cloudfire

# CODICE ETICO

APPROVATO CON DELIBERA DEL CDA IN DATA 15 MAGGIO 2026

REV.0 PRIMA ADOZIONE

ALLEGATO AL: "MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

# SOMMARIO

*Il Consiglio di Amministrazione ha deliberato che il Modello si compone di Parte Generale e Parte Speciale e include, tra gli allegati, il presente Codice Etico e il Sistema Disciplinare.*

## 1. IDENTITÀ AZIENDALE E SCOPO DEL CODICE

CloudFire S.r.l. (di seguito anche "CloudFire" o la "Società") è una realtà specializzata nell'erogazione di servizi tecnologici avanzati, con particolare riferimento a soluzioni cloud, cybersecurity, infrastrutture digitali e servizi gestiti, rivolti a clienti pubblici e privati sull'intero territorio nazionale. La Società ha sede legale in Reggio Emilia (RE), Via Giambattista Vico 93, CAP 42124, è iscritta al Registro Imprese dell'Emilia con numero REA RE-311443 e svolge quale attività prevalente la fornitura di infrastrutture informatiche, hosting e attività connesse (Codice ATECO 63.10.10).

In considerazione della natura delle proprie attività — che comporta l'accesso e la gestione di sistemi, dati e infrastrutture critiche per conto dei clienti — CloudFire riconosce che la correttezza, la sicurezza delle informazioni, la riservatezza e l'integrità dei comportamenti costituiscono valori non negoziabili e presupposti essenziali per lo svolgimento responsabile della propria attività.

Il presente Codice Etico (di seguito anche "Codice") è adottato da CloudFire S.r.l. in attuazione dei principi di legalità, correttezza, integrità e trasparenza che ispirano l'intera organizzazione aziendale. Esso costituisce documento di riferimento fondamentale per tutti coloro che operano nell'interesse della Società e si integra con:

- il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 (Parte Generale e Parte Speciale), predisposto con delibera del CdA del 21 aprile 2025, ed adottato con delibera del 15/05/2026;
- le policy e procedure interne tempo per tempo vigenti;
- il Regolamento Aziendale CloudFire il Regolamento Sistemi Informatici attualmente vigenti;
- la Politica di controllo degli accessi attualmente vigente (ISMS-DOC-A05-15-1;
- la Procedura Whistleblowing adottata ai sensi del D.Lgs. 24/2023 tempo per tempo vigente;
- il NDA – Non Disclosure Agreement tempo per tempo vigenti.

La Società mantiene e applica un sistema di gestione per la sicurezza delle informazioni (ISMS) conforme e certificato secondo la norma ISO/IEC 27001:2022 (certificato n. IT23-

13504D), con riferimento ai controlli ISO/IEC 27017:2015 e ISO/IEC 27018:2019, nonché un sistema di gestione per la qualità certificato ISO 9001:2015 (certificato n. IT23-13504A), attualmente vigente.

Il Codice esprime i principi, i valori e le regole di condotta che CloudFire riconosce come propri, al fine di:

- diffondere una solida cultura aziendale orientata all'etica, alla trasparenza e al rispetto delle leggi;
- promuovere comportamenti responsabili, corretti e professionali;
- tutelare gli interessi della Società, dei dipendenti, dei clienti, dei partner e di tutti gli stakeholder;
- preservare CloudFire da rischi di natura legale, reputazionale e organizzativa;
- prevenire comportamenti che possano integrare le fattispecie di reato di cui al D.Lgs. 231/2001.

## 2. DESTINATARI E AMBITO DI APPLICAZIONE

Il presente Codice si applica a tutti i soggetti che, a vario titolo, operano nell'ambito dell'organizzazione CloudFire S.r.l. (di seguito, collettivamente, i "Destinatari"):

- **membri del Consiglio di Amministrazione** e, più in generale, tutti coloro che esercitano funzioni di rappresentanza, amministrazione, direzione o attività gestionali e di controllo, anche di fatto (apicali ai sensi del D.Lgs. 231/2001);
- **dipendenti** (personale subordinato, incluso il personale con funzioni direttive/manageriali);
- **collaboratori** che svolgono attività continuativa o parasubordinata a favore della Società (es. apprendisti, stagisti, figure junior inserite in percorsi formativi o professionalizzanti);
- **soggetti terzi** che operano su mandato, incarico o per conto di CloudFire nello svolgimento delle attività classificate come sensibili nel Risk Assessment 2026, quali ad esempio consulenti tecnici, professionisti esterni, partner commerciali e fornitori coinvolti nei processi a rischio-reato.

Ogni Destinatario è tenuto a:

- rispettare pienamente le prescrizioni del Codice, del Modello 231 e delle procedure interne collegate;
- adottare comportamenti improntati a lealtà, correttezza, trasparenza e diligenza nello svolgimento delle proprie attività;

- contribuire attivamente alla prevenzione dei reati-presupposto e alla tutela dell'integrità, della reputazione e dell'operatività della Società;
- chiedere supporto in caso di dubbio interpretativo;
- segnalare violazioni o situazioni anomale secondo i canali previsti dal Modello.

## 3. PRINCIPI GUIDA

CloudFire S.r.l. fonda la propria operatività sui seguenti principi etici e di comportamento, che costituiscono il riferimento imprescindibile per le scelte quotidiane di ciascun Destinatario:

**Legalità:** rispetto rigoroso di leggi, regolamenti, provvedimenti delle Autorità e impegni contrattuali, in tutte le operazioni svolte da CloudFire.

**Integrità:** nessuno scorciatoia è ammessa, nemmeno sotto pressione. La Società censura fermamente qualsiasi comportamento illecito, anche quando potrebbe apparentemente comportare un vantaggio economico immediato.

**Trasparenza e tracciabilità:** ogni operazione, transazione e azione deve essere verificabile, documentata, coerente e congrua. Le decisioni, le spese e le attività devono essere autorizzate, motivate e conservate in forma tracciabile.

**Rispetto delle persone:** ambiente di lavoro dignitoso, inclusivo e sicuro, nel quale la dignità di ciascuno è sempre tutelata.

**Tutela delle informazioni e dei dati:** protezione del patrimonio informativo aziendale e dei clienti, nel rispetto della normativa applicabile in materia di protezione dei dati personali (GDPR) e di sicurezza delle informazioni (ISO/IEC 27001).

**Responsabilità:** ciascuno risponde delle proprie azioni e collabora attivamente ai controlli. Nessun soggetto può gestire in autonomia un intero processo.

**Lealtà:** si opera in buona fede, con correttezza e senso di responsabilità, tutelando la reputazione e il patrimonio — materiale e informativo — della Società [3].

**Imparzialità:** nelle relazioni interne ed esterne si adottano criteri oggettivi e meritocratici, evitando qualunque forma di favoritismo o discriminazione.

**Diligenza e professionalità:** le attività si svolgono con competenza, accuratezza e puntualità, perseguendo qualità ed efficienza nel rispetto delle regole e degli impegni assunti.

**Sicurezza informatica e protezione dei sistemi:** gli accessi a sistemi, dati e infrastrutture — propri e dei clienti — sono un bene critico da proteggere. Ogni soggetto opera nel rispetto del principio del minimo privilegio e della tracciabilità

delle attività tecniche.

**Privacy:** il trattamento di dati personali — di dipendenti, candidati, clienti e terzi — avviene nel rispetto del GDPR e della normativa applicabile, con adeguate misure di sicurezza e limitando l'accesso ai soli soggetti autorizzati.

**Qualità e affidabilità del servizio:** CloudFire si impegna a rispettare gli SLA contrattuali, a gestire con correttezza reclami e contestazioni e a non promettere prestazioni che non è in grado di garantire.

**Sostenibilità e tutela dell'ambiente:** si adottano comportamenti responsabili e orientati alla riduzione degli sprechi e degli impatti ambientali, nel rispetto della normativa vigente e con particolare attenzione alla corretta gestione dei rifiuti, inclusi i RAEE.

## 4. REGOLE DI COMPORTAMENTO

### 4.1 Conflitti di interesse

I Destinatari evitano situazioni che possano compromettere l'imparzialità e la correttezza delle proprie decisioni e azioni nell'interesse della Società.

**È obbligatorio:**

- comunicare tempestivamente al CEO, alla funzione HR/Compliance o all'OdV (secondo i canali interni) qualsiasi situazione di conflitto di interessi, anche solo potenziale;
- astenersi da decisioni o attività che possano essere influenzate da interessi personali, fino all'ottenimento di indicazioni aziendali.

In particolare, i soggetti che svolgono attività tecniche con accesso a sistemi o dati di clienti devono segnalare immediatamente qualsiasi interesse o relazione personale con il cliente che possa influenzare l'obiettività del loro operato.

### 4.2 Rapporti con clienti, mercato e comunicazione

CloudFire comunica in modo chiaro, affidabile e verificabile con tutti i propri interlocutori.

**È vietato:**

- diffondere claim, brochure, presentazioni o messaggi non veritieri, ingannevoli o privi di evidenze tecniche o contrattuali a supporto;
- utilizzare contenuti, asset, testi, immagini, software, banche dati o marchi di terzi senza i necessari diritti o autorizzazioni;

- utilizzare o far utilizzare i loghi, i marchi o le referenze di clienti senza specifica autorizzazione scritta;
- gestire campagne digitali o database di contatti in assenza di base giuridica, informativa o misure di sicurezza adeguate ai sensi del GDPR.

**È obbligatorio:**

- rispettare impegni contrattuali, SLA e regole di trasparenza verso i clienti;
- conservare evidenze rilevanti (offerte, ordini, contratti, report, comunicazioni) in forma tracciabile e reperibile;
- gestire reclami, contestazioni e note di credito con correttezza e documentazione adeguata.

4.3 Rapporti con la Pubblica Amministrazione e le Autorità

CloudFire adotta una politica di tolleranza zero verso qualsiasi forma di utilità indebita in favore o in danno di pubblici ufficiali o incaricati di pubblico servizio.

**È vietato:**

- offrire, promettere, riconoscere o accettare denaro, favori o vantaggi (diretti o indiretti) per influenzare decisioni o ottenere vantaggi da parte di soggetti pubblici;
- gestire interlocuzioni o invii documentali con le Autorità senza il coinvolgimento dei soggetti aziendali autorizzati;
- rendere dichiarazioni non veritiere, incomplete o fuorvianti, o esibire documentazione alterata, in qualsiasi sede istituzionale o giudiziale.

**È obbligatorio:**

- gestire tutte le interlocuzioni con la Pubblica Amministrazione, le Autorità e gli enti pubblici con correttezza, veridicità e piena tracciabilità;
- in caso di ispezioni o richieste documentali da parte di Autorità (es. Guardia di Finanza, Agenzia delle Entrate, INPS, INAIL, Ispettorato del Lavoro), coinvolgere immediatamente i soggetti aziendali autorizzati e, ove del caso, i consulenti legali e fiscali esterni, garantendo la completezza e la correttezza di tutta la documentazione trasmessa;
- conservare tutta la documentazione relativa ai rapporti con la PA in archivi dedicati, ordinati e reperibili.

4.4 Regali, omaggi, ospitalità, liberalità e sponsorizzazioni

Omaggi, ospitalità, liberalità e sponsorizzazioni sono ammessi esclusivamente se leciti,

proporzionati, autorizzati e tracciati.

**È vietato:**

- offrire o ricevere omaggi, ospitalità o sponsorizzazioni finalizzati a influenzare decisioni, ottenere o accelerare contratti, rinnovi, condizioni economiche o altri vantaggi per la Società;
- effettuare pagamenti o riconoscere benefici a favore di beneficiari non trasparenti, non identificati o con modalità non tracciabili (es. contanti);
- aggirare soglie, poteri autorizzativi o controlli tramite frazionamento delle operazioni o causali generiche;
- utilizzare omaggi in contanti o equivalenti (le gift card non sono consentite, salvo policy specifica); omaggi a familiari o terzi non giustificati sono in ogni caso vietati;
- effettuare erogazioni a favore di partiti, movimenti politici, candidati o campagne elettorali, direttamente o indirettamente.

**È obbligatorio:**

- seguire le deleghe, le soglie e i livelli autorizzativi aziendali per qualsiasi omaggio, ospitalità o liberalità;
- conservare la documentazione completa (richiesta, approvazione, contratto/lettera, evidenze di esecuzione, rendicontazione);
- verificare che i destinatari di liberalità o sponsorizzazioni siano soggetti identificati e legittimati, con verifica minima di identità, reputazione e coerenza con i valori aziendali.

4.5 Correttezza contabile e gestione dei pagamenti

La Società garantisce criteri di selezione, inserimento e crescita professionale improntati a trasparenza e merito, nel rispetto delle pari opportunità. Eventuali sistemi premiali e riconoscimenti devono essere coerenti con comportamenti conformi al presente Codice e con i valori aziendali.

Ogni operazione economica e finanziaria deve essere registrata in modo corretto, completo e verificabile, con piena coerenza tra la sostanza dell'operazione e la sua rappresentazione contabile.

**È vietato:**

- registrare operazioni inesistenti o con causali fittizie;
- frazionare operazioni per aggirare soglie o approvazioni interne; - effettuare o ricevere pagamenti non tracciati, con modalità non coerenti con il soggetto contrattuale o verso conti non intestati alla controparte;
- modificare le coordinate bancarie (IBAN) di un fornitore senza validazione

indipendente e documentazione scritta; ogni cambio IBAN richiede verifica formale dell'identità del richiedente.

**È obbligatorio:**

- garantire piena tracciabilità di ogni operazione (ordini, contratti, fatture, note spese, rendiconti);
- rispettare i controlli su beneficiari, coordinate bancarie e congruità dei pagamenti;
- gestire ordinate e adeguate riconciliazioni contabili, con conservazione della documentazione per i periodi previsti dalla legge.

### 4.6 Persone, rispetto e pari opportunità

CloudFire tutela la dignità, l'equità e la professionalità di ciascuna persona che opera all'interno o in relazione con la Società.

**È vietato:**

- porre in essere condotte discriminatorie o lesive della dignità della persona nelle fasi di selezione, gestione, valutazione o cessazione del rapporto;
- molestare, intimidire o creare un clima ostile, ritorsivo o offensivo;
- assumere o gestire rapporti di lavoro in violazione delle norme applicabili (es. assunzioni non formalizzate, inquadramenti fittizi, pagamenti fuori busta, elusione di contributi o ritenute);
- promettere, offrire, dare o accettare utilità indebite in relazione ad assunzioni, avanzamenti, premi, valutazioni o scelta di consulenti/fornitori HR;
- falsificare, alterare o omettere documenti relativi a contratti, presenze, autorizzazioni, note spese o attestati formativi.

**È obbligatorio:**

- collaborare con rispetto e professionalità, contribuendo a un ambiente inclusivo e sicuro;
- garantire processi HR improntati a trasparenza, tracciabilità e segregazione dei compiti;
- assicurare che presenze, straordinari, trasferte e rimborsi siano autorizzati, documentati e verificabili;
- segnalare tempestivamente richieste anomale o pressioni indebite tramite i canali previsti e, se del caso, verso l'OdV.

### 4.7 Salute e sicurezza sul lavoro

La sicurezza delle persone viene prima della velocità operativa. CloudFire ha adottato una struttura organizzativa e un sistema di gestione documentale in materia di salute e sicurezza in conformità al D.Lgs. 81/2008. Il Responsabile del Servizio di Prevenzione e

Protezione (RSPP) interno è Roberto Bondavalli.

**È vietato:**

- svolgere attività lavorative in assenza delle condizioni di sicurezza previste o in violazione delle prescrizioni e procedure applicabili;
- manomettere, rimuovere o bypassare dispositivi di sicurezza o presidi di protezione.

**È obbligatorio:**

- rispettare le procedure, le istruzioni operative e i dispositivi di protezione individuale (DPI);
- partecipare alla formazione, all'informazione e all'addestramento previsti e attenersi alle istruzioni ricevute;
- segnalare tempestivamente al proprio responsabile situazioni pericolose, incidenti, near miss e ogni evento rilevante;
- per attività svolte presso datacenter e siti di terze parti (es. DATA4 – Campus di Cornaredo), rispettare le regole di accesso fisico, le procedure di emergenza del sito ospitante e le prescrizioni del gestore, oltre alle regole interne CloudFire sul lavoro in aree sicure (art. 16.9 del Regolamento Aziendale CloudFire – V1.2025).

### 4.8 Sicurezza delle informazioni, dati e strumenti informatici

Gli strumenti informatici e le informazioni aziendali — incluse quelle dei clienti — costituiscono un patrimonio critico. Il Regolamento Aziendale CloudFire – V1.2025 e il Regolamento Sistemi Informatici – V1.2025 sono vincolanti per tutti i Destinatari. La Società mantiene un sistema ISMS certificato ISO/IEC 27001:2022.

**È vietato:**

- accedere o tentare di accedere a sistemi informatici, dati o risorse senza autorizzazione, oltre i limiti delle autorizzazioni assegnate o per finalità non coerenti con il ruolo;
- condividere credenziali, utilizzare credenziali di terzi o consentire a terzi l'uso delle proprie; conservare password in chiaro o in modalità non sicura;
- creare, utilizzare o mantenere account privilegiati non tracciati o non autorizzati, account generici o non riconducibili a un soggetto identificato;
- installare, detenere, diffondere o utilizzare software, strumenti o codice idonei a danneggiare/interrompere sistemi o comunicazioni, o a eludere controlli di sicurezza, anche a fini di test se non autorizzati e gestiti in ambiente controllato [5];
- alterare, cancellare o manipolare log, evidenze o dati con lo scopo di

nascondere attività, incidenti, errori o violazioni;
- utilizzare software privo di licenza o in violazione dei diritti di proprietà intellettuale, o diffondere contenuti protetti in modo non autorizzato;
- effettuare accessi tecnici a sistemi o dati del cliente al di fuori di quanto contrattualmente previsto e senza autorizzazione documentata.

**È obbligatorio:**
- rispettare le policy e procedure aziendali in materia di sicurezza delle informazioni, gestione accessi, change management, backup, incident response e gestione dei fornitori IT;
- applicare il principio del minimo privilegio (least privilege) e utilizzare gli accessi privilegiati solo quando necessario e in modo tracciabile [5];
- garantire la tracciabilità delle attività tecniche rilevanti (configurazioni, rilasci, modifiche, accessi privilegiati, ripristini) con conservazione delle evidenze;
- segnalare tempestivamente anomalie o incidenti (es. sospetti accessi non autorizzati, malware, perdita o compromissione di credenziali, vulnerabilità critiche, data breach, indisponibilità rilevante) secondo i canali previsti;
- gestire con particolare attenzione gli accessi e le attività tecniche su sistemi e dati del cliente, nel rispetto di quanto contrattualmente previsto;
- consentire gli aggiornamenti di sicurezza e non installare programmi non autorizzati, come previsto dal Regolamento Sistemi Informatici;
- effettuare gli accessi remoti ai sistemi — propri e dei clienti — esclusivamente tramite canali autorizzati e protetti (es. VPN), con profili coerenti e log attivi.
- Gli eventi di sicurezza possono essere segnalati anche all'helpdesk aziendale (help@cloudfire.it, +39 0522 17534) secondo quanto previsto dalla regolamentazione interna.

### 4.9 Rapporti con fornitori, consulenti e terzi

I rapporti con soggetti terzi devono essere trasparenti, contrattualizzati e gestiti nel rispetto dei principi del Codice e del Modello 231.

**È vietato:**
- utilizzare terzi per aggirare regole, controlli o divieti previsti dal Codice o dal Modello 231;
- corrispondere compensi, provvigioni o commissioni a professionisti esterni in misura non congrua rispetto alle prestazioni o non coerente con l'incarico conferito.

**È obbligatorio:**
- formalizzare per iscritto ogni incarico o contratto con terzi, prevedendo ove

applicabile: clausole di compliance 231/anticorruzione, obblighi di riservatezza, requisiti di sicurezza e clausole risolutive in caso di violazione;
- effettuare una verifica minima sull'identità, l'affidabilità reputazionale e l'assenza di conflitti di interesse della controparte prima di avviare qualsiasi rapporto commerciale rilevante;
- verificare la congruità dei compensi e la tracciabilità di tutti i pagamenti;
- nello scambio di informazioni riservate, applicare ove pertinente il NDA – Non Disclosure Agreement vigente;
- gestire gli accessi di terzi (fornitori, MSP, consulenti IT) a sistemi o dati con autorizzazione preventiva, limitata nel tempo e nelle funzioni, effettuata con modalità protette e tracciata; revocare gli accessi al cessare dell'esigenza;
- in caso di trattamento di dati personali per conto di CloudFire o del Cliente, adottare le specifiche previsioni contrattuali ex art. 28 GDPR.

4.10 Tutela del patrimonio e proprietà intellettuale

**È vietato:**
- utilizzare o diffondere software o contenuti senza licenza o autorizzazione;
- riprodurre, diffondere o utilizzare contenuti protetti da copyright (testi, immagini, codice sorgente, banche dati) senza le necessarie autorizzazioni.

**È obbligatorio:**
- tutelare i segreti aziendali, il know-how e le informazioni riservate della Società e dei clienti;
- rispettare gli obblighi di riservatezza derivanti dai rapporti contrattuali e dall'NDA aziendale;
- mantenere un registro delle licenze software e verificarne periodicamente la conformità.

4.11 Rapporti con l'Autorità Giudiziaria e gestione del contenzioso

**È vietato:**
- alterare, distruggere, occultare o manomettere documenti, evidenze o dati (anche digitali) relativi a contenziosi, ispezioni o richieste dell'Autorità;
- rendere dichiarazioni false o fuorvianti in sede giudiziale o stragiudiziale;
- esercitare pressioni volte a condizionare dichiarazioni rese o da rendere all'Autorità Giudiziaria;
- conferire incarichi legali o disporre pagamenti in assenza di formale conferimento e delle necessarie autorizzazioni e tracciabilità;
- intrattenere rapporti, negoziazioni o scambi informativi con controparti o ausiliari dell'Autorità senza preventiva autorizzazione e fuori dai canali aziendali competenti.

**È obbligatorio:**

- gestire il contenzioso tramite soggetti aziendali autorizzati e, ove necessario, tramite legali esterni incaricati per iscritto con indicazione dell'oggetto e del compenso;
- conservare la documentazione di causa in archivi dedicati, in forma ordinata e immodificabile, garantendo la ricostruibilità delle decisioni;
- informare tempestivamente l'OdV di qualsiasi contenzioso che presenti profili di rischio ai fini del D.Lgs. 231/2001.

4.12 Gestione Asset e Adempimenti Ambientali — Rifiuti di Apparecchiature Elettriche ed Elettroniche (RAEE)

In attuazione dell'art. 25-undecies del D.Lgs. 231/2001 e al fine di presidiare i rischi di commissione dei reati ambientali, CloudFire assicura il rispetto delle disposizioni applicabili alla propria attività in materia ambientale, con particolare riferimento alla gestione dei Rifiuti di Apparecchiature Elettriche ed Elettroniche (RAEE).

CloudFire non svolge attività produttive né gestisce impianti industriali; tuttavia, nell'ambito della propria attività di fornitura di infrastrutture informatiche, la Società tratta apparecchiature elettriche ed elettroniche (server, apparati di rete, endpoint, hardware dismesso) il cui smaltimento deve avvenire nel rigoroso rispetto della normativa vigente.

**È vietato:**

- smaltire o abbandonare apparecchiature elettriche ed elettroniche dismesse al di fuori dei canali di raccolta e smaltimento autorizzati previsti dalla normativa vigente in materia di RAEE;
- affidare la gestione o lo smaltimento di RAEE a soggetti non autorizzati o privi delle necessarie abilitazioni;
- effettuare operazioni di trasporto, stoccaggio o trattamento di rifiuti in violazione delle disposizioni del D.Lgs. 152/2006 (Codice dell'Ambiente) e della normativa RAEE applicabile (D.Lgs. 49/2014 e s.m.i.).

**È obbligatorio:**

- gestire il ritiro, il deposito temporaneo e il conferimento delle apparecchiature dismesse esclusivamente attraverso soggetti/sistemi di raccolta collettivi autorizzati ai sensi della normativa RAEE vigente;
- conservare la documentazione relativa allo smaltimento (formulari, registri, certificati di avvenuto smaltimento) in archivi dedicati e facilmente reperibili per eventuali verifiche da parte delle Autorità competenti;
- segnalare tempestivamente all'OdV e alla funzione Compliance qualsiasi anomalia, irregolarità o richiesta inusuale connessa alla gestione e allo

smaltimento di apparecchiature dismesse o rifiuti;
- aggiornare periodicamente le verifiche di idoneità dei fornitori e partner incaricati della gestione RAEE, assicurando la tracciabilità dell'intera filiera di smaltimento;
- garantire che il personale coinvolto nella gestione degli asset informatici e nella loro dismissione riceva adeguata formazione sugli obblighi normativi in materia ambientale e RAEE.

Eventuali violazioni della normativa ambientale, incluse quelle in materia di RAEE, devono essere immediatamente segnalate all'OdV secondo i flussi informativi del Modello.

## 5. ORGANISMO DI VIGILANZA, MODELLO 231 E SEGNALAZIONI (WHISTLEBLOWING)

### 5.1 L'Organismo di Vigilanza

CloudFire ha adottato il Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001 con delibera del Consiglio di Amministrazione del 21 aprile 2025. L'Organismo di Vigilanza (OdV) è configurato in forma monocratica nella persona dell'**Avv. Carmen Pisanello**, cui sono attribuiti autonomi poteri di iniziativa e di controllo, in piena indipendenza funzionale dal CdA e dalle funzioni aziendali.

L'OdV è incaricato di:
- vigilare sull'osservanza e sull'efficace attuazione del Modello 231 [19];
- verificare la validità e l'adeguatezza del Modello rispetto alla prevenzione dei reati [19];
- curare l'aggiornamento del Modello e proporre al CdA le modifiche necessarie;
- ricevere i flussi informativi dalle funzioni aziendali;
- ricevere e gestire le segnalazioni whistleblowing ai sensi del D.Lgs. 24/2023.

**Canale di comunicazione con l'OdV:** cloudfire.odv@studiolegalepisanello.com.

L'omesso invio delle informazioni dovute all'OdV integra violazione del Modello.

### 5.2 Cosa segnalare

Devono essere segnalati all'OdV (anche in forma di dubbio o perplessità, senza necessità di certezza della violazione):

- violazioni del Codice Etico, del Modello 231 o delle procedure interne;
- pressioni indebite, pagamenti anomali, richieste non trasparenti;
- manipolazione di documenti, log o evidenze digitali;
- incidenti IT rilevanti (inclusi data breach), accessi non autorizzati, violazioni delle regole di accesso e uso improprio di credenziali privilegiate;

- gravi violazioni delle norme di salute e sicurezza sul lavoro, infortuni gravi o near miss critici;
- violazioni della normativa ambientale e anomalie nella gestione dei RAEE;
- richieste di ispezioni o contestazioni da parte delle Autorità (es. ITL, INAIL, VV.F.);
- ritorsioni o minacce verso chi segnala;
- situazioni che configurino conflitti di interesse in relazione ad attività/processi sensibili.

### 5.3 Tutela del segnalante

In conformità al D.Lgs. 24/2023, CloudFire assicura la presenza di canali di segnalazione interna idonei a garantire la riservatezza dell'identità del segnalante, della persona coinvolta e di ogni soggetto menzionato, nonché del contenuto della segnalazione e della documentazione allegata.

Chi segnala in buona fede è pienamente tutelato. Sono vietate ritorsioni, discriminazioni e qualsiasi trattamento pregiudizievole nei confronti del segnalante. La violazione di tale divieto è soggetta alle misure del Sistema Disciplinare.

CloudFire ha adottato un canale di segnalazione interna accessibile tramite piattaforma online. Fino all'attivazione della piattaforma, le segnalazioni possono essere trasmesse direttamente all'OdV all'indirizzo dedicato: **cloudfire.odv@studiolegalepisanello.com**, nel rispetto dei requisiti di riservatezza, circostanziazione e buona fede.

## 6. VIOLAZIONI E CONSEGUENZE

La violazione delle prescrizioni del presente Codice Etico costituisce condotta non conforme ai principi del Modello 231 e può integrare un illecito disciplinare. Il mancato rispetto delle regole contenute nel Codice costituisce elemento di valutazione professionale e può avere riflessi sul percorso di carriera e sui sistemi premiali/retributivi.

Le conseguenze disciplinari e contrattuali sono regolate dal Sistema Disciplinare allegato al Modello 231 e sono graduate in funzione della natura del rapporto con la Società, della gravità della violazione e del ruolo dell'autore. L'applicazione delle sanzioni prescinde dall'instaurazione e dagli esiti di un eventuale procedimento penale.

In sintesi:

- **Dipendenti:** richiamo verbale, ammonizione scritta, multa, sospensione, licenziamento disciplinare, secondo quanto previsto dal CCNL applicabile e dalla legge;

- **Dirigenti:** richiamo verbale, richiamo scritto, risoluzione del rapporto;
- **Collaboratori/consulenti/terzi:** applicazione delle misure contrattuali fino alla risoluzione del contratto, ferma la facoltà di richiedere il risarcimento dei danni;
- **Amministratori:** richiamo formale, revoca o limitazione dei poteri delegati, ulteriori iniziative deliberate dal CdA;
- **Membri dell'OdV:** revoca dell'incarico da parte del CdA.

## 7. STRUTTURA ORGANIZZATIVA DI RIFERIMENTO

Per completezza e ai fini della corretta applicazione del Codice, si riportano i principali ruoli aziendali di riferimento:

| Ruolo | Nominativo |
|---|---|
| Amministratore Delegato – CEO | Roberto Bondavalli |
| Direttore Tecnico – CTO | Fabio Mario Pasetti |
| DPO (esterno) | Clementina Baroni |
| Finance | Chiara Fanti |
| RSGI, Compliance & Controller (esterno) | Martina Montanari |
| HR (esterno) | Francesca Fiori |
| RSPP (interno) | Roberto Bondavalli |
| Organismo di Vigilanza (monocratico) | Avv. Carmen Pisanello |

## 8. DIFFUSIONE, FORMAZIONE E AGGIORNAMENTO

### 8.1 Diffusione

CloudFire assicura che il presente Codice Etico, il Modello 231 e la Procedura Whistleblowing siano resi disponibili a tutti i Destinatari mediante strumenti idonei (es. repository digitale aziendale, area condivisa, intranet o altra modalità di diffusione tracciabile).

La Società provvede a:

- inviare una comunicazione a tutto il personale relativa all'avvenuta adozione del Modello e del Codice Etico e alla nomina dell'OdV;
- inviare una comunicazione a tutto il personale relativa all'implementazione del canale di segnalazione interna e alla nomina del Responsabile Whistleblowing;
- assicurare che i fornitori, consulenti e partner rilevanti ricevano adeguata

informativa sul Codice e, ove possibile, l'inserimento nei contratti di specifiche clausole che disciplinino gli obblighi di condotta e le conseguenze di eventuali violazioni.

### 8.2 Formazione

CloudFire promuove programmi di formazione e awareness volti a garantire ai Destinatari la conoscenza dei contenuti del D.Lgs. 231/2001, del D.Lgs. 24/2023 (Whistleblowing) e delle prescrizioni del Modello, del Codice Etico e della Procedura Whistleblowing.

La formazione è differenziata nei contenuti e nelle modalità in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dell'eventuale attribuzione di funzioni di rappresentanza e gestione. In particolare, il personale tecnico che svolge attività su sistemi informatici e infrastrutture cloud riceve formazione specifica sui rischi informatici, sulla sicurezza delle informazioni e sulla gestione degli asset.

Le iniziative formative possono svolgersi in presenza, da remoto o tramite piattaforme di e-learning. La documentazione relativa (comunicazioni, registri presenze, attestati, materiali didattici) è conservata in forma tracciabile.

### 8.3 Aggiornamento

L'adozione e le modifiche sostanziali del Codice Etico sono di competenza del Consiglio di Amministrazione. L'OdV è responsabile di sottoporre al CdA proposte di aggiornamento e adeguamento del Codice e del Modello in caso di:

- significative violazioni;
- identificazione di nuove aree a rischio o mutamenti dell'assetto organizzativo;
- modifiche del quadro normativo di riferimento;
- emersione di aree di miglioramento a seguito delle attività di verifica.

Il Codice è identificato da numero di versione e data di adozione. Ogni revisione è tracciata in apposito Registro delle Revisioni. La versione vigente è resa disponibile ai Destinatari con modalità idonee e tracciabili.