Servizi e Tecnologie Enti Pubblici

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO D.LGS. 231/2001

Approvata con Deliberazione del C.d.A. in data 07 dicembre 2015

Aggiornato con Deliberazione del C.d.A. in data 27 marzo 2019

Aggiornata con Deliberazione del C.d.A. in data 10 marzo 2026

Firma del Presidente del C.d.A. _____

STEP S.r.l.
Via Antonio Gramsci, 28
07037 Sorso (SS)
Partita IVA 02104860909

PARTE GENERALE

Articolo 1 – Premessa

STEP S.r.l. opera nel settore della gestione, accertamento e riscossione delle entrate degli enti locali, un ambito caratterizzato da un elevato livello di esposizione ai rischi corruttivi, amministrativi, informatici e reputazionali.

La natura pubblicistica delle attività svolte, la gestione di dati sensibili e giudiziari dei contribuenti, l'interazione costante con la Pubblica Amministrazione e la rilevanza economica dei flussi finanziari trattati rendono necessario un sistema di prevenzione dei rischi strutturato, efficace e costantemente aggiornato.

Il presente Modello di Organizzazione, Gestione e Controllo (di seguito "Modello") è adottato ai sensi del D.Lgs. 231/2001 e rappresenta:

- uno strumento di prevenzione dei reati,
- un presidio di legalità e trasparenza,
- un elemento di rafforzamento della governance,
- un sistema di controllo interno,
- un riferimento per tutti i soggetti che operano per conto della Società.

Il Modello si integra con:

- il Codice Etico,
- il Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT),
- il Sistema di Gestione della Sicurezza sul Lavoro (SGSL),
- il Sistema Qualità,
- il sistema privacy (GDPR),
- il sistema informativo aziendale,
- le procedure interne,
- l'organigramma aggiornato al 12 marzo 2026,
- il sistema delle deleghe e procure.

Il Modello è un documento dinamico, soggetto a revisione periodica in relazione a:

- modifiche normative,
- modifiche organizzative,
- nuove aree di rischio,
- esiti delle verifiche dell'OdV,
- evoluzione delle best practice.

Articolo 2 – Il quadro normativo

2.1 La responsabilità amministrativa degli enti

Il D.Lgs. 231/2001 ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per reati commessi nel loro interesse o vantaggio da:

- soggetti apicali,
- soggetti sottoposti alla direzione o vigilanza degli apicali,
- soggetti che operano anche di fatto per conto dell'ente.

La responsabilità dell'ente si aggiunge a quella della persona fisica autore del reato.

2.2 Le sanzioni

Le sanzioni previste includono:

- sanzioni pecuniarie,
- sanzioni interdittive,

- confisca,
- pubblicazione della sentenza.

Le sanzioni interdittive possono comprendere:

- interdizione dall'esercizio dell'attività,
- sospensione o revoca di licenze e concessioni,
- divieto di contrarre con la P.A.,
- esclusione da finanziamenti e contributi,
- divieto di pubblicizzare beni e servizi.

2.3 Evoluzione normativa 2001–2026

Il catalogo dei reati presupposto è stato ampliato nel tempo, includendo:

- reati contro la P.A.,
- reati societari,
- reati tributari (D.Lgs. 75/2020),
- reati informatici e trattamento illecito dei dati,
- reati ambientali,
- reati in materia di sicurezza sul lavoro,
- riciclaggio e autoriciclaggio,
- reati contro la proprietà industriale e intellettuale,
- reati transnazionali,
- reati in materia di whistleblowing (D.Lgs. 24/2023),
- reati connessi alla sicurezza informatica (Recepimento Direttiva NIS2).

2.4 Linee Guida Confindustria 2021

Il Modello è costruito in conformità alle Linee Guida Confindustria 2021, che rappresentano il principale riferimento metodologico per la costruzione dei modelli organizzativi.

Articolo 3 – Finalità del Modello

Il Modello ha la funzione di:

- prevenire la commissione dei reati previsti dal D.Lgs. 231/2001,
- diffondere una cultura della legalità e del controllo,
- rafforzare la governance aziendale,
- tutelare STEP da rischi legali, economici e reputazionali,
- garantire trasparenza nei rapporti con la Pubblica Amministrazione,
- assicurare correttezza nella gestione delle entrate e dei tributi locali,
- definire un sistema strutturato di presidi organizzativi e procedurali,
- individuare i processi sensibili e i relativi controlli,
- assicurare la tracciabilità delle decisioni,
- definire responsabilità chiare e coerenti con le deleghe e procure.

Il Modello ha anche una funzione educativa: sviluppare nei dipendenti, dirigenti, amministratori, consulenti e partner la consapevolezza che comportamenti non conformi possono determinare responsabilità penali e disciplinari.

Articolo 4 – Costruzione del Modello

4.1 Principi metodologici

La costruzione del Modello STEP si fonda sui principi metodologici indicati dalle Linee Guida Confindustria 2021, che prevedono:

- **mappatura dei rischi** (risk assessment),

- **analisi dei controlli esistenti** (as is analysis),
- **valutazione del rischio residuo**,
- **definizione dei presidi di controllo**,
- **formalizzazione delle procedure**,
- **attribuzione delle responsabilità**,
- **definizione dei flussi informativi**,
- **istituzione dell'Organismo di Vigilanza**,
- **definizione del sistema disciplinare**,
- **piano di formazione e comunicazione**,
- **monitoraggio e aggiornamento periodico**.

Il Modello è costruito secondo un approccio **risk-based**, che prevede l'individuazione delle attività aziendali nelle quali è più probabile la commissione dei reati previsti dal D.Lgs. 231/2001.

4.2 Fasi di costruzione del Modello

Fase 1 – Analisi documentale

Sono stati analizzati:

- organigramma 2026,
- deleghe e procure,
- procedure interne,
- contratti e convenzioni con enti locali,
- sistemi informatici,
- flussi finanziari,
- sistema qualità,
- sistema sicurezza,
- sistema privacy,
- sistema whistleblowing.

Fase 2 – Interviste ai responsabili di settore

Sono stati coinvolti:

- Direzione Generale,
- Ufficio Legale,
- Responsabile Anticorruzione – OdV,
- Settore Tributi Maggiori,
- Settore Tributi Minori,
- Settore Coattiva,
- Settore Contabilità,
- Settore Gare e Appalti,
- Settore IT e Digitalizzazione,
- Settore Risorse Umane,
- Settore Acquisti e Logistica.
- Delegato del Titolare Trattamento Dati Personali
- Punto di Contatto ACN

Le interviste hanno permesso di:

- identificare i processi sensibili,
- individuare i controlli esistenti,
- valutare le criticità,
- definire i presidi necessari.

Fase 3 – Mappatura dei processi sensibili

La mappatura ha individuato:

- attività a rischio,
- reati applicabili,
- controlli esistenti,
- controlli mancanti,
- rischio residuo.

Fase 4 – Definizione dei presidi di controllo

I presidi includono:

- segregazione delle funzioni,
- tracciabilità,
- autorizzazioni,
- verifiche periodiche,
- controlli informatici,
- controlli contabili,
- controlli di secondo livello,
- reporting all'OdV.

Fase 5 – Redazione del Modello

Il Modello è composto da:

- Parte Generale,
- Parti Speciali A–K,
- Allegati 1–6.

4.3 Integrazione con l'organigramma

Il Modello recepisce integralmente l'organigramma aggiornato al 12 marzo 2026, che definisce:

- ruoli,
- responsabilità,
- linee di riporto,
- funzioni di controllo,
- settori operativi,
- aree territoriali.

L'organigramma è parte integrante del Modello e garantisce:

- chiarezza delle responsabilità,
- segregazione delle funzioni,
- tracciabilità delle decisioni.

4.4 Integrazione con deleghe e procure

Il sistema delle deleghe e procure garantisce:

- coerenza tra poteri e responsabilità,
- tracciabilità delle decisioni,
- prevenzione dei conflitti di interesse.

Ogni delega è:

- specifica,
- coerente con il ruolo,
- formalizzata,
- aggiornata periodicamente.

4.5 Integrazione con procedure interne

Le procedure interne rappresentano lo strumento operativo attraverso il quale il Modello è attuato. Esse disciplinano:

- attività operative,
- controlli,
- responsabilità,
- flussi informativi.

Articolo 5 – Organismo di Vigilanza

5.1 Natura e ruolo dell'OdV

L'Organismo di Vigilanza (OdV) è l'organo interno incaricato di:

- vigilare sull'efficace attuazione del Modello,
- verificarne l'adeguatezza,
- proporre aggiornamenti,
- gestire il sistema di segnalazione interna,
- effettuare verifiche periodiche,
- monitorare i processi sensibili,
- coordinare la formazione 231.

L'OdV è dotato di:

- autonomia,
- indipendenza,
- continuità d'azione,
- professionalità,
- poteri di iniziativa e controllo.

5.2 Requisiti dell'OdV

L'OdV deve possedere:

- competenze giuridiche,
- competenze organizzative,
- competenze in materia di controllo interno,
- competenze in materia di risk management,
- competenze in materia di sicurezza informatica,
- competenze in materia di privacy,
- competenze in materia di anticorruzione.

5.3 Funzioni dell'OdV

Funzioni di vigilanza

L'OdV vigila:

- sull'attuazione del Modello,
- sull'adeguatezza dei presidi,
- sulla coerenza delle procedure,
- sulla tracciabilità delle attività,
- sulla segregazione delle funzioni,
- sulla gestione dei flussi informativi.

Funzioni di controllo

L'OdV:

- effettua audit periodici,
- verifica i processi sensibili,
- analizza i flussi finanziari,
- verifica la gestione delle banche dati,
- verifica la gestione delle credenziali,

- verifica la gestione delle gare e appalti,
- verifica la gestione dei rapporti con la P.A.

Funzioni di gestione del whistleblowing

L'OdV:

- riceve le segnalazioni,
- garantisce la riservatezza,
- protegge il segnalante,
- conduce le verifiche,
- redige report,
- propone azioni correttive.

Funzioni di formazione

L'OdV:

- definisce i contenuti della formazione,
- verifica la partecipazione,
- valuta l'efficacia,
- propone aggiornamenti.

5.4 Poteri dell'OdV

L'OdV ha:

- libero accesso a ogni documento aziendale,
- poteri ispettivi,
- poteri di richiesta di informazioni,
- poteri di convocazione,
- poteri di audit,
- poteri di segnalazione al CdA,
- un budget autonomo.

5.5 Reporting dell'OdV

L'OdV riferisce:

- **continuativamente** all'Amministratore Delegato,
- **semestralmente** al CdA e al Collegio Sindacale,
- **annualmente** tramite una relazione sulle attività svolte.

Articolo 6 – Sistema disciplinare

6.1 Funzione del sistema disciplinare

Il sistema disciplinare garantisce l'effettività del Modello e sanziona:

- violazioni del Modello,
- violazioni del Codice Etico,
- violazioni del PTPCT,
- violazioni delle procedure interne,
- ostacolo all'attività dell'OdV,
- mancata collaborazione,
- violazioni in materia di whistleblowing.

6.2 Destinatari

Il sistema disciplinare si applica a:

- dipendenti,
- dirigenti,
- amministratori,

- consulenti,
- fornitori,
- partner.

6.3 Tipologie di sanzioni

Per i dipendenti

- richiamo verbale,
- richiamo scritto,
- sospensione,
- licenziamento.

Per i dirigenti

- sospensione,
- revoca dell'incarico.

Per i consulenti e fornitori

- risoluzione del contratto,
- esclusione da future collaborazioni.

Per gli amministratori

- segnalazione al CdA,
- revoca dell'incarico.

Articolo 7 – Formazione e comunicazione

7.1 Formazione

La formazione è:

- obbligatoria,
- periodica,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Tipologie di formazione

- formazione base,
- formazione avanzata,
- formazione specialistica,
- formazione per i nuovi assunti.

7.2 Comunicazione

La comunicazione avviene tramite:

- intranet,
- circolari interne,
- newsletter,
- incontri formativi,
- kit di onboarding.

Articolo 8 – Aggiornamento del Modello

Il Modello è aggiornato:

- in caso di modifiche normative,
- in caso di modifiche organizzative,
- in caso di nuove aree di rischio,
- su proposta dell'OdV,

- su decisione del CdA.

Articolo 9 – Integrazione con organigramma, deleghe, procure e procedure interne

Il Modello è pienamente integrato con:

- organigramma 2026,
- deleghe e procure,
- procedure interne,
- sistemi informatici,
- sistemi di gestione qualità,
- sistemi di sicurezza sul lavoro,
- sistemi privacy.

PARTE SPECIALE A – REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e comportamentali finalizzati a prevenire la commissione dei reati contro la Pubblica Amministrazione (P.A.), categoria di reati di particolare rilevanza per STEP S.r.l. in ragione:

- della natura pubblicistica delle attività svolte,
- della gestione di funzioni delegate dagli enti locali,
- dell'interazione costante con funzionari pubblici, dirigenti, responsabili di servizio e soggetti incaricati di pubblico servizio,
- della gestione di flussi finanziari rilevanti,
- della gestione di dati sensibili e giudiziari dei contribuenti,
- della partecipazione a procedure di gara e affidamenti pubblici,
- della gestione di ispezioni, verifiche e audit da parte degli enti affidanti.

La prevenzione dei reati contro la P.A. rappresenta un presidio essenziale per la tutela dell'integrità aziendale, della reputazione della Società e della fiducia degli enti pubblici affidanti.

Articolo 2. Normativa di riferimento

I reati contro la Pubblica Amministrazione rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dagli artt. 24 e 25 del Decreto e comprendono, tra gli altri:

2.1 Peculato (art. 314 c.p.)

Appropriazione indebita da parte di un pubblico ufficiale o incaricato di pubblico servizio di denaro o altra cosa mobile altrui di cui abbia disponibilità per ragioni del suo ufficio.

2.2 Concussione (art. 317 c.p.)

Costrizione del privato a dare o promettere indebitamente denaro o altra utilità.

2.3 Corruzione propria e impropria (artt. 318–322 c.p.)

- Corruzione per l'esercizio della funzione
- Corruzione per atto contrario ai doveri d'ufficio
- Corruzione in atti giudiziari
- Istigazione alla corruzione

2.4 Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)

Condotta in cui il pubblico ufficiale induce il privato a dare o promettere indebitamente denaro o altra utilità.

2.5 Abuso d'ufficio (art. 323 c.p.)

Violazione di norme di legge o regolamento da parte del pubblico ufficiale per procurare a sé o ad altri un ingiusto vantaggio patrimoniale.

2.6 Truffa ai danni dello Stato (art. 640, comma 2, n. 1 c.p.)

Induzione in errore della P.A. mediante artifici o raggiri.

2.7 Frode nelle pubbliche forniture (art. 356 c.p.)

Inadempimento doloso di obblighi contrattuali verso la P.A.

2.8 Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.)

Ottenimento indebito di contributi, finanziamenti o altre erogazioni pubbliche.

2.9 Reati introdotti dalla Legge 190/2012

- corruzione tra privati,
- traffico di influenze illecite,
- obblighi di trasparenza,

- obblighi di prevenzione della corruzione.

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati contro la P.A.:

3.1 Partecipazione a gare pubbliche

- predisposizione della documentazione di gara,
- gestione dei rapporti con stazioni appaltanti,
- gestione delle richieste di chiarimento,
- presentazione delle offerte,
- gestione delle fasi di aggiudicazione.

3.2 Gestione delle convenzioni con gli enti locali

- negoziazione,
- stipula,
- rinnovo,
- esecuzione,
- rendicontazione.

3.3 Gestione delle ispezioni e verifiche

- accesso agli atti,
- riscontro alle richieste degli enti,
- gestione delle osservazioni,
- gestione delle contestazioni.

3.4 Gestione dei rapporti istituzionali

- incontri con funzionari pubblici,
- comunicazioni formali,
- partecipazione a tavoli tecnici.

3.5 Gestione dei flussi finanziari verso la P.A.

- riversamenti,
- rendicontazioni,
- gestione delle somme riscosse.

3.6 Gestione dei contributi pubblici

- richieste,
- rendicontazioni,
- verifiche.

3.7 Gestione dei procedimenti amministrativi

- emissione di atti,
- notifiche,
- gestione delle posizioni debitorie.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati contro la P.A. includono:

4.1 Segregazione delle funzioni

- chi accerta non riscuote,
- chi riscuote non contabilizza,
- chi contabilizza non autorizza,

- chi autorizza non controlla.

4.2 Tracciabilità delle decisioni

Ogni attività deve essere:

- documentata,
- verificabile,
- archiviata,
- accessibile all'OdV.

4.3 Obbligo di documentazione

Ogni interazione con la P.A. deve essere:

- formalizzata,
- protocollata,
- conservata.

4.4 Controlli di linea

Effettuati dai responsabili di settore.

4.5 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- Controllo di Gestione,
- Qualità,
- DPO,
- RSPP.

4.6 Controlli dell'OdV

Audit periodici su:

- gare,
- convenzioni,
- flussi finanziari,
- rapporti con la P.A.,
- ispezioni,
- rendicontazioni.

4.7 Flussi informativi verso l'OdV

Obbligatori per:

- gare e appalti,
- ispezioni,
- contestazioni,
- anomalie,
- segnalazioni,
- rapporti con la P.A.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti

È vietato:

- promettere, offrire o ricevere denaro o utilità,
- intrattenere rapporti informali con funzionari pubblici,
- utilizzare canali non ufficiali,
- alterare documenti,
- manipolare dati,

- ostacolare ispezioni,
- favorire contribuenti o terzi,
- utilizzare informazioni riservate per fini personali.

5.2 Obblighi

È obbligatorio:

- mantenere un comportamento trasparente,
- documentare ogni attività,
- rispettare le procedure interne,
- segnalare anomalie,
- collaborare con l'OdV,
- utilizzare esclusivamente canali ufficiali.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- bandi di gara,
- offerte presentate,
- verbali di gara,
- convenzioni stipulate,
- ispezioni ricevute,
- contestazioni,
- richieste di chiarimento,
- rapporti con funzionari pubblici,
- anomalie nei flussi finanziari,
- segnalazioni whistleblowing.

Articolo 7. Formazione specifica

La formazione sui reati contro la P.A. è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Gare e Appalti,
- Commerciale,
- Ufficio Legale,
- Direzione Generale,
- Tributi Maggiori,
- Tributi Minori,
- Coattiva.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,

- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE B – REATI SOCIETARI

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e comportamentali finalizzati a prevenire la commissione dei **reati societari**, categoria di reati rilevante per STEP S.r.l. in relazione:

- alla formazione del bilancio,
- alla gestione delle informazioni societarie,
- ai rapporti con gli organi di controllo,
- alle operazioni sul capitale,
- alla gestione dei libri sociali,
- alla comunicazione verso l'esterno di dati economico-finanziari,
- alla gestione dei flussi informativi verso il Collegio Sindacale e la società di revisione.

I reati societari assumono particolare rilevanza per STEP in quanto:

- la Società gestisce ingenti flussi finanziari derivanti dalla riscossione delle entrate degli enti locali;
- la corretta rappresentazione contabile è essenziale per garantire trasparenza verso gli enti affidanti;
- la gestione dei dati economici e finanziari è soggetta a controlli esterni (revisione, organi di vigilanza, enti locali);
- la reputazione della Società dipende dalla correttezza delle informazioni societarie diffuse.

Articolo 2. Normativa di riferimento

I reati societari rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dall'art. 25-ter del Decreto e comprendono, tra gli altri:

2.1 False comunicazioni sociali (artt. 2621 e 2622 c.c.)
Consistono nell'esporre fatti materiali non rispondenti al vero o nell'omettere informazioni rilevanti sulla situazione economica, patrimoniale o finanziaria della Società.

2.2 Ostacolo all'esercizio delle funzioni di vigilanza (art. 2625 c.c.)
Comportamenti che impediscono o ostacolano l'attività del Collegio Sindacale o della società di revisione.

2.3 Indebita restituzione dei conferimenti (art. 2626 c.c.)
Restituzione ai soci dei conferimenti effettuati, in violazione delle norme di tutela del capitale sociale.

2.4 Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
Distribuzione di utili non realmente conseguiti o destinati per legge a riserva.

2.5 Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Riduzioni del capitale sociale o fusioni/scissioni in violazione delle norme a tutela dei creditori.

2.6 Formazione fittizia del capitale (art. 2632 c.c.)
Sovrastima dei conferimenti o attribuzione di capitale inesistente.

2.7 Aggiotaggio (art. 2637 c.c.)
Diffusione di notizie false o artifici idonei a provocare alterazioni del valore delle partecipazioni sociali.

2.8 Ostacolo alla revisione (art. 2625 c.c.)
Comportamenti che impediscono o ostacolano l'attività della società di revisione.

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati societari:

3.1 Formazione del bilancio

- raccolta dei dati contabili,
- scritture di assestamento,
- valutazioni di bilancio,
- predisposizione della nota integrativa,
- predisposizione della relazione sulla gestione.

3.2 Gestione dei libri sociali

- libro soci,
- libro delle decisioni del CdA,
- libro delle decisioni dei soci,
- libro del Collegio Sindacale.

3.3 Comunicazioni societarie verso l'esterno

- comunicazioni agli enti affidanti,
- comunicazioni alla società di revisione,
- comunicazioni al Collegio Sindacale,
- comunicazioni agli istituti di credito.

3.4 Operazioni sul capitale

- aumenti e riduzioni di capitale,
- distribuzione degli utili,
- operazioni straordinarie.

3.5 Rapporti con la società di revisione

- trasmissione dei documenti,
- riscontro alle richieste,
- gestione delle verifiche.

3.6 Rapporti con il Collegio Sindacale

- flussi informativi obbligatori,
- trasmissione dei documenti,
- gestione delle richieste.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati societari includono:

4.1 Segregazione delle funzioni

- chi registra non autorizza,
- chi autorizza non controlla,
- chi controlla non contabilizza.

4.2 Tracciabilità delle operazioni

Ogni operazione deve essere:

- documentata,
- verificabile,
- archiviata,
- accessibile all'OdV.

4.3 Procedure contabili formalizzate

STEP adotta procedure che disciplinano:

- registrazioni contabili,
- riconciliazioni,
- chiusure periodiche,
- scritture di assestamento,
- valutazioni di bilancio.

4.4 Controlli di linea

Effettuati dal Settore Contabilità.

4.5 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- Controllo di Gestione,
- Qualità.

4.6 Controlli della società di revisione

La società di revisione effettua:

- verifiche periodiche,
- verifiche a campione,
- verifiche di coerenza,
- verifiche di completezza.

4.7 Controlli del Collegio Sindacale

Il Collegio Sindacale:

- vigila sull'osservanza della legge,
- vigila sull'adeguatezza dell'assetto organizzativo,
- vigila sull'adeguatezza del sistema di controllo interno.

4.8 Controlli dell'OdV

L'OdV effettua audit su:

- bilancio,
- flussi informativi,
- rapporti con revisione e sindaci,
- operazioni sul capitale.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti

È vietato:

- alterare dati contabili,
- omettere informazioni rilevanti,
- fornire informazioni false o incomplete,
- ostacolare l'attività del Collegio Sindacale,
- ostacolare l'attività della società di revisione,
- diffondere notizie false,
- manipolare il valore delle partecipazioni sociali.

5.2 Obblighi

È obbligatorio:

- fornire informazioni complete e veritiere,
- collaborare con gli organi di controllo,
- rispettare le procedure contabili,
- documentare ogni operazione,

- segnalare anomalie.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- bozze di bilancio,
- scritture di assestamento rilevanti,
- comunicazioni con la società di revisione,
- comunicazioni con il Collegio Sindacale,
- operazioni sul capitale,
- anomalie contabili,
- segnalazioni whistleblowing.

Articolo 7. Formazione specifica

La formazione sui reati societari è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore Contabilità,
- Direzione Generale,
- Ufficio Legale,
- Revisione interna.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE C – REATI TRIBUTARI

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e comportamentali finalizzati a prevenire la commissione dei **reati tributari**, introdotti nel catalogo dei reati presupposto del D.Lgs. 231/2001 dal **D.Lgs. 75/2020**, che ha recepito la Direttiva (UE) 2017/1371 (c.d. "Direttiva PIF").
I reati tributari assumono particolare rilevanza per STEP S.r.l. in ragione:

- della gestione di ingenti flussi finanziari derivanti dalla riscossione delle entrate degli enti locali;
- della gestione di documenti contabili e fiscali rilevanti;
- della necessità di garantire trasparenza e correttezza nei rapporti con l'Agenzia delle Entrate, gli enti locali e gli organi di controllo;
- della responsabilità nella rendicontazione delle somme riscosse;
- della gestione di processi contabili complessi e articolati;
- della rilevanza reputazionale connessa alla corretta gestione delle informazioni fiscali.

La prevenzione dei reati tributari è un presidio essenziale per la tutela dell'integrità aziendale e della reputazione della Società.

Articolo 2. Normativa di riferimento

I reati tributari rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dall'art. 25-quinquiesdecies del Decreto e comprendono:

2.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/2000)
Consiste nell'indicare elementi passivi fittizi mediante l'utilizzo di fatture false.

2.2 Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000)
Consiste nell'indicare elementi attivi o passivi falsi mediante artifici contabili.

2.3 Dichiarazione infedele (art. 4 D.Lgs. 74/2000)
Consiste nell'indicare elementi attivi inferiori o elementi passivi superiori al reale.

2.4 Omessa dichiarazione (art. 5 D.Lgs. 74/2000)
Consiste nel non presentare la dichiarazione dei redditi o IVA.

2.5 Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. 74/2000)
Consiste nell'emissione di documenti falsi per consentire a terzi l'evasione fiscale.

2.6 Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000)
Consiste nel distruggere o occultare documenti contabili per impedire la ricostruzione del reddito o del volume d'affari.

2.7 Indebita compensazione (art. 10-quater D.Lgs. 74/2000)
Consiste nell'utilizzare crediti inesistenti o non spettanti per compensare debiti fiscali.

2.8 Sottrazione fraudolenta al pagamento delle imposte (art. 11 D.Lgs. 74/2000)
Consiste nel compiere atti fraudolenti per sottrarsi al pagamento delle imposte.

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati tributari:

3.1 Predisposizione delle dichiarazioni fiscali

- raccolta dei dati contabili,
- predisposizione delle dichiarazioni,

- trasmissione telematica,
- gestione dei rapporti con consulenti fiscali.

3.2 Gestione dei documenti contabili

- registrazioni contabili,
- conservazione dei documenti,
- archiviazione digitale,
- gestione dei registri IVA.

3.3 Gestione dei flussi finanziari

- pagamenti,
- incassi,
- riconciliazioni bancarie,
- riversamenti agli enti locali.

3.4 Gestione delle fatture passive e attive

- ricezione,
- registrazione,
- verifica della correttezza,
- controllo delle operazioni.

3.5 Gestione dei rapporti con l'Agenzia delle Entrate

- riscontro alle richieste,
- gestione delle verifiche,
- gestione delle comunicazioni.

3.6 Gestione dei rapporti con gli enti locali

- rendicontazioni,
- riversamenti,
- verifiche.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati tributari includono:

4.1 Segregazione delle funzioni

- chi registra non autorizza,
- chi autorizza non controlla,
- chi controlla non contabilizza.

4.2 Tracciabilità delle operazioni

Ogni operazione deve essere:

- documentata,
- verificabile,
- archiviata,
- accessibile all'OdV.

4.3 Procedure contabili formalizzate

STEP adotta procedure che disciplinano:

- registrazioni contabili,
- riconciliazioni,
- chiusure periodiche,
- scritture di assestamento,
- valutazioni fiscali.

4.4 Controlli di linea
Effettuati dal Settore Contabilità.
4.5 Controlli di secondo livello
Effettuati da:

- Ufficio Legale,
- Controllo di Gestione,
- Qualità.

4.6 Controlli dell'Agenzia delle Entrate
STEP collabora pienamente con:

- verifiche fiscali,
- accessi,
- ispezioni,
- richieste documentali.

4.7 Controlli dell'OdV
L'OdV effettua audit su:

- dichiarazioni fiscali,
- flussi finanziari,
- documenti contabili,
- rapporti con consulenti fiscali.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti
È vietato:

- alterare dati contabili o fiscali,
- omettere informazioni rilevanti,
- utilizzare fatture false,
- emettere fatture per operazioni inesistenti,
- occultare o distruggere documenti contabili,
- utilizzare crediti inesistenti,
- sottrarsi al pagamento delle imposte,
- ostacolare verifiche fiscali.

5.2 Obblighi
È obbligatorio:

- fornire informazioni complete e veritiere,
- collaborare con gli organi di controllo,
- rispettare le procedure contabili e fiscali,
- documentare ogni operazione,
- segnalare anomalie.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- bozze delle dichiarazioni fiscali,
- scritture di assestamento rilevanti,
- comunicazioni con consulenti fiscali,
- comunicazioni con l'Agenzia delle Entrate,
- anomalie contabili,

- segnalazioni whistleblowing.

Articolo 7. Formazione specifica

La formazione sui reati tributari è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore Contabilità,
- Direzione Generale,
- Ufficio Legale,
- Revisione interna.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE D – REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e tecnici finalizzati a prevenire la commissione dei **reati informatici** e dei **reati connessi al trattamento illecito dei dati personali**, categorie di reati di particolare rilevanza per STEP S.r.l. in ragione:

- della gestione di **banche dati tributarie**, contenenti dati personali, sensibili e giudiziari dei contribuenti;
- dell'utilizzo di **sistemi informatici complessi**, interconnessi e integrati con piattaforme esterne;
- dell'accesso a **sistemi informatici degli enti locali**;
- della gestione di **credenziali di accesso** e profili autorizzativi differenziati;
- della gestione di **flussi informatici** relativi a pagamenti, riversamenti e rendicontazioni;
- dell'utilizzo di **software proprietari**, applicativi gestionali e sistemi di digitalizzazione;
- dell'obbligo di conformità al **GDPR**, al **D.Lgs. 196/2003**, alla **Direttiva NIS2** e alle **Linee Guida ACN**.

La prevenzione dei reati informatici e dei reati in materia di privacy è un presidio essenziale per la tutela dell'integrità aziendale, della sicurezza dei dati e della fiducia degli enti pubblici affidanti.

Articolo 2. Normativa di riferimento

I reati informatici rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dagli artt. 24-bis e 24-ter del Decreto e comprendono, tra gli altri:

2.1 Accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.)
Accesso non autorizzato a sistemi informatici protetti da misure di sicurezza.

2.2 Detenzione e diffusione abusiva di codici di accesso (art. 615-quater c.p.)
Detenzione o diffusione di password, token, credenziali o strumenti di autenticazione.

2.3 Diffusione di malware (art. 615-quinquies c.p.)
Diffusione di programmi informatici diretti a danneggiare sistemi o dati.

2.4 Intercettazione illecita di comunicazioni informatiche (art. 617-quater c.p.)
Intercettazione di comunicazioni tra sistemi informatici.

2.5 Danneggiamento di sistemi informatici (artt. 635-bis e ss. c.p.)
Danneggiamento di dati, programmi o sistemi informatici.

2.6 Frode informatica (art. 640-ter c.p.)
Alterazione del funzionamento di un sistema informatico per procurare un ingiusto profitto.

2.7 Reati connessi al trattamento illecito dei dati personali
Ai sensi dell'art. 167 del D.Lgs. 196/2003 e del GDPR, sono rilevanti:

- trattamento illecito di dati personali,
- comunicazione o diffusione illecita di dati,
- accesso non autorizzato a dati personali,
- mancata adozione delle misure di sicurezza,
- violazione dei principi di minimizzazione, integrità e riservatezza.

2.8 Normativa europea e nazionale di riferimento

- Regolamento UE 2016/679 (GDPR)
- D.Lgs. 196/2003 (Codice Privacy)
- Direttiva NIS2 (UE 2022/2555)
- Linee Guida ACN sulla sicurezza informatica

- Linee Guida del Garante Privacy
- Linee Guida AgID
- ~~D.Lgs. 65/2018 (recepimento NIS1)~~ D. Lgs. 138/2024 (recepimento NIS2)
- Cyber Resilience Act (UE) 2024/2847

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati informatici e privacy:

3.1 Gestione dei sistemi informatici

- amministrazione dei server,
- gestione delle reti,
- gestione dei firewall,
- gestione dei sistemi di backup,
- gestione dei sistemi di logging,
- gestione degli aggiornamenti software,
- analisi delle vulnerabilità delle reti.

3.2 Gestione delle credenziali di accesso

- creazione,
- modifica,
- revoca,
- gestione dei profili autorizzativi,
- gestione delle autenticazioni multifattoriali,
- politica di aggiornamento.

3.3 Gestione delle banche dati tributarie

- accesso ai dati dei contribuenti,
- consultazione delle posizioni debitorie,
- aggiornamento dei dati,
- estrazione di report,
- gestione delle interrogazioni massive.
- politica di archiviazione e dismissione

3.4 Gestione dei sistemi di digitalizzazione e notificazione

- piattaforme di notifica digitale,
- sistemi di georeferenziazione,
- sistemi di gestione documentale,
- sistemi di firma digitale.

3.5 Gestione dei flussi informatici verso gli enti locali

- riversamenti,
- rendicontazioni,
- scambio di file,
- integrazioni API.

3.6 Gestione dei sistemi di pagamento

- integrazione con PSP,
- gestione dei flussi PagoPA,
- riconciliazioni automatiche.

3.7 Gestione dei data breach

- rilevazione,

- analisi,
- notifica al Delegato Titolare del Trattamento Dati,
- notifica al Garante (se necessario),
- notifica agli interessati (se necessario),
- notifica al CSIRT (secondo specifica)

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati informatici includono:

4.1 Misure tecniche

Autenticazione forte

- password complesse,
- autenticazione multifattoriale (MFA),
- token di sessione software.

Logging e monitoraggio

- registrazione degli accessi,
- registrazione delle operazioni,
- conservazione dei log,
- monitoraggio degli eventi di sicurezza.

Firewall e sistemi di protezione

- firewall perimetrali,
- firewall applicativi (secondo specifica)
- sistemi IDS (analisi euristica)
- sistemi XDR

Backup e disaster recovery

- backup logica 3-2-1
- conservazione off-site,
- test periodici di ripristino.

Cifratura

- cifratura dei dati a riposo (secondo spefica)
- cifratura dei dati in transito.

4.2 Misure organizzative

Segregazione degli accessi

- profili differenziati,
- accessi minimi necessari (principio del "least privilege"),
- revoca immediata degli accessi in caso di cessazione.

Procedure formalizzate

- gestione credenziali,
- gestione incidenti,
- gestione data breach,
- gestione backup,
- gestione aggiornamenti.

Formazione obbligatoria

- sicurezza informatica,
- phishing,
- social engineering,
- privacy.

4.3 Misure di controllo

Controlli di linea
Effettuati dal Settore IT e Digitalizzazione.
Controlli di secondo livello
Effettuati da:

- Delegato del Titolare del Trattamento,
- Punto di Contatto ACN/NIS2,
- Ufficio Legale,
- Qualità.

Controlli dell'OdV
Audit periodici su:

- accessi ai sistemi,
- gestione delle credenziali,
- gestione delle banche dati,
- gestione dei data breach,
- gestione dei flussi informatici.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti

È vietato:

- accedere a sistemi informatici senza autorizzazione,
- utilizzare credenziali altrui,
- condividere password,
- installare software non autorizzati,
- esportare dati senza titolo,
- utilizzare dispositivi personali non autorizzati,
- alterare dati informatici,
- cancellare log o tracce informatiche,
- ostacolare verifiche informatiche,
- utilizzare dati dei contribuenti per fini personali.

5.2 Obblighi

È obbligatorio:

- utilizzare solo strumenti autorizzati,
- rispettare le procedure informatiche,
- segnalare incidenti di sicurezza,
- proteggere le credenziali,
- mantenere riservatezza sui dati,
- collaborare con il DPO e con l'OdV.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- report sugli accessi ai sistemi,
- report sui data breach,
- report sugli incidenti informatici,
- report sulle anomalie,
- report sulle attività del Delegato del Titolare del Trattamento,
- report sulle attività del Punto di Contatto ACN/NIS2,

- segnalazioni whistleblowing.

Articolo 7. Formazione specifica

La formazione sui reati informatici e privacy è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore IT e Digitalizzazione,
- Settore Postale e Digitalizzazione,
- Settore Tributi Maggiori,
- Settore Tributi Minori,
- Settore Coattiva,
- Delegato del Titolare del Trattamento
- Punto di Contatto ACN/NIS2.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione al Garante Privacy,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE E – REATI AMBIENTALI

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e tecnici finalizzati a prevenire la commissione dei **reati ambientali**, categoria di reati rilevante ai fini del D.Lgs. 231/2001 e particolarmente significativa per STEP S.r.l. in relazione:

- alla gestione dei rifiuti prodotti dalle attività aziendali,
- alla gestione degli ambienti di lavoro e delle infrastrutture,
- alla gestione di apparecchiature elettroniche e RAEE,
- alla gestione di toner, batterie, materiali di consumo e supporti informatici,
- alla gestione dei contratti di smaltimento,
- alla gestione dei fornitori e appaltatori che operano presso le sedi aziendali,
- alla tutela del territorio e dell'ambiente circostante,
- alla conformità alle normative ambientali nazionali e regionali.

Sebbene STEP non svolga attività industriali o produttive ad alto impatto ambientale, la normativa 231 richiede comunque l'adozione di presidi adeguati per prevenire condotte illecite, anche solo potenziali, connesse alla gestione dei rifiuti e alla tutela dell'ambiente.

Articolo 2. Normativa di riferimento

I reati ambientali rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dall'art. 25-undecies del Decreto e comprendono, tra gli altri:

2.1 Reati in materia di gestione dei rifiuti (artt. 256 e 260 D.Lgs. 152/2006)

- gestione illecita di rifiuti,
- abbandono o deposito incontrollato,
- smaltimento non autorizzato,
- attività di raccolta, trasporto, recupero o smaltimento senza autorizzazione.

2.2 Inquinamento ambientale (art. 452-bis c.p.)

Causare una compromissione o un deterioramento significativo e misurabile dell'ambiente.

2.3 Disastro ambientale (art. 452-quater c.p.)

Alterazione irreversibile dell'equilibrio di un ecosistema.

2.4 Traffico illecito di rifiuti (art. 452-quaterdecies c.p.)

Attività organizzate per il traffico illecito di rifiuti.

2.5 Violazioni in materia di scarichi idrici (art. 137 D.Lgs. 152/2006)

2.6 Violazioni in materia di emissioni in atmosfera (art. 279 D.Lgs. 152/2006)

2.7 Violazioni in materia di sostanze pericolose (art. 257 D.Lgs. 152/2006)

2.8 Reati in materia di tutela del suolo e del sottosuolo

2.9 Reati in materia di tutela della fauna e della flora

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati ambientali:

3.1 Gestione dei rifiuti prodotti dalle attività aziendali

- rifiuti assimilabili agli urbani,
- rifiuti da ufficio,
- toner e cartucce esauste,

- apparecchiature elettroniche (RAEE),
- batterie e accumulatori,
- materiali di consumo informatico,
- imballaggi.

3.2 Gestione dei contratti di smaltimento

- selezione dei fornitori,
- verifica delle autorizzazioni,
- gestione dei formulari,
- tracciabilità dei rifiuti,
- conservazione della documentazione.

3.3 Gestione degli ambienti di lavoro

- manutenzione degli impianti,
- gestione dei condizionatori,
- gestione dei gruppi di continuità (UPS),
- gestione dei sistemi elettrici,
- gestione dei materiali pericolosi eventualmente presenti.

3.4 Gestione dei fornitori e appaltatori

- imprese di pulizia,
- imprese di manutenzione,
- imprese informatiche,
- imprese di smaltimento rifiuti.

3.5 Gestione delle apparecchiature elettroniche

- acquisto,
- utilizzo,
- manutenzione,
- dismissione,
- smaltimento RAEE.

3.6 Gestione dei consumi energetici

- monitoraggio dei consumi,
- gestione dei contratti di fornitura,
- gestione delle apparecchiature ad alto consumo.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati ambientali includono:

4.1 Segregazione delle funzioni

- chi produce rifiuti non li smaltisce,
- chi smaltisce non autorizza,
- chi autorizza non controlla.

4.2 Tracciabilità dei rifiuti

Ogni rifiuto deve essere:

- classificato,
- identificato,
- conferito correttamente,
- smaltito tramite fornitori autorizzati,
- accompagnato da documentazione (formulari, DDT, certificazioni).

4.3 Verifica delle autorizzazioni dei fornitori

STEP verifica:

- iscrizione all'Albo Gestori Ambientali,
- autorizzazioni al trasporto,
- autorizzazioni allo smaltimento,
- validità delle certificazioni.

4.4 Procedure formalizzate

STEP adotta procedure che disciplinano:

- gestione dei rifiuti,
- gestione dei RAEE,
- gestione dei toner,
- gestione dei materiali pericolosi,
- gestione dei fornitori ambientali.

4.5 Controlli di linea

Effettuati da:

- Settore Acquisti e Logistica,
- Settore IT e Digitalizzazione,
- Settore Postale e Digitalizzazione.

4.6 Controlli di secondo livello

Effettuati da:

- RSPP,
- Ufficio Legale,
- Qualità.

4.7 Controlli dell'OdV

L'OdV effettua audit su:

- gestione dei rifiuti,
- gestione dei RAEE,
- gestione dei fornitori,
- gestione dei formulari,
- gestione delle manutenzioni.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti

È vietato:

- smaltire rifiuti in modo non conforme,
- conferire rifiuti a soggetti non autorizzati,
- abbandonare rifiuti,
- mescolare rifiuti pericolosi e non pericolosi,
- alterare documenti ambientali,
- ostacolare controlli ambientali,
- utilizzare materiali pericolosi senza autorizzazione.

5.2 Obblighi

È obbligatorio:

- rispettare le procedure ambientali,
- utilizzare i contenitori dedicati,
- conferire i rifiuti ai fornitori autorizzati,
- conservare la documentazione,

- segnalare anomalie,
- collaborare con l'OdV e con il RSPP.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- contratti con fornitori ambientali,
- formulari di smaltimento,
- certificazioni RAEE,
- report del RSPP,
- segnalazioni di anomalie,
- verbali di ispezione,
- segnalazioni whistleblowing.

Articolo 7. Formazione specifica

La formazione sui reati ambientali è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore Acquisti e Logistica,
- Settore IT e Digitalizzazione,
- Settore Postale e Digitalizzazione,
- RSPP,
- Responsabili di sede.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE F – SICUREZZA SUL LAVORO (ART. 30 D.LGS. 81/2008)

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e tecnici finalizzati a prevenire la commissione dei **reati in materia di salute e sicurezza sul lavoro**, rilevanti ai fini del D.Lgs. 231/2001 e disciplinati dall'art. 25-septies del Decreto.

I reati in materia di sicurezza assumono particolare rilevanza per STEP S.r.l. in ragione:

- della presenza di personale operativo distribuito su più sedi territoriali,
- dell'utilizzo di apparecchiature informatiche, postazioni di lavoro e archivi,
- della gestione di attività di front-office e back-office,
- della presenza di personale che opera presso sedi di enti locali,
- della gestione di fornitori e appaltatori che accedono ai locali aziendali,
- della necessità di garantire ambienti di lavoro sicuri, ergonomici e conformi alla normativa,
- dell'obbligo di adottare un Sistema di Gestione della Sicurezza sul Lavoro (SGSL) conforme all'art. 30 del D.Lgs. 81/2008.

La prevenzione dei reati in materia di sicurezza è un presidio essenziale per la tutela dell'integrità fisica dei lavoratori, della reputazione aziendale e della continuità operativa.

Articolo 2. Normativa di riferimento

I reati in materia di sicurezza sul lavoro rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dall'art. 25-septies del Decreto e comprendono:

2.1 Omicidio colposo (art. 589 c.p.)

Quando commesso con violazione delle norme sulla sicurezza sul lavoro.

2.2 Lesioni personali colpose gravi o gravissime (art. 590 c.p.)

Quando commesse con violazione delle norme sulla sicurezza sul lavoro.

2.3 Normativa di settore

- **D.Lgs. 81/2008** – Testo Unico sulla Sicurezza
- **D.Lgs. 106/2009** – correttivo del Testo Unico
- **Accordi Stato-Regioni** sulla formazione
- **Norme UNI-INAIL** sui sistemi di gestione della sicurezza
- **Linee guida INAIL sui SGSL**
- **Norme tecniche CEI** per impianti elettrici
- **Norme UNI EN ISO 45001** (sistemi di gestione della sicurezza)

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati in materia di sicurezza:

3.1 Valutazione dei rischi (DVR)

- identificazione dei pericoli,
- valutazione dei rischi,
- individuazione delle misure di prevenzione e protezione,
- aggiornamento periodico del DVR,
- valutazioni specifiche (VDT, stress lavoro-correlato, movimentazione carichi, rischio elettrico).

3.2 Gestione dei DPI

- individuazione dei DPI necessari,
- consegna ai lavoratori,
- formazione sull'uso,
- sostituzione periodica,
- verifica dell'utilizzo.

3.3 Formazione obbligatoria

- formazione generale e specifica,
- formazione per preposti, dirigenti, RLS, RSPP, addetti antincendio e primo soccorso,
- aggiornamenti periodici,
- registrazione delle presenze,
- verifica dell'apprendimento.

3.4 Gestione delle emergenze

- piano di emergenza ed evacuazione,
- prove di evacuazione,
- gestione degli estintori e presidi antincendio,
- gestione dei presidi di primo soccorso.

3.5 Gestione dei fornitori e appaltatori

- verifica dei requisiti tecnico-professionali (DUVRI),
- coordinamento delle attività,
- gestione dei rischi interferenziali,
- controllo degli accessi.

3.6 Gestione delle postazioni di lavoro

- ergonomia,
- illuminazione,
- microclima,
- attrezzature informatiche,
- sedute e arredi.

3.7 Gestione degli impianti e delle attrezzature

- impianti elettrici,
- impianti di climatizzazione,
- gruppi di continuità (UPS),
- attrezzature informatiche,
- manutenzioni periodiche.

3.8 Gestione degli infortuni e near-miss

- registrazione,
- analisi delle cause,
- misure correttive,
- comunicazioni obbligatorie.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati in materia di sicurezza includono:

4.1 Sistema di Gestione della Sicurezza (SGSL)

STEP adotta un SGSL conforme:

- all'art. 30 del D.Lgs. 81/2008,
- alle Linee Guida INAIL,
- alla norma UNI ISO 45001.

Il SGSL comprende:

- politiche di sicurezza,
- obiettivi,
- procedure,
- istruzioni operative,
- controlli,
- audit interni,
- riesame della Direzione.

4.2 Ruoli e responsabilità

Datore di lavoro

- adozione del DVR,
- nomina del RSPP,
- formazione dei lavoratori,
- vigilanza.

RSPP

- valutazione dei rischi,
- formazione,
- audit,
- gestione delle emergenze.

Medico competente

- sorveglianza sanitaria,
- giudizi di idoneità,
- visite periodiche.

Preposti

- vigilanza operativa,
- segnalazione delle anomalie.

Lavoratori

- rispetto delle procedure,
- utilizzo dei DPI,
- segnalazione dei rischi.

4.3 Procedure formalizzate

STEP adotta procedure che disciplinano:

- valutazione dei rischi,
- gestione dei DPI,
- gestione delle emergenze,
- gestione degli infortuni,
- gestione dei fornitori,
- gestione delle manutenzioni,
- formazione.

4.4 Controlli di linea

Effettuati da:

- RSPP,
- preposti,
- responsabili di settore.

4.5 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- Qualità,
- Medico Competente.

4.6 Controlli dell'OdV

L'OdV effettua audit su:

- DVR,
- formazione,
- DPI,
- infortuni,
- manutenzioni,
- fornitori,
- emergenze.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti

È vietato:

- utilizzare attrezzature non autorizzate,
- manomettere dispositivi di sicurezza,
- ignorare procedure o istruzioni operative,
- non utilizzare i DPI,
- ostacolare controlli,
- non segnalare situazioni di pericolo,
- utilizzare impianti o attrezzature non conformi.

5.2 Obblighi

È obbligatorio:

- rispettare le procedure di sicurezza,
- utilizzare i DPI,
- partecipare alla formazione,
- segnalare rischi e anomalie,
- collaborare con RSPP e OdV.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- DVR e aggiornamenti,
- verbali di audit,
- report del RSPP,
- report del Medico Competente,
- registro infortuni,
- segnalazioni di near-miss,
- verbali di ispezione,
- segnalazioni whistleblowing.

Articolo 7. Formazione specifica

La formazione sulla sicurezza è:

- obbligatoria,
- periodica,

- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- tutti i lavoratori,
- preposti,
- dirigenti,
- addetti emergenze,
- RLS.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE G – RICICLAGGIO E AUTORICICLAGGIO

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e comportamentali finalizzati a prevenire la commissione dei **reati di riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita**, rilevanti ai fini del D.Lgs. 231/2001.
Questi reati assumono particolare rilevanza per STEP S.r.l. in ragione:

- della gestione di **flussi finanziari rilevanti** derivanti dalla riscossione delle entrate degli enti locali;
- della gestione di **pagamenti, riversamenti e rendicontazioni** verso gli enti affidanti;
- della gestione di **rapporti con fornitori, consulenti e partner**;
- della gestione di **rapporti con istituti bancari e sistemi di pagamento**;
- della gestione di **banche dati tributarie** contenenti informazioni economiche sensibili;
- della necessità di garantire **trasparenza, tracciabilità e correttezza** in tutte le operazioni finanziarie;
- della rilevanza reputazionale connessa alla gestione di fondi pubblici.

La prevenzione dei reati di riciclaggio è un presidio essenziale per la tutela dell'integrità aziendale, della reputazione della Società e della fiducia degli enti pubblici affidanti.

Articolo 2. Normativa di riferimento

I reati di riciclaggio rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dall'art. 25-octies del Decreto e comprendono:

2.1 Riciclaggio (art. 648-bis c.p.)
Consiste nel:

- sostituire,
- trasferire,
- compiere altre operazioni su denaro, beni o utilità provenienti da delitto non colposo,

al fine di ostacolare l'identificazione della loro provenienza delittuosa.

2.2 Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)
Consiste nell'impiegare in attività economiche o finanziarie denaro, beni o utilità provenienti da delitto non colposo.

2.3 Autoriciclaggio (art. 648-ter.1 c.p.)
Consiste nel:

- impiegare,
- sostituire,
- trasferire

denaro, beni o utilità provenienti da delitto non colposo **commesso dallo stesso autore**, in modo da ostacolare l'identificazione della loro provenienza.

2.4 Normativa antiriciclaggio (D.Lgs. 231/2007)
Pur non essendo STEP un soggetto obbligato ai sensi del D.Lgs. 231/2007, la Società adotta comunque presidi coerenti con i principi della normativa antiriciclaggio, tra cui:

- adeguata verifica della controparte,
- tracciabilità dei flussi finanziari,
- conservazione dei documenti,

- segnalazione di operazioni sospette (ove applicabile).

2.5 Normativa europea

- Direttiva (UE) 2015/849 (IV Direttiva Antiriciclaggio)
- Direttiva (UE) 2018/843 (V Direttiva Antiriciclaggio)
- Regolamento (UE) 2023/1113 sui trasferimenti di fondi

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati di riciclaggio:

3.1 Gestione dei flussi finanziari

- incassi,
- pagamenti,
- riversamenti agli enti locali,
- riconciliazioni bancarie,
- gestione dei conti correnti dedicati.

3.2 Gestione dei rapporti con fornitori e partner

- selezione dei fornitori,
- verifica dei requisiti,
- gestione dei contratti,
- gestione dei pagamenti.

3.3 Gestione dei rapporti con consulenti

- incarichi professionali,
- compensi,
- verifiche sulla controparte.

3.4 Gestione dei sistemi di pagamento

- PagoPA,
- PSP,
- bonifici,
- RID,
- carte di pagamento.

3.5 Gestione delle banche dati tributarie

- accesso ai dati economici dei contribuenti,
- gestione delle posizioni debitorie,
- gestione delle rateizzazioni.

3.6 Gestione dei flussi informatici verso gli enti locali

- rendicontazioni,
- riversamenti,
- scambio di file XML.

3.7 Gestione dei rapporti con istituti bancari

- apertura e gestione dei conti correnti,
- gestione dei mandati di pagamento,
- gestione delle deleghe bancarie.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati di riciclaggio includono:

4.1 Segregazione delle funzioni

- chi gestisce i flussi finanziari non autorizza i pagamenti,
- chi autorizza non contabilizza,
- chi contabilizza non controlla.

4.2 Tracciabilità delle operazioni

Ogni operazione deve essere:

- documentata,
- verificabile,
- archiviata,
- accessibile all'OdV.

4.3 Adeguata verifica della controparte

STEP verifica:

- identità del fornitore,
- sede legale,
- iscrizione alla CCIAA,
- eventuali procedure concorsuali,
- eventuali segnalazioni negative,
- titolarità effettiva (ove rilevante).

4.4 Procedure formalizzate

STEP adotta procedure che disciplinano:

- gestione dei flussi finanziari,
- gestione dei pagamenti,
- gestione dei fornitori,
- gestione dei contratti,
- gestione delle rendicontazioni.

4.5 Controlli di linea

Effettuati da:

- Settore Contabilità,
- Settore Acquisti e Logistica,
- Settore Coattiva.

4.6 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- Controllo di Gestione,
- Qualità.

4.7 Controlli dell'OdV

L'OdV effettua audit su:

- flussi finanziari,
- rapporti con fornitori,
- rapporti con consulenti,
- rapporti con istituti bancari,
- anomalie contabili.

Articolo 5. Indicatori di anomalia

STEP considera indicatori di possibile rischio:

- richieste di pagamento verso conti esteri non giustificati,
- richieste di pagamento verso soggetti diversi dal fornitore,

- variazioni improvvise delle coordinate bancarie,
- fornitori con assetto societario opaco,
- operazioni prive di giustificazione economica,
- compensazioni non autorizzate,
- richieste di pagamento in contanti,
- operazioni frazionate.

Articolo 6. Regole di comportamento

6.1 Divieti assoluti

È vietato:

- effettuare pagamenti non giustificati,
- effettuare pagamenti verso conti non riconducibili al fornitore,
- effettuare operazioni prive di giustificazione economica,
- utilizzare fondi aziendali per finalità personali,
- ostacolare controlli,
- alterare documenti contabili,
- occultare informazioni rilevanti.

6.2 Obblighi

È obbligatorio:

- verificare l'identità della controparte,
- verificare la coerenza economica dell'operazione,
- rispettare le procedure interne,
- documentare ogni operazione,
- segnalare anomalie,
- collaborare con l'OdV.

Articolo 7. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- anomalie nei flussi finanziari,
- variazioni delle coordinate bancarie dei fornitori,
- operazioni sospette,
- segnalazioni whistleblowing,
- report del Controllo di Gestione,
- report del Settore Contabilità.

Articolo 8. Formazione specifica

La formazione sui reati di riciclaggio è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore Contabilità,
- Settore Acquisti e Logistica,
- Settore Coattiva,

- Direzione Generale,
- Ufficio Legale.

Articolo 9. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE H – WHISTLEBLOWING (D.Lgs. 24/2023)

Articolo 1. Premessa

La presente Parte Speciale disciplina il sistema di **segnalazione interna (whistleblowing)** adottato da STEP S.r.l. in conformità al:

- **D.Lgs. 24/2023**, attuativo della Direttiva (UE) 2019/1937,
- **Linee Guida ANAC 2023**,
- **Linee Guida Confindustria 2021**,
- **D.Lgs. 231/2001**,
- **Codice Etico**,
- **Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT)**.

Il whistleblowing rappresenta un presidio fondamentale per:

- prevenire la commissione di reati,
- intercettare tempestivamente comportamenti illeciti o irregolarità,
- rafforzare la cultura della legalità,
- tutelare l'integrità aziendale,
- proteggere i segnalanti da ritorsioni,
- garantire trasparenza e accountability.

STEP adotta un sistema di segnalazione conforme ai più elevati standard europei, assicurando:

- **riservatezza**,
- **anonimato**,
- **protezione del segnalante**,
- **indipendenza dell'Organismo di Vigilanza**,
- **tracciabilità delle attività**,
- **tempestività delle verifiche**,
- **assenza di conflitti di interesse**.

Articolo 2. Normativa di riferimento

Il sistema di whistleblowing di STEP si fonda sulle seguenti norme:

2.1 D.Lgs. 24/2023

Che disciplina:

- la protezione delle persone che segnalano violazioni del diritto dell'Unione e del diritto nazionale,
- i canali interni ed esterni di segnalazione,
- la tutela contro le ritorsioni,
- gli obblighi di riservatezza,
- le modalità di gestione delle segnalazioni.

2.2 Direttiva (UE) 2019/1937

Che ha introdotto:

- standard minimi europei di protezione del segnalante,
- obblighi per le organizzazioni pubbliche e private,
- requisiti per i canali di segnalazione.

2.3 Linee Guida ANAC 2023

Che disciplinano:

- requisiti tecnici dei canali di segnalazione,

- modalità di gestione delle segnalazioni,
- misure di tutela del segnalante,
- obblighi di conservazione dei dati.

2.4 D.Lgs. 231/2001

Che prevede:

- l'obbligo di canali di segnalazione idonei,
- la tutela del segnalante,
- il divieto di ritorsione,
- l'obbligo di informazione all'OdV.

Articolo 3. Ambito di applicazione

Il sistema di whistleblowing si applica a:

- dipendenti,
- dirigenti,
- amministratori,
- collaboratori,
- consulenti,
- fornitori,
- partner,
- tirocinanti,
- volontari,
- ex dipendenti,
- candidati a posizioni lavorative.

Sono tutelate anche le persone che:

- assistono il segnalante,
- sono collegate al segnalante da un rapporto professionale,
- sono coinvolte nella segnalazione.

Articolo 4. Oggetto delle segnalazioni

Possono essere segnalate:

4.1 Violazioni del Modello 231

- comportamenti contrari alle Parti Speciali,
- violazioni delle procedure interne,
- violazioni del Codice Etico.

4.2 Reati presupposto del D.Lgs. 231/2001

- corruzione,
- peculato,
- abuso d'ufficio,
- reati societari,
- reati tributari,
- reati informatici,
- reati ambientali,
- riciclaggio,
- reati in materia di sicurezza sul lavoro,
- reati contro la proprietà intellettuale,
- reati transnazionali,

- reati specifici del settore riscossione.

4.3 Violazioni del diritto dell'Unione

- appalti pubblici,
- protezione dei dati personali,
- sicurezza delle reti e dei sistemi informativi (NIS2),
- tutela dell'ambiente,
- tutela dei consumatori.

4.4 Illeciti amministrativi, contabili, civili o disciplinari

4.5 Irregolarità, abusi, conflitti di interesse

Articolo 5. Canali di segnalazione

STEP mette a disposizione:

5.1 Canale interno digitale (principale)

- piattaforma informatica dedicata,
- accessibile da intranet e da link esterno,
- conforme ai requisiti ANAC,
- con crittografia end-to-end,
- con possibilità di segnalazione anonima,
- con tracciamento delle attività,
- con gestione separata dei dati.

5.2 Canale interno orale

- linea telefonica dedicata,
- messaggistica vocale protetta,
- incontro diretto con l'OdV.

5.3 Canale esterno ANAC

Il segnalante può rivolgersi ad ANAC quando:

- il canale interno non è attivo,
- la segnalazione interna non ha avuto seguito,
- vi è rischio di ritorsione,
- la violazione costituisce pericolo imminente o palese per l'interesse pubblico.

5.4 Divulgazione pubblica

È ammessa solo nei casi previsti dal D.Lgs. 24/2023.

Articolo 6. Gestione delle segnalazioni

La gestione delle segnalazioni è affidata all'**Organismo di Vigilanza**, che opera in piena autonomia e indipendenza.

6.1 Ricezione

L'OdV:

- riceve la segnalazione,
- verifica la completezza,
- registra la segnalazione,
- assegna un codice identificativo,
- invia un avviso di ricezione entro 7 giorni.

6.2 Istruttoria

L'OdV:

- analizza la segnalazione,

- richiede eventuali integrazioni,
- acquisisce documenti,
- effettua audizioni,
- coinvolge le funzioni competenti (senza rivelare l'identità del segnalante),
- valuta la fondatezza.

6.3 Conclusione

L'OdV:

- conclude l'istruttoria entro 3 mesi (prorogabili a 6),
- redige un rapporto finale,
- propone azioni correttive,
- propone sanzioni disciplinari,
- informa il CdA (senza rivelare l'identità del segnalante).

Articolo 7. Tutela del segnalante

STEP garantisce:

7.1 Riservatezza

È vietato rivelare:

- l'identità del segnalante,
- elementi che possano indirettamente identificarlo,
- il contenuto della segnalazione.

7.2 Protezione contro le ritorsioni

Sono vietate:

- sanzioni disciplinari,
- licenziamenti,
- demansionamenti,
- trasferimenti,
- mobbing,
- discriminazioni,
- minacce,
- pressioni.

7.3 Anonimato

Il segnalante può scegliere di:

- rimanere anonimo,
- rivelare la propria identità solo all'OdV.

7.4 Protezione dei dati personali

La gestione delle segnalazioni avviene nel rispetto del:

- GDPR,
- D.Lgs. 196/2003,
- Linee Guida del Garante Privacy.

Articolo 8. Obblighi del segnalante

Il segnalante deve:

- agire in buona fede,
- fornire informazioni veritiere,
- non utilizzare il canale per finalità personali,

- non effettuare segnalazioni diffamatorie.

Articolo 9. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- tutte le segnalazioni ricevute,
- documentazione istruttoria,
- report periodici,
- esiti delle verifiche,
- misure correttive adottate,
- sanzioni disciplinari applicate.

Articolo 10. Formazione specifica

La formazione sul whistleblowing è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- tutti i dipendenti,
- dirigenti,
- responsabili di settore,
- Ufficio Legale,
- Risorse Umane.

Articolo 11. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE I – REATI CONTRO LA PROPRIETÀ INDUSTRIALE E INTELLETTUALE

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e tecnici finalizzati a prevenire la commissione dei **reati contro la proprietà industriale e intellettuale**, categoria di reati rilevante ai fini del D.Lgs. 231/2001 e particolarmente significativa per STEP S.r.l. in ragione:

- dell'utilizzo di **software proprietari**, applicativi gestionali e piattaforme informatiche protette da licenze d'uso;
- della gestione di **banche dati tributarie**, contenenti informazioni tutelate dal diritto d'autore;
- dell'utilizzo di **sistemi di georeferenziazione, digitalizzazione e notificazione** protetti da copyright;
- dell'utilizzo di **marchi, loghi, documentazione tecnica e contenuti digitali** protetti da diritti di proprietà industriale;
- della gestione di **fornitori IT** e contratti di licenza;
- della necessità di garantire **conformità alle normative sul copyright**, sulle licenze software e sulla tutela dei segreti aziendali.

La prevenzione dei reati contro la proprietà industriale e intellettuale è un presidio essenziale per la tutela dell'integrità aziendale, della reputazione della Società e della conformità contrattuale con i fornitori IT e gli enti pubblici affidanti.

Articolo 2. Normativa di riferimento

I reati contro la proprietà industriale e intellettuale rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dall'art. 25-novies del Decreto e comprendono, tra gli altri:

2.1 Contraffazione, alterazione o uso illecito di marchi o segni distintivi (art. 473 c.p.)

Consiste nella:

- contraffazione,
- alterazione,
- uso illecito

di marchi, loghi, brevetti, modelli o disegni industriali.

2.2 Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

Consiste nell'importazione, detenzione o commercializzazione di prodotti recanti marchi contraffatti.

2.3 Violazione del diritto d'autore (artt. 171–171-ter L. 633/1941)

Include:

- duplicazione abusiva di software,
- installazione non autorizzata di programmi,
- diffusione di contenuti protetti,
- riproduzione non autorizzata di banche dati,
- utilizzo di documentazione tecnica protetta.

2.4 Reati in materia di segreti commerciali (art. 623 c.p.)

Consiste nella rivelazione o utilizzazione di segreti aziendali o informazioni riservate.

2.5 Normativa europea e nazionale di riferimento

- Direttiva 2004/48/CE (enforcement dei diritti di proprietà intellettuale)
- Regolamento (UE) 2017/1001 (marchio dell'Unione Europea)
- Codice della Proprietà Industriale (D.Lgs. 30/2005)
- Legge sul diritto d'autore (L. 633/1941)

- Normativa sulle licenze software (EULA, SLA, contratti di licenza)

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati contro la proprietà industriale e intellettuale:

3.1 Gestione delle licenze software

- acquisto di licenze,
- installazione dei programmi,
- gestione dei contratti di licenza,
- rinnovi,
- verifiche di conformità.

3.2 Gestione delle banche dati tributarie

- accesso ai dati,
- estrazione di report,
- utilizzo dei dati per finalità istituzionali,
- divieto di duplicazione non autorizzata.

3.3 Gestione dei sistemi di digitalizzazione e notificazione

- utilizzo di software proprietari,
- gestione delle API,
- gestione dei sistemi di georeferenziazione,
- gestione dei sistemi di firma digitale.

3.4 Gestione dei contenuti digitali

- documentazione tecnica,
- manuali,
- modelli,
- template,
- loghi e marchi.

3.5 Gestione dei rapporti con fornitori IT

- contratti di licenza,
- contratti di manutenzione,
- contratti di sviluppo software,
- contratti di assistenza.

3.6 Gestione dei segreti aziendali

- algoritmi,
- procedure interne,
- know-how,
- documentazione riservata.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati contro la proprietà industriale e intellettuale includono:

4.1 Segregazione delle funzioni

- chi acquista software non lo installa,
- chi installa non autorizza,
- chi autorizza non controlla.

4.2 Gestione centralizzata degli acquisti IT

Tutti gli acquisti di software e licenze sono gestiti dal:

- Settore IT e Digitalizzazione,
- Settore Acquisti e Logistica.

4.3 Inventario delle licenze

STEP mantiene un inventario aggiornato di:

- software installati,
- licenze attive,
- licenze scadute,
- licenze in rinnovo.

4.4 Procedure formalizzate

STEP adotta procedure che disciplinano:

- installazione software,
- gestione delle licenze,
- gestione dei fornitori IT,
- gestione dei contenuti digitali,
- gestione dei segreti aziendali.

4.5 Controlli di linea

Effettuati da:

- Settore IT e Digitalizzazione,
- Settore Postale e Digitalizzazione.

4.6 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- Qualità,
- DPO (per i dati personali).

4.7 Controlli dell'OdV

L'OdV effettua audit su:

- licenze software,
- installazioni,
- contratti IT,
- gestione dei contenuti digitali,
- gestione delle banche dati.

Articolo 5. Regole di comportamento

5.1 Divieti assoluti

È vietato:

- installare software non autorizzati,
- utilizzare licenze scadute o non valide,
- duplicare software senza autorizzazione,
- condividere contenuti protetti,
- utilizzare loghi o marchi senza autorizzazione,
- divulgare segreti aziendali,
- utilizzare banche dati per finalità non istituzionali,
- esportare dati senza titolo,
- alterare documentazione tecnica protetta.

5.2 Obblighi

È obbligatorio:

- utilizzare solo software autorizzati,
- rispettare i contratti di licenza,
- segnalare anomalie,
- proteggere i segreti aziendali,
- rispettare le procedure interne,
- collaborare con l'OdV.

Articolo 6. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- inventario delle licenze,
- contratti IT,
- report sulle installazioni,
- segnalazioni di anomalie,
- segnalazioni whistleblowing,
- report del Settore IT.

Articolo 7. Formazione specifica

La formazione sui reati contro la proprietà industriale e intellettuale è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore IT e Digitalizzazione,
- Settore Postale e Digitalizzazione,
- Settore Tributi Maggiori,
- Settore Tributi Minori,
- Settore Coattiva.

Articolo 8. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE J – REATI TRANSNAZIONALI

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e comportamentali finalizzati a prevenire la commissione dei **reati transnazionali**, categoria di reati rilevante ai fini del D.Lgs. 231/2001 e disciplinata dalla Legge 146/2006.

I reati transnazionali assumono particolare rilevanza per STEP S.r.l. in ragione:

- della gestione di **fornitori esteri**, in particolare nel settore IT, cloud, cybersecurity e servizi digitali;
- dell'utilizzo di **piattaforme informatiche e servizi cloud** con server localizzati in Paesi UE ed extra-UE;
- della gestione di **flussi di dati personali e tributari** che possono essere trasferiti all'estero;
- della gestione di **pagamenti internazionali** verso fornitori o partner;
- della gestione di **rapporti contrattuali con società multinazionali**;
- della necessità di garantire **conformità alle normative europee e internazionali** in materia di sicurezza informatica, privacy, antiriciclaggio e tutela dei dati;
- della crescente esposizione ai rischi di **cybercrime transnazionale**, frodi informatiche e traffico illecito di dati.

La prevenzione dei reati transnazionali è un presidio essenziale per la tutela dell'integrità aziendale, della reputazione della Società e della conformità alle normative internazionali.

Articolo 2. Normativa di riferimento

I reati transnazionali rilevanti ai fini del D.Lgs. 231/2001 sono disciplinati dalla **Legge 146/2006**, che recepisce la Convenzione ONU contro la criminalità organizzata transnazionale (c.d. "Convenzione di Palermo").

Sono considerati reati transnazionali quelli che:

- coinvolgono più di uno Stato,
- sono commessi in uno Stato ma hanno effetti sostanziali in un altro,
- sono commessi da un gruppo criminale operante in più Stati,
- implicano trasferimenti di beni, persone o dati tra Stati.

2.1 Reati transnazionali rilevanti per STEP

2.1.1 Associazione per delinquere (art. 416 c.p.)

Quando finalizzata alla commissione di reati transnazionali.

2.1.2 Associazione di tipo mafioso (art. 416-bis c.p.)

Quando operante in più Stati.

2.1.3 Riciclaggio e autoriciclaggio transnazionale

Quando coinvolgono flussi finanziari esteri.

2.1.4 Frode informatica transnazionale (art. 640-ter c.p.)

Quando coinvolge sistemi informatici localizzati all'estero.

2.1.5 Traffico illecito di dati

Quando i dati sono trasferiti o venduti all'estero.

2.1.6 Reati informatici transfrontalieri

- accesso abusivo a sistemi esteri,
- attacchi informatici provenienti dall'estero,
- diffusione di malware transnazionale.

2.2 Normativa europea e internazionale

- **Regolamento UE 2016/679 (GDPR)** – trasferimenti extra-UE
- **Direttiva NIS2 (UE 2022/2555)** – sicurezza informatica
- **Regolamento (UE) 2023/1113** – trasferimenti di fondi
- **Convenzione di Budapest sul cybercrime**
- **Convenzione ONU contro la criminalità organizzata transnazionale**

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati transnazionali:

3.1 Gestione dei fornitori esteri

- fornitori IT,
- fornitori cloud,
- fornitori di cybersecurity,
- fornitori di servizi digitali,
- fornitori di software proprietari.

3.2 Gestione dei trasferimenti di dati all'estero

- trasferimenti verso Paesi UE,
- trasferimenti verso Paesi extra-UE,
- utilizzo di server localizzati all'estero,
- utilizzo di piattaforme cloud internazionali.

3.3 Gestione dei pagamenti internazionali

- bonifici esteri,
- pagamenti verso fornitori esteri,
- pagamenti in valuta estera.

3.4 Gestione dei contratti con società multinazionali

- contratti di licenza software,
- contratti di manutenzione,
- contratti di assistenza,
- contratti di cloud computing.

3.5 Gestione dei sistemi informatici con componenti estere

- sistemi di sicurezza,
- firewall,
- sistemi di logging,
- sistemi di backup,
- piattaforme di digitalizzazione.

3.6 Gestione dei flussi finanziari transnazionali

- pagamenti,
- riconciliazioni,
- rendicontazioni.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati transnazionali includono:

4.1 Due diligence rafforzata sui fornitori esteri

STEP verifica:

- identità del fornitore,

- sede legale,
- autorizzazioni,
- reputazione,
- eventuali procedimenti giudiziari,
- titolarità effettiva,
- conformità GDPR,
- conformità NIS2.

4.2 Verifica dei trasferimenti di dati all'estero

STEP verifica:

- base giuridica del trasferimento,
- presenza di garanzie adeguate (SCC, BCR),
- localizzazione dei server,
- misure di sicurezza adottate dal fornitore,
- conformità alle Linee Guida EDPB.

4.3 Tracciabilità dei flussi finanziari

Ogni operazione deve essere:

- documentata,
- verificabile,
- archiviata,
- accessibile all'OdV.

4.4 Procedure formalizzate

STEP adotta procedure che disciplinano:

- gestione dei fornitori esteri,
- gestione dei trasferimenti di dati,
- gestione dei pagamenti internazionali,
- gestione dei contratti IT,
- gestione dei sistemi informatici.

4.5 Controlli di linea

Effettuati da:

- Settore Contabilità,
- Settore Acquisti e Logistica,
- Settore IT e Digitalizzazione.

4.6 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- DPO,
- Punto di Contatto ACN/NIS2,
- Qualità.

4.7 Controlli dell'OdV

L'OdV effettua audit su:

- fornitori esteri,
- contratti internazionali,
- trasferimenti di dati,
- pagamenti esteri,
- anomalie informatiche.

Articolo 5. Indicatori di anomalia

STEP considera indicatori di possibile rischio:

- fornitori con sede in Paesi ad alto rischio,
- richieste di pagamento verso conti esteri non giustificati,
- variazioni improvvise delle coordinate bancarie,
- trasferimenti di dati non autorizzati,
- utilizzo di server extra-UE senza garanzie adeguate,
- richieste di accesso ai sistemi da parte di soggetti esteri,
- operazioni prive di giustificazione economica,
- contratti IT con clausole opache.

Articolo 6. Regole di comportamento

6.1 Divieti assoluti

È vietato:

- effettuare pagamenti verso conti esteri non verificati,
- trasferire dati all'estero senza autorizzazione,
- utilizzare fornitori esteri non verificati,
- installare software provenienti da fonti non ufficiali,
- ostacolare controlli,
- alterare documenti,
- occultare informazioni rilevanti.

6.2 Obblighi

È obbligatorio:

- verificare l'identità della controparte,
- verificare la localizzazione dei server,
- rispettare le procedure interne,
- documentare ogni operazione,
- segnalare anomalie,
- collaborare con l'OdV.

Articolo 7. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- contratti con fornitori esteri,
- report sui trasferimenti di dati,
- report del DPO,
- report del Punto di Contatto ACN/NIS2,
- anomalie nei flussi finanziari,
- segnalazioni whistleblowing.

Articolo 8. Formazione specifica

La formazione sui reati transnazionali è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,

- verificata tramite test.

Destinatari prioritari:

- Settore IT e Digitalizzazione,
- Settore Acquisti e Logistica,
- Settore Contabilità,
- Ufficio Legale,
- DPO,
- Punto di Contatto ACN/NIS2.

Articolo 9. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

PARTE SPECIALE K – REATI SPECIFICI DEL SETTORE RISCOSSIONE ENTRATE E TRIBUTI LOCALI

Articolo 1. Premessa

La presente Parte Speciale disciplina i presidi organizzativi, procedurali e comportamentali finalizzati a prevenire la commissione dei **reati specificamente connessi alle attività di gestione, accertamento e riscossione delle entrate e dei tributi locali**, settore nel quale STEP S.r.l. opera in regime di affidamento da parte degli enti locali.

Questa Parte Speciale rappresenta un elemento **distintivo** del Modello STEP, poiché:

- integra le Parti Speciali generali con presidi specifici del settore;
- recepisce le peculiarità operative della riscossione;
- tiene conto della natura pubblicistica delle attività svolte;
- considera la gestione di dati sensibili e giudiziari dei contribuenti;
- considera la gestione di flussi finanziari pubblici;
- considera la gestione di atti amministrativi e procedimenti coattivi;
- considera la gestione di rapporti con contribuenti, enti locali, autorità giudiziarie e forze dell'ordine.

La prevenzione dei reati in questo ambito è essenziale per:

- tutelare la legalità dell'azione amministrativa delegata;
- garantire la trasparenza nei confronti degli enti affidanti;
- proteggere i contribuenti;
- preservare la reputazione della Società;
- assicurare la correttezza dei flussi finanziari;
- evitare responsabilità penali e amministrative.

Articolo 2. Normativa di riferimento

I reati rilevanti in questo ambito includono:

2.1 Reati contro la Pubblica Amministrazione

(già trattati nella Parte Speciale A, ma qui riletti in chiave settoriale)

- peculato (art. 314 c.p.),
- abuso d'ufficio (art. 323 c.p.),
- corruzione (artt. 318–322 c.p.),
- induzione indebita (art. 319-quater c.p.),
- truffa ai danni dello Stato (art. 640, comma 2, n. 1 c.p.),
- frode nelle pubbliche forniture (art. 356 c.p.).

2.2 Reati tributari

(già trattati nella Parte Speciale C, ma qui riletti in chiave settoriale)

- dichiarazione fraudolenta,
- dichiarazione infedele,
- omessa dichiarazione,
- indebita compensazione,
- emissione o utilizzo di fatture false,
- occultamento o distruzione di documenti contabili.

2.3 Reati informatici

(già trattati nella Parte Speciale D, ma qui riletti in chiave settoriale)

- accesso abusivo a banche dati tributarie,
- manipolazione di posizioni debitorie,

- alterazione di atti,
- cancellazione di dati,
- diffusione illecita di dati dei contribuenti.

2.4 Reati di riciclaggio e autoriciclaggio

(già trattati nella Parte Speciale G)

- manipolazione dei flussi finanziari,
- utilizzo improprio di somme riscosse,
- occultamento di fondi pubblici.

2.5 Reati specifici del settore riscossione

Pur non essendo tipizzati come "reati di settore", la giurisprudenza e la prassi individuano condotte tipiche:

- manipolazione delle posizioni debitorie,
- cancellazione indebita di carichi,
- alterazione di atti di accertamento,
- alterazione di atti di riscossione,
- favoritismi verso contribuenti,
- omessa rendicontazione,
- ritardato riversamento,
- utilizzo improprio di somme riscosse,
- accesso abusivo alle banche dati tributarie,
- notifiche irregolari o simulate,
- gestione impropria delle rateizzazioni,
- gestione impropria delle sospensioni,
- gestione impropria delle sanzioni.

Articolo 3. Attività sensibili

L'analisi dei processi aziendali ha individuato le seguenti attività sensibili ai fini della prevenzione dei reati specifici del settore:

3.1 Accertamento delle entrate

- analisi delle banche dati,
- incrocio delle informazioni,
- emissione degli avvisi,
- gestione delle rettifiche,
- gestione delle esenzioni,
- gestione delle agevolazioni.

3.2 Liquidazione dei tributi

- calcolo degli importi,
- applicazione delle aliquote,
- applicazione delle sanzioni,
- applicazione degli interessi,
- gestione delle riduzioni.

3.3 Riscossione ordinaria

- gestione dei pagamenti,
- gestione delle rateizzazioni,
- gestione delle sospensioni,
- gestione delle compensazioni,

- gestione delle posizioni debitorie.

3.4 Riscossione coattiva

- emissione degli atti esecutivi,
- ingiunzioni,
- pignoramenti,
- fermi amministrativi,
- ipoteche,
- gestione delle opposizioni,
- gestione dei rapporti con l'autorità giudiziaria.

3.5 Gestione delle banche dati tributarie

- accesso,
- consultazione,
- aggiornamento,
- estrazione di report,
- gestione delle interrogazioni massive.

3.6 Gestione delle notifiche

- notifiche digitali,
- notifiche postali,
- notifiche tramite messo notificatore,
- gestione delle relate,
- gestione delle compiute giacenze.

3.7 Gestione dei flussi finanziari

- incassi,
- riversamenti,
- rendicontazioni,
- riconciliazioni bancarie.

3.8 Gestione dei rapporti con i contribuenti

- sportello fisico,
- sportello digitale,
- richieste di chiarimento,
- reclami,
- istanze di autotutela.

3.9 Gestione dei rapporti con gli enti locali

- convenzioni,
- report periodici,
- ispezioni,
- audit,
- richieste di chiarimento.

Articolo 4. Presidi di controllo

I presidi di controllo adottati da STEP per prevenire i reati specifici del settore includono:

4.1 Segregazione delle funzioni

- chi accerta non riscuote,
- chi riscuote non contabilizza,
- chi contabilizza non autorizza,

- chi autorizza non controlla,
- chi controlla non modifica le posizioni debitorie.

4.2 Tracciabilità delle operazioni

Ogni attività deve essere:

- documentata,
- verificabile,
- archiviata,
- accessibile all'OdV.

4.3 Gestione centralizzata delle credenziali

- profili differenziati,
- accessi minimi necessari,
- revoca immediata degli accessi,
- logging delle operazioni.

4.4 Procedure formalizzate

STEP adotta procedure che disciplinano:

- accertamento,
- liquidazione,
- riscossione ordinaria,
- riscossione coattiva,
- notifiche,
- gestione delle banche dati,
- gestione dei flussi finanziari,
- gestione delle rateizzazioni,
- gestione delle sospensioni,
- gestione delle compensazioni.

4.5 Controlli di linea

Effettuati da:

- Settore Tributi Maggiori,
- Settore Tributi Minori,
- Settore Coattiva,
- Settore Contabilità.

4.6 Controlli di secondo livello

Effettuati da:

- Ufficio Legale,
- Qualità,
- DPO (per i dati personali),
- Punto di Contatto ACN/NIS2 (per la sicurezza informatica).

4.7 Controlli dell'OdV

L'OdV effettua audit su:

- accertamento,
- riscossione,
- notifiche,
- flussi finanziari,
- rapporti con i contribuenti,
- rapporti con gli enti locali,
- gestione delle banche dati.

Articolo 5. Rischi tipici del settore

STEP considera rischi tipici:

- manipolazione delle posizioni debitorie,
- cancellazione indebita di carichi,
- alterazione di atti,
- favoritismi verso contribuenti,
- accesso abusivo alle banche dati,
- notifiche simulate o irregolari,
- gestione impropria delle rateizzazioni,
- gestione impropria delle sospensioni,
- gestione impropria delle compensazioni,
- ritardato riversamento,
- omessa rendicontazione,
- utilizzo improprio di somme riscosse.

Articolo 6. Regole di comportamento

6.1 Divieti assoluti

È vietato:

- modificare posizioni debitorie senza titolo,
- cancellare carichi senza autorizzazione,
- alterare atti,
- manipolare dati,
- favorire contribuenti,
- accedere alle banche dati senza titolo,
- effettuare notifiche irregolari,
- utilizzare somme riscosse per finalità non istituzionali,
- ritardare o omettere riversamenti,
- ostacolare ispezioni,
- occultare informazioni,
- utilizzare informazioni riservate per fini personali.

6.2 Obblighi

È obbligatorio:

- rispettare le procedure interne,
- documentare ogni attività,
- utilizzare solo canali ufficiali,
- segnalare anomalie,
- collaborare con l'OdV,
- rispettare i tempi di riversamento,
- garantire la correttezza delle notifiche,
- garantire la correttezza delle posizioni debitorie.

Articolo 7. Flussi informativi verso l'OdV

Devono essere trasmessi all'OdV:

- report su accertamento e riscossione,
- report sulle notifiche,
- report sui flussi finanziari,

- report sulle rateizzazioni,
- report sulle sospensioni,
- report sulle compensazioni,
- segnalazioni di anomalie,
- segnalazioni whistleblowing,
- verbali di ispezione degli enti locali.

Articolo 8. Formazione specifica

La formazione sui reati specifici del settore è:

- obbligatoria,
- annuale,
- modulata per ruolo,
- documentata,
- verificata tramite test.

Destinatari prioritari:

- Settore Tributi Maggiori,
- Settore Tributi Minori,
- Settore Coattiva,
- Settore Contabilità,
- Settore Postale e Digitalizzazione,
- Ufficio Legale.

Articolo 9. Responsabilità e sanzioni

La violazione delle regole contenute nella presente Parte Speciale comporta:

- sanzioni disciplinari,
- sanzioni contrattuali,
- segnalazione all'OdV,
- segnalazione al CdA,
- eventuale segnalazione all'autorità giudiziaria.

ALLEGATO 1 – ORGANIGRAMMA AZIENDALE

L'organigramma di STEP S.r.l., aggiornato al 12 marzo 2026, rappresenta la struttura organizzativa attraverso la quale la Società esercita le proprie funzioni operative, amministrative, tecniche e di controllo. Esso costituisce parte integrante del Modello 231, poiché definisce ruoli, responsabilità, linee di riporto e ambiti di competenza, garantendo la chiarezza delle funzioni e la corretta segregazione dei compiti.

Al vertice della struttura si colloca il **Consiglio di Amministrazione**, composto da Salvatore Foddai e Andrea Chiandotto, con le parti di supporto Silvia Frassetto, Giorgio Zavattaro e Simone Razzu. Il Consiglio esercita le funzioni di indirizzo strategico e di supervisione complessiva dell'ente.

È istituito il **Comitato Parità di Genere**, presieduto da Silvia Frassetto e Salvatore Foddai, con funzioni di monitoraggio e promozione delle politiche di equità e inclusione.

Il **Collegio Sindacale** esercita le funzioni di controllo contabile e di vigilanza sull'osservanza delle norme.

ALLEGATO 2 – SISTEMA DELLE DELEGHE E PROCURE

Il sistema delle deleghe e procure di STEP è strutturato in modo da garantire coerenza tra i poteri attribuiti e le responsabilità operative, assicurando che ogni funzione sia esercitata da soggetti dotati delle competenze necessarie e che ogni potere sia tracciabile e verificabile.

Le **deleghe interne** definiscono i poteri gestionali attribuiti ai responsabili di settore, ai dirigenti e ai coordinatori. Esse riguardano, tra l'altro, la gestione del personale, la firma di atti amministrativi, la gestione dei rapporti con gli enti locali, la supervisione delle attività di riscossione, la gestione dei sistemi informatici e la validazione dei dati contabili.

Le **procure notarili** attribuiscono poteri di rappresentanza verso terzi, con particolare riferimento alla firma di contratti, alla partecipazione a gare pubbliche, alla gestione dei rapporti con la Pubblica Amministrazione e alla sottoscrizione di atti aventi rilevanza esterna. I procuratori generali e speciali sono individuati nell'organigramma e operano entro i limiti stabiliti dalle procure depositate.

Il sistema delle deleghe e procure è integrato nel Modello 231 e costituisce un presidio essenziale per la prevenzione dei reati, poiché garantisce la chiarezza dei poteri, la responsabilità delle decisioni e la tracciabilità delle attività.

ALLEGATO 3 – PROCEDURE INTERNE COLLEGATE AL MODELLO

Le procedure interne rappresentano lo strumento operativo attraverso il quale STEP attua concretamente il Modello 231. Esse disciplinano i processi sensibili, definiscono i controlli, stabiliscono le responsabilità e garantiscono la tracciabilità delle attività.

Tra le procedure rilevanti ai fini del Modello si segnalano:

– la procedura di gestione delle gare e degli appalti;
– la procedura di gestione dei rapporti con la Pubblica Amministrazione;
– la procedura di accertamento e riscossione dei tributi;
– la procedura di gestione dei pagamenti e dei flussi finanziari;
– la procedura di gestione delle banche dati tributarie;
– la procedura di gestione dei sistemi informatici e della sicurezza informatica;
– la procedura di gestione dei reclami e delle segnalazioni;
– la procedura di gestione del whistleblowing;
– la procedura di gestione della sicurezza sul lavoro;
– la procedura di gestione della privacy e del trattamento dei dati personali;
– la procedura di gestione della qualità e delle certificazioni.

Ogni procedura è soggetta a revisione periodica e deve essere coerente con il Modello 231, con il Codice Etico e con il PTPCT.

ALLEGATO 4 – SCHEMA DI RACCORDO MODELLO–ORGANIGRAMMA–PROCEDURE

Il presente allegato illustra il raccordo tra il Modello 231, l'organigramma e le procedure interne, evidenziando la coerenza tra i presidi organizzativi, i poteri attribuiti e i controlli previsti.
Il Modello individua i processi sensibili e definisce i principi di comportamento e i presidi di controllo. L'organigramma assegna le responsabilità operative e garantisce la segregazione delle funzioni. Le procedure interne disciplinano le attività e definiscono i controlli operativi.
Il raccordo tra questi elementi assicura:
– la tracciabilità delle decisioni;
– la responsabilità delle funzioni;
– la prevenzione dei conflitti di interesse;
– la coerenza tra poteri e responsabilità;
– la prevenzione dei reati;
– la piena attuazione del Modello 231.

ALLEGATO 5 – MAPPATURA DEI PROCESSI SENSIBILI 231

La mappatura dei processi sensibili rappresenta uno degli elementi cardine del Modello 231, poiché consente di individuare le attività aziendali nelle quali, per natura, complessità o modalità operative, può manifestarsi un rischio di commissione dei reati previsti dal D.Lgs. 231/2001.
La mappatura è stata effettuata analizzando l'organigramma aggiornato al 12 marzo 2026, le deleghe e procure, le procedure interne e i flussi operativi dei settori aziendali. L'analisi ha coinvolto i responsabili di settore, la Direzione Generale, l'Ufficio Legale, il Responsabile Anticorruzione – ODV, il DPO, il RSPP e le funzioni trasversali.
Dall'analisi sono emerse le seguenti macro-aree di rischio:

1. Processi connessi ai rapporti con la Pubblica Amministrazione

Rientrano in questa categoria le attività di partecipazione a gare e appalti, la gestione delle convenzioni con gli enti locali, la rendicontazione dei servizi, la gestione delle ispezioni e dei rapporti istituzionali. Tali attività coinvolgono principalmente il Settore Gare e Appalti, il Settore Commerciale, la Direzione Generale e l'Ufficio Legale.

2. Processi connessi alla gestione delle entrate e dei tributi locali

Le attività di accertamento, liquidazione, riscossione ordinaria e coattiva, gestione delle banche dati tributarie, emissione degli atti e gestione dei pagamenti costituiscono un'area di rischio elevato. Sono coinvolti i Settori Tributi Maggiori, Tributi Minori, Coattiva, Contabilità, Postale e Digitalizzazione.

3. Processi contabili, finanziari e societari

La formazione del bilancio, la gestione dei flussi finanziari, la predisposizione delle comunicazioni societarie e i rapporti con il Collegio Sindacale e la società di revisione coinvolgono il Settore Contabilità, la Direzione Generale e l'Ufficio Legale.

4. Processi informatici e trattamento dei dati personali

La gestione dei sistemi informatici, delle credenziali di accesso, delle banche dati tributarie e dei sistemi di digitalizzazione coinvolge il Settore IT e Sviluppo, il Settore Postale e Digitalizzazione, il DPO e il Punto di Contatto ACN – NIS2.

5. Processi di gestione del personale

La selezione, l'assunzione, la gestione delle presenze, la formazione e la valutazione del personale coinvolgono il Settore Risorse Umane e la Direzione Generale.

6. Processi di acquisto di beni e servizi
La selezione dei fornitori, la gestione dei contratti, gli ordini e i pagamenti coinvolgono il Settore Acquisti e Logistica, la Contabilità e la Direzione Generale.
7. Processi di sicurezza sul lavoro
La valutazione dei rischi, la gestione dei DPI, la formazione obbligatoria e la sorveglianza sanitaria coinvolgono il RSPP, il Medico Competente, i RLS e la Direzione Generale.
8. Processi di gestione delle segnalazioni (whistleblowing)
La ricezione, analisi e gestione delle segnalazioni coinvolge l'Organismo di Vigilanza e l'Ufficio Legale.
La mappatura è soggetta a revisione periodica e costituisce un allegato dinamico del Modello 231.

ALLEGATO 6 – REGISTRO DEI RISCHI 231

Il Registro dei Rischi 231 rappresenta lo strumento attraverso il quale STEP valuta, classifica e monitora i rischi di commissione dei reati previsti dal D.Lgs. 231/2001. Esso integra la mappatura dei processi sensibili e consente di individuare i presidi di controllo necessari.
La metodologia adottata da STEP prevede:
1. Identificazione del rischio
Per ogni processo sensibile viene individuato il potenziale reato applicabile, sulla base del catalogo previsto dal D.Lgs. 231/2001 e delle attività svolte.
2. Valutazione del rischio
Il rischio viene valutato considerando la probabilità di accadimento e l'impatto potenziale, tenendo conto della natura del processo, della complessità operativa, del livello di esposizione verso la Pubblica Amministrazione e della sensibilità dei dati trattati.
3. Valutazione dei controlli esistenti
Per ogni processo vengono analizzati i presidi già in essere, quali procedure interne, segregazione delle funzioni, controlli informatici, verifiche contabili, supervisione dei responsabili di settore e controlli dell'OdV.
4. Determinazione del rischio residuo
Il rischio residuo rappresenta il livello di rischio che permane dopo l'applicazione dei controlli esistenti.
5. Individuazione delle azioni di miglioramento
Per i processi con rischio residuo medio o elevato vengono individuate azioni correttive, quali aggiornamento delle procedure, rafforzamento dei controlli, formazione del personale o revisione delle deleghe.
Il Registro dei Rischi è aggiornato annualmente dall'OdV, in collaborazione con la Direzione Generale e i responsabili di settore.