# CODICE ETICO

**Cyber Evolution S.r.l. – LECS**

*Versione 1.0*

## Sommario

1. Premessa e finalità ..... 2
2. Ambito di applicazione ..... 2
3. Valori guida ..... 2
**4**. Principi di condotta ..... 2
4.1 Legalità e integrità ..... 2
4.2 Centralità del cliente e tutela degli impatti ..... 3
4.3 Trasparenza tecnica e comunicativa (no “black box” opaca) ..... 3
4.4 Sicurezza, privacy e riservatezza ..... 3
4.5 Qualità, robustezza e miglioramento continuo ..... 3
4.6 Correttezza nel canale indiretto e nelle partnership ..... 3
4.7 Conflitti di interesse ..... 4
4.8 Risorse umane: rispetto, inclusione e sviluppo ..... 4
4.9 Uso corretto di asset e tecnologie ..... 4
5. Rapporti con stakeholder ..... 4
5.1 Distributori, reseller e partner tecnologici ..... 4
5.2 Fornitori ..... 4
5. Istituzioni e comunità ..... 4
6. Attuazione, segnalazioni e sanzioni ..... 4
6.1 Governance ..... 4
6.2 Formazione e comunicazione ..... 4
6.3 Canali di segnalazione (whistleblowing) ..... 5
6.4 Conseguenze ..... 5
7. Impegno finale ..... 5

## 1. Premessa e finalità

Cyber Evolution S.r.l. progetta e sviluppa soluzioni di cybersecurity, tra cui LECS, con l'obiettivo di rendere la protezione digitale proattiva, semplice, trasparente e accessibile, riducendo complessità operative e rischi per aziende, persone e servizi essenziali.

Il presente Codice Etico definisce i principi e le regole di condotta che guidano decisioni e comportamenti di:

- soci, amministratori e dirigenti;
- dipendenti e collaboratori;
- partner commerciali (distributori, reseller) e partner tecnologici;
- fornitori e terze parti che operano per conto dell'azienda.

## 2. Ambito di applicazione

Il Codice si applica a tutte le attività di Cyber Evolution e alla promozione ed erogazione di LECS, in tutti i mercati e canali (vendita diretta selettiva e soprattutto canale indiretto tramite distributori/reseller e partner verticali).

## 3. Valori guida

Cyber Evolution fonda la propria identità su:

- Innovazione responsabile: tecnologie proprietarie e approccio AI-driven orientati alla protezione reale e misurabile.
- Affidabilità e continuità operativa: sicurezza come garanzia di operatività, resilienza e riduzione del rischio.
- Semplicità e "zero effort": soluzioni progettate per ridurre carico operativo, tempi e complessità (installazione, gestione, reportistica).
- Trasparenza: report chiari, visibilità e comunicazione comprensibile anche a interlocutori non tecnici.
- Compliance e legalità: orientamento a requisiti normativi e tracciabilità (es. GDPR, NIS2), con condotte sempre conformi alla legge.
- Partnership e supporto: modello di crescita basato su canale, enablement, formazione e collaborazione corretta e misurabile.
- Etica della protezione: difendere dati e infrastrutture significa proteggere persone, famiglie, lavoro e servizi.

## 4. Principi di condotta

### 4.1 Legalità e integrità

Operiamo nel rispetto di leggi, regolamenti, contratti e policy interne.

Rifiutiamo pratiche scorrette: corruzione, favoritismi, frodi, alterazione di documenti o dichiarazioni ingannevoli.

Manteniamo registrazioni accurate e verificabili (amministrative, tecniche, commerciali).

## 4.2 Centralità del cliente e tutela degli impatti

Promuoviamo e forniamo soluzioni orientate a ridurre rischi e impatti (fermi operativi, perdita di dati, danni reputazionali).

Comunichiamo benefici, limiti e condizioni d'uso in modo chiaro, evitando promesse assolute non dimostrabili.

## 4.3 Trasparenza tecnica e comunicativa (no "black box" opaca)

Evitiamo narrazioni volutamente oscure o allarmistiche.

Rendiamo comprensibili: cosa viene rilevato, quali azioni vengono intraprese, quali evidenze e report sono disponibili.

Manteniamo un tono professionale, autorevole ma accessibile, concreto e basato su casi d'uso e prove.

## 4.4 Sicurezza, privacy e riservatezza

Proteggiamo dati, informazioni riservate, segreti industriali e know-how (nostri e dei clienti/partner).

Applichiamo il principio di minimizzazione: trattiamo solo i dati necessari, per finalità legittime e dichiarate.

Le informazioni acquisite in attività di prevendita, supporto, demo e post-vendita sono confidenziali e non riutilizzabili impropriamente.

## 4.5 Qualità, robustezza e miglioramento continuo

Progettiamo con criteri di qualità, test, documentazione e miglioramento continuo.

Gestiamo vulnerabilità e incidenti con responsabilità, tempestività e tracciabilità (approccio di responsible disclosure quando applicabile).

Ogni rilascio o cambiamento rilevante privilegia sicurezza, continuità e chiarezza verso canale e clienti.

## 4.6 Correttezza nel canale indiretto e nelle partnership

Poiché la strategia di go-to-market è principalmente basata su distributori/reseller e partner verticali, adottiamo regole chiare:

Equità e non discriminazione: criteri trasparenti per onboarding, qualificazione, supporto e benefici del partner program.

Enablement reale: formazione, materiali e strumenti operativi coerenti, aggiornati e verificabili.

No concorrenza sleale: rispetto delle aree e delle opportunità concordate, evitando sovrapposizioni opportunistiche.

Co-marketing responsabile: comunicazioni co-branded solo se veritiere, autorizzate e coerenti con identità Cyber Evolution/LECS.

Installazione e supporto: standard di qualità e rispetto degli SLA/patti, con escalation definite, riducendo il rischio per l'end-user.

### 4.7 Conflitti di interesse

Ogni conflitto di interesse (personale, economico, familiare) va dichiarato.

È vietato trarre vantaggio personale da informazioni o relazioni sviluppate in azienda.

### 4.8 Risorse umane: rispetto, inclusione e sviluppo

Promuoviamo un ambiente di lavoro basato su rispetto, meritocrazia, sicurezza psicologica e crescita delle competenze.

Tolleranza zero verso molestie, discriminazioni, intimidazioni o comportamenti offensivi.

### 4.9 Uso corretto di asset e tecnologie

Strumenti, dati e accessi aziendali vanno usati solo per finalità lavorative autorizzate.

È vietata la condivisione non autorizzata di credenziali, dataset, log o materiali tecnici/commerciali.

## 5. Rapporti con stakeholder

### 5.1 Distributori, reseller e partner tecnologici

Relazione orientata a crescita sostenibile, qualità, formazione e fiducia.

Protezione reciproca della reputazione: condotte scorrette su un cliente ricadono sull'intera filiera.

Chiarezza contrattuale, trasparenza dei livelli di servizio, supporto responsabile.

Comunicazione proporzionata: niente "terror marketing", sì a consapevolezza e prevenzione.

### 5.2 Fornitori

Selezione su competenza, affidabilità, sicurezza, compliance e rispetto del presente Codice.

Clausole di riservatezza e requisiti minimi di sicurezza informatica quando necessario.

### 5. Istituzioni e comunità

Collaboriamo in modo trasparente con autorità e organismi competenti, nel rispetto delle norme.

In contesti sensibili (sanità, PA, utility), adottiamo attenzione rafforzata su tracciabilità, riservatezza e compliance.

## 6. Attuazione, segnalazioni e sanzioni

### 6.1 Governance

La Direzione definisce responsabilità interne (OdV organism di vigilanza)per la diffusione del Codice, la formazione e la gestione delle segnalazioni.

Il Codice viene rivisto periodicamente, anche in base a evoluzioni normative e di mercato.

### 6.2 Formazione e comunicazione

Il Codice è consegnato e spiegato a nuovi assunti e collaboratori.

Per il canale, i principi etici sono integrati in onboarding e partner program (materiali, webinar, procedure).

### 6.3 Canali di segnalazione (whistleblowing)

Cyber Evolution mette a disposizione canali riservati per segnalare violazioni o rischi (anche in buona fede), garantendo riservatezza e assenza di ritorsioni.

### 6.4 Conseguenze

Le violazioni possono comportare richiami formali, misure disciplinari, sospensione o risoluzione dei rapporti con partner o fornitori, e azioni legali ove necessario.

## 7. Impegno finale

Cyber Evolution e LECS si impegnano a costruire sicurezza proattiva e comprensibile, capace di proteggere continuità operativa e valore delle organizzazioni, nel rispetto di legalità, trasparenza e responsabilità verso clienti, partner e comunità.

**Rev_01/2026**