ambiente, elettronica, rifiuti/RAEE, imballaggi | Art. 25-undecies | MEDIO | Gestione rifiuti elettronici e materiali, soggetti autorizzati, nuove fattispecie ambientali. |
| Assunzioni e personale extra-UE | Art. 25-duodecies | BASSO-MEDIO | Verifica titoli di soggiorno e condizioni di impiego. |
| Contenzioso e rapporti con autorità giudiziaria | Art. 25-decies | BASSO-MEDIO | Dichiarazioni, conservazione documenti, non interferenza con testimoni. |
| Terrorismo, tratta, razzismo, patrimonio culturale, animali, frodi sportive | Artt. 25-quater e ss. applicabili | BASSO/REMOTO | Nessun processo core ordinario individuato; presidi generali e monitoraggio. |

## 14. Protocolli per famiglie di reato

### 14.1 Rapporti con la Pubblica Amministrazione, gare e fondi pubblici

**Artt. 24 e 25 D.Lgs. 231/2001**

#### Attività sensibili

- partecipazione a gare, affidamenti e procedure pubbliche;
- richieste di contributi, crediti agevolati, bandi R&D e rendicontazione;
- rapporti con enti, autorità, università pubbliche, strutture sanitarie pubbliche e soggetti assimilabili;
- ispezioni, autorizzazioni e certificazioni pubbliche;

### Protocolli minimi

- divieto assoluto di utilità indebite, promesse, favori o pagamenti di facilitazione;
- doppio controllo su dichiarazioni e documenti presentati alla PA;
- tracciabilità di incontri significativi con funzionari e soggetti pubblici;
- verifica di eleggibilità e rendicontazione delle spese finanziate;
- omaggi/ospitalità solo entro policy, soglie e finalità lecite;
- consulenti o intermediari verso PA solo previa due diligence, contratto e compensi congrui;
- separazione tra chi prepara l'offerta, chi approva condizioni economiche e chi sottoscrive.

## 14.2 Delitti informatici e trattamento illecito di dati

**Art. 24-bis**

### Attività sensibili

- sviluppo e test di strumenti di cybersecurity;
- accesso remoto a reti e sistemi di clienti;
- PoC, supporto e incident response;
- amministrazione di infrastrutture, cloud, repository e ambienti di laboratorio;

### Protocolli minimi

- accesso esclusivamente su autorizzazione documentata e perimetro definito;
- account nominativi, MFA ove appropriata, minimo privilegio e revoca tempestiva;
- logging delle attività privilegiate e conservazione proporzionata al rischio;
- divieto di test offensivi fuori perimetro o senza mandato;
- separazione degli ambienti sviluppo/test/produzione;
- gestione sicura di exploit, malware samples, credenziali e segreti;
- procedure di vulnerability disclosure e incident handling;
- divieto di alterare o sopprimere log ed evidenze.

## 14.3 Delitti contro industria e commercio, marchi e origine

**Artt. 25-bis e 25-bis.1**

### Attività sensibili

- commercializzazione di appliance e prodotti;
- packaging, etichettatura e documentazione di origine;
- uso di marchi, loghi, certificazioni e claim "Made in Italy";
- materiale commerciale e comparativo;

### Protocolli minimi

- verifica preventiva della base documentale di ogni claim di origine o certificazione;
- tracciabilità di componenti, assemblaggio e fornitori;
- approvazione Legal/Compliance per claim sensibili, marchi di terzi e comparazioni;
- divieto di indicazioni idonee a indurre in errore su provenienza, produttore o caratteristiche;
- controllo delle grafiche e diciture apposte da OEM/contract manufacturer.

## 14.4 Reati societari e corruzione tra privati

**Art. 25-ter**

### Attività sensibili

- bilancio, report agli investitori, operazioni sul capitale;
- rapporti con clienti/fornitori privati, partner e distributori;
- premi, commissioni, rebate e incentivi;

### Protocolli minimi

- contabilità completa e documentata;
- verifica indipendente delle scritture di chiusura significative;
- criteri trasparenti per sconti e commissioni;
- divieto di retrocommissioni e utilità occulte;
- gestione formalizzata dei conflitti di interesse;
- conservazione di delibere, contratti e motivazioni delle operazioni straordinarie.

## 14.5 Salute e sicurezza sul lavoro

**Art. 25-septies**

### Attività sensibili

- uffici, laboratori R&D e movimentazione hardware;
- trasferte e installazioni presso clienti;
- uso di attrezzature elettriche/elettroniche;
- appalti e accesso a siti terzi;

### Protocolli minimi

- DVR aggiornato e nomine obbligatorie;
- formazione, informazione e addestramento;
- gestione near miss e infortuni;
- verifica requisiti tecnico-professionali di appaltatori quando applicabile;
- procedure per attività presso siti cliente e rischi interferenziali;
- sorveglianza su manutenzioni e conformità attrezzature.

## 14.6 Ricettazione, riciclaggio, autoriciclaggio e strumenti di pagamento

**Artt. 25-octies e 25-octies.1**

### Attività sensibili

- incassi e pagamenti;
- rimborsi, note credito e commissioni;
- acquisti da fornitori e partner internazionali;
- strumenti di pagamento digitali;

### Protocolli minimi

- pagamenti solo su conti verificati e coerenti con la controparte;

- verifica rafforzata per variazioni IBAN;
- divieto di frazionamenti artificiosi o pagamenti anomali;
- controllo di congruità delle prestazioni;
- riconciliazioni e segregazione credenziali bancarie;
- escalation di transazioni incoerenti con geografia, contratto o profilo controparte.

## 14.7 Violazione del diritto d'autore e proprietà intellettuale

**Art. 25-novies**

### Attività sensibili

- sviluppo software/firmware;
- uso di componenti open source e dipendenze;
- dataset, documentazione, immagini e materiali marketing;
- integrazione di software di terzi;

### Protocolli minimi

- Software Bill of Materials (SBOM) o inventario equivalente per componenti rilevanti;
- policy open source e verifica licenze;
- approvazione delle dipendenze con obblighi copyleft o restrittivi;
- repository aziendali con controllo accessi;
- procedure per contributi esterni e codice di terzi;
- verifica diritti su immagini, dataset, brevetti e documentazione.

## 14.8 Reati tributari

**Art. 25-quinquiesdecies**

### Attività sensibili

- ciclo attivo/passivo, IVA, imposte dirette;
- fatture per servizi, consulenze, R&D e internazionali;
- crediti d'imposta e agevolazioni;

### Protocolli minimi

- verifica esistenza e congruità della prestazione prima della registrazione;
- controllo anagrafiche e documenti fiscali;
- riconciliazioni periodiche;
- approvazione qualificata delle dichiarazioni fiscali;
- documentazione dei crediti/agevolazioni e dei presupposti;
- divieto di distruzione o occultamento di documentazione contabile;
- escalation all'organo amministrativo di posizioni fiscali controverse rilevanti.

## 14.9 Contrabbando e dogane

**Art. 25-sexiesdecies**

### Attività sensibili

- importazione/esportazione di appliance, mini-PC, componenti e ricambi;
- spedizioni extra-UE;
- classificazione tariffaria e valore in dogana;

### Protocolli minimi

- fornitori e spedizionieri selezionati e contrattualizzati;
- documentazione doganale conservata e riconciliata con ordini/fatture;
- classificazione, origine e valore supportati da evidenze;
- nessuna istruzione a dichiarare valori o descrizioni non veritiere;
- verifica di licenze o restrizioni applicabili a prodotti dual-use se pertinenti.

## 14.10 Reati ambientali

**Art. 25-undecies**

### Attività sensibili

- rifiuti elettronici, batterie, componenti difettosi;
- imballaggi e materiali di laboratorio;
- fornitori di smaltimento;

### Protocolli minimi

- classificazione dei rifiuti e conferimento a soggetti autorizzati;
- conservazione formulari/registri ove applicabili;
- divieto di abbandono o miscelazione illecita;
- due diligence dei fornitori ambientali;
- gestione di RAEE e batterie secondo ruoli effettivamente ricoperti dalla società;
- rivalutazione 2026 alla luce delle modifiche in materia di criminalità ambientale.

## 14.11 Impiego di cittadini di paesi terzi

**Art. 25-duodecies**

### Attività sensibili

- assunzioni, consulenze personali e personale distaccato;

### Protocolli minimi

- verifica documentale dei titoli di soggiorno e lavoro;
- scadenziario e rinnovi;
- divieto di intermediazione irregolare o condizioni abusive;
- controlli su agenzie e fornitori di manodopera.

## 14.12 Violazione delle misure restrittive dell'Unione europea

**Art. 25-octies.2**

### Attività sensibili

- vendite e distribuzione internazionale;
- partner, reseller, end user e spedizioni;
- pagamenti transfrontalieri;
- supporto, licenze software e servizi remoti;

### Protocolli minimi

- screening di controparti e beneficiari effettivi rispetto alle liste UE applicabili;
- controllo paese, end user ed end use per operazioni a rischio;
- blocco/escalation in caso di match, red flag o triangolazioni anomale;
- clausole contrattuali su sanzioni e riesportazione;
- documentazione delle decisioni di compliance;
- formazione specifica a Sales, Channel, Finance e Operations;
- monitoraggio degli aggiornamenti normativi e delle misure restrittive applicabili.

## 14.13 Induzione a non rendere dichiarazioni o dichiarazioni mendaci

**Art. 25-decies**

### Attività sensibili

- ispezioni, contenziosi, procedimenti e audizioni;

### Protocolli minimi

- divieto di pressioni, minacce, incentivi o istruzioni dirette ad alterare dichiarazioni;
- legal hold e conservazione dei documenti;
- coordinamento con consulenti legali senza alterare l'autonomia del dichiarante;
- segnalazione immediata all'OdV di tentativi di interferenza.

## 14.14 Famiglie a rischio residuale o remoto

Alla data del presente documento risultano, salvo diversa evidenza emersa in sede di interviste, a rischio residuale o remoto le famiglie relative a: terrorismo ed eversione; pratiche di mutilazione; delitti contro la personalità individuale non connessi a rapporti di lavoro; abusi di mercato in assenza di strumenti/operazioni rilevanti; razzismo e xenofobia; frode in competizioni sportive e gioco; delitti contro il patrimonio culturale e riciclaggio di beni culturali; delitti contro gli animali. Tali famiglie restano soggette ai principi del Codice Etico e devono essere rivalutate in caso di evoluzione delle attività.

# 15. Protocolli trasversali di controllo

## 15.1 Due diligence terze parti

- identificazione della controparte e verifica dati societari;
- titolare effettivo per controparti a rischio, quando appropriato;
- screening sanzioni e PEP ove giustificato dal rischio;
- verifica reputazionale proporzionata;
- conflitti di interesse;
- coerenza tra compenso e prestazione;

- clausole 231, anticorruzione, sanzioni, audit e risoluzione;
- riesame periodico dei partner strategici e internazionali.

## 15.2 Ciclo passivo

- richiesta/acquisto autorizzato;
- ordine o contratto prima della prestazione salvo eccezioni motivate;
- evidenza ricezione bene/servizio;
- controllo fattura e corrispondenza con ordine/prestazione;
- pagamento tracciabile e autorizzato;
- controllo rafforzato per consulenze, success fee e intermediari.

## 15.3 Ciclo attivo

- offerta approvata secondo soglie;
- contratto/ordine cliente archiviato;
- sconti fuori soglia motivati;
- fatturazione coerente con consegna/licenza/servizio;
- gestione note credito e refund con doppia approvazione sopra soglia;
- registro partner e deal registration con controlli anticorruzione e conflitti.

## 15.4 Secure development e controllo strumenti cyber

- repository nominativi e branch protection sui componenti critici;
- code review proporzionata;
- secret scanning e divieto di credenziali hard-coded;
- gestione dipendenze e vulnerability scanning;
- tracciabilità di build e release;
- inventario di tool offensivi, exploit e malware sample con accesso limitato;
- autorizzazione scritta per test su sistemi di terzi;
- retention di log tecnici compatibile con privacy, sicurezza e investigazioni.

## 15.5 Regali, ospitalità, sponsorizzazioni e liberalità

- ammessi solo per finalità lecite, proporzionate e trasparenti;
- vietati se finalizzati a influenzare impropriamente decisioni;
- soglie di approvazione e registro per operazioni oltre soglia;
- due diligence del beneficiario per sponsorizzazioni significative;
- divieto di contanti salvo spese minute disciplinate.

## 15.6 Conflitti di interesse

Amministratori, dipendenti e collaboratori devono dichiarare situazioni di interesse personale, familiare o economico che possano interferire con decisioni aziendali. Il soggetto in conflitto si astiene dalla decisione e il conflitto viene documentato.

## 16. Piano di attuazione e monitoraggio

| Priorità | Azione | Responsabile | Evidenza attesa |
|---|---|---|---|
| P0 | Approvare risk assessment definitivo dopo interviste ai process owner | Organo amministrativo / Compliance | Matrice firmata e verbale |
| P0 | Definire composizione, nomina, budget e regolamento OdV | Organo amministrativo | Delibera, lettera incarico, regolamento |
| P0 | Verificare/attivare canale whistleblowing e raccordo OdV | Legal/HR/Privacy | Procedura e informativa |
| P0 | Formalizzare procure, deleghe e limiti di spesa | CEO/Board | Matrice poteri |
| P1 | Policy anticorruzione e rapporti PA | Legal/Sales | Procedura + registro omaggi |
| P1 | Due diligence partner/distributori e sanzioni UE | Legal/Sales/Finance | Checklist e screening |
| P1 | Procedura import/dogane/origine e claim Made in Italy | Operations/Legal | Workflow e fascicolo origine |
| P1 | Policy open source/IP e secure SDLC | CTO/R&D | Policy + SBOM/inventario |
| P1 | Presidi fiscali e ciclo passivo/attivo | Finance | Procedure e controlli |
| P1 | Mappatura RAEE/rifiuti elettronici | Operations/HSE | Istruzione e fornitori autorizzati |
| P2 | Piano formazione 231 per ruolo | HR/Compliance | Registro formazione e test |
| P2 | Piano audit OdV annuale | OdV | Piano verifiche e verbali |

# ALLEGATI OPERATIVI

## Allegato A - Matrice di risk assessment preliminare

| Processo | Rischi | Livello | Controlli chiave | Evidenze |
|---|---|---|---|---|
| Governance e CdA | Societari; fiscali; PA | ALTO | Delibere, deleghe, conflitti, reporting finanziario | Verbali, procure, attestazioni |
| Gare/PA/Contributi | PA; frodi pubbliche | ALTO | Dual review, tracciabilità, rendicontazione, intermediari | Fascicolo gara/bando, meeting log |
| Sales/Channel | Corruzione privata; riciclaggio; sanzioni | ALTO | Due diligence, soglie sconto, commissioni, screening | Partner file, approval, screening |
| Procurement | Corruzione privata; riciclaggio; industria/commercio | MEDIO-ALTO | Vendor onboarding, PO, 3-way match | Vendor file, PO, evidenza ricezione |
| Import/Export | Contrabbando; origine; sanzioni UE | ALTO | Dogane, origine, end user, sanzioni | MRN/doc doganali, dichiarazioni origine |
| R&D/Software | Cybercrime; copyright | ALTO | Secure SDLC, accessi, licenze, logging | Repo audit, SBOM, ticket |
| Supporto/PoC | Cybercrime; data | ALTO | Mandato, scope, account nominativi, log | SoW/PoC, access log |
| Finance/Tax | Fiscali; societari; riciclaggio | ALTO | Segregazione, riconciliazioni, tax review | Bilanci, check fiscali, bank approval |
| HR | Immigrazione; salute/sicurezza | MEDIO | Right-to-work, onboarding, formazione | Fascicolo HR, attestati |
| HSE/Lab | Omicidio/lesioni colpose | MEDIO | DVR, RSPP, formazione, near miss | DVR, registri |
| Marketing | Industria/commercio; marchi; copyright | MEDIO-ALTO | Claim review, diritti immagini, origine | Approval record |
| Ambiente | Reati ambientali | MEDIO | RAEE, smaltitori autorizzati, registri | FIR/contratti dove applicabili |
| Contenzioso | Art. 25-decies | BASSO-MEDIO | Legal hold, non interferenza | Legal file |

## Allegato B - Flussi informativi verso l'OdV

| Flusso | Trigger/Frequenza | Informazioni minime |
|---|---|---|
| Nuove gare/PA rilevanti | Trimestrale | ente, importo, responsabile, intermediari, anomalie |
| Contributi/bandi | Trimestrale | progetto, importo, stato, spese, rilievi |
| Partner internazionali | Onboarding + annuale | country, ownership, screening, commissione, red flags |
| Sanzioni/export | Evento | match, paese, end user, decisione compliance |
| Dogane/origine | Trimestrale | volumi, paesi, contestazioni, rettifiche |
| Cyber incident/accessi | Evento | sistemi, perimetro, autorizzazioni, impatto legale |
| IP/copyright | Evento | contestazione, componente, licenza, remediation |
| Fiscale | Trimestrale | verifiche, rilievi, crediti, rettifiche significative |
| HSE | Semestrale + evento | infortuni, near miss, ispezioni, azioni |
| Whistleblowing 231 | Secondo protocollo | categoria, stato, esito senza dati eccedenti |
| Disciplinare 231 | Semestrale | violazione, misura, remediation |

## Allegato C - Clausole 231 per terze parti

**Testo base da adattare al singolo contratto:**

La Controparte dichiara di conoscere i principi del D.Lgs. 231/2001 e si impegna, nello svolgimento delle attività oggetto del contratto, a non porre in essere comportamenti idonei a determinare la responsabilità amministrativa di Cyber Evolution S.r.l. ai sensi del medesimo decreto. La Controparte si impegna altresì a rispettare, per quanto applicabili, il Codice Etico e i principi del Modello 231 comunicati da Cyber Evolution, nonché le norme anticorruzione, le misure restrittive dell'Unione europea e le disposizioni in materia di tutela dei sistemi informatici, proprietà intellettuale, lavoro, ambiente e sicurezza. La violazione grave o reiterata di tali obblighi, ovvero il rifiuto ingiustificato di fornire informazioni ragionevolmente richieste ai fini di verifica, costituisce inadempimento rilevante e potrà comportare sospensione o risoluzione del rapporto secondo quanto previsto dal contratto e dalla legge.

## Allegato D - Checklist di adozione

☐ Risk assessment validato con process owner

☐ Organigramma allegato e aggiornato

☐ Procure/deleghe coerenti e formalizzate

☐ Codice Etico approvato

☐ OdV nominato e regolamento approvato

☐ Budget OdV definito

☐ Flussi OdV attivati

☐ Canale whistleblowing conforme e comunicato

☐ Sistema disciplinare coordinato con CCNL/contratti

☐ Policy anticorruzione/PA

☐ Procedura partner/distributori e sanzioni UE

☐ Procedura dogane/origine/import-export

☐ Policy open source/IP

☐ Secure SDLC e gestione accessi privilegiati

☐ Procedure amministrativo-contabili e fiscali

☐ Presidi HSE/DVR

☐ Gestione RAEE/rifiuti elettronici

☐ Piano formazione 231

☐ Clausole 231 nei contratti rilevanti

☐ Piano audit annuale OdV

☐ Calendario revisione normativa annuale

# Allegato E - Registro aggiornamenti normativi

| Data | Evento | Valutazione richiesta |
|---|---|---|
| 01/07/2025 | Introduzione art. 25-undevicies - delitti contro gli animali | Valutazione di pertinenza: preliminarmente remota per attività core. |
| 24/01/2026 | Entrata in vigore art. 25-octies.2 - misure restrittive UE | Alta rilevanza per distribuzione internazionale, export, servizi e pagamenti transfrontalieri. |
| 02/06/2026 | D.Lgs. 81/2026 - tutela penale dell'ambiente e modifiche 231 | Riesame protocolli ambiente e gestione rifiuti/RAEE. |
| Continuo | Modifiche al catalogo 231 e normativa settoriale | Monitoraggio Legal/Compliance e proposta aggiornamento OdV. |

# Riferimenti consultati

| Fonte | URL |
|---|---|
| Normattiva - D.Lgs. 231/2001, testo vigente al 18/09/2026 | https://www.normattiva.it/atto/caricaDettaglioAtto?atto.codiceRedazionale=001G0293 |
| Confindustria - Linee Guida 231, giugno 2021 | https://www.confindustria.it/documenti/le-nuove-linee-guida-231-di-confindustria-per-la-costruzione-dei-modelli-di-organizzazione-gestione-e-controllo |
| ANAC - Linee guida whistleblowing, Delibera 311/2023 e aggiornamenti | https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing |
| Normattiva - D.Lgs. 81/2026, tutela penale dell'ambiente | https://www.normattiva.it/atto/caricaDettaglioAtto?atto.codiceRedazionale=26G00096 |
| Cyber Evolution - sito istituzionale | https://cyberevolution.it/ |
| LECS - sito istituzionale | https://lecs.io/ |

# Approvazione

Il presente Modello entra in vigore dalla data della sua approvazione mediante delibera dell'organo amministrativo, dopo il completamento della validazione dei processi e degli allegati societari. Ogni versione successiva dovrà riportare data, motivazione della revisione e organo approvante.

Approvazione avvenuta in data **29/06/2026** dal Consiglio di Amministrazione della società CYBER EVOLUTION SRL.

**CYBER EVOLUTION SRL**
Il Presidente del CDA
Dottor Tonino Celani