Sistema Qualità
Sistema di Gestione
Ambientale
ISO 9001
ISO 14001
www.dekra-seal.com
DEKRA certificato

OLAB S.r.l.
Via Cavallera, 2
25030, Torbole Casaglia (BS) - Italy
Tel. +39 030 2159411

C.C.I.A.A. 309654
C.F. 02963700170 **P. IVA** IT 02963700170
Registro Società Tribunale BS 38321
Cap. Soc. 1.820.000,00 Euro i.v.
www.olab.it | olab@olab.it

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

GLOBAL POLICY

PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE (IA)

E PARTE SPECIALE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D.LGS. 231/2001

Approvato con delibera del Consiglio di Amministrazione del [-] dicembre 2025

INDICE

1. PREMESSA E CONTESTO STRATEGICO

La presente Policy Aziendale per l'Utilizzo dell'Intelligenza Artificiale (di seguito "Policy IA") è adottata da OLAB (la "Società") quale strumento di governo responsabile dell'innovazione tecnologica, in un contesto industriale caratterizzato da elevati requisiti di affidabilità, sicurezza, continuità produttiva e responsabilità del produttore.
La Società è leader nei settori del fluid control e della refrigerazione sostenibile, occupandosi direttamente, con passione e impegno costante, nella progettazione, produzione e commercializzazione di componenti meccanici ed elettromeccanici destinati a impieghi industriali e retail nei quali errori progettuali, produttivi o di controllo possono generare conseguenze rilevanti sotto il profilo della sicurezza, della responsabilità civile e penale e della reputazione aziendale.
In tale contesto, l'Intelligenza Artificiale rappresenta un'opportunità di efficientamento e supporto decisionale, ma anche una fonte di nuovi rischi tecnologici, organizzativi e legali che devono essere presidiati attraverso regole chiare, controlli adeguati e responsabilità definite.

---

2. FINALITÀ, VALORE GIURIDICO E AMBITO DI APPLICAZIONE

2.1 Finalità

La presente Policy IA persegue le seguenti finalità:

- garantire un utilizzo dell'IA conforme alla normativa vigente;
- tutelare la sicurezza dei prodotti, dei processi e dei lavoratori;
- preservare il controllo umano sulle decisioni tecniche rilevanti;
- proteggere il patrimonio informativo, tecnologico e industriale;
- prevenire i rischi di responsabilità amministrativa ex D.Lgs. 231/2001.

2.2 Valore giuridico

La Policy costituisce regolamento interno vincolante e integra il Codice Etico, il Modello 231, il sistema di gestione della qualità, il DVR e le policy IT e cybersecurity.

2.3 Ambito soggettivo e oggettivo

La Policy IA si applica a dipendenti, dirigenti, amministratori, collaboratori, consulenti e fornitori che operano per conto della Società.

3. QUADRO NORMATIVO DI RIFERIMENTO

La presente Policy IA è adottata nell'ambito dei seguenti provvedimenti:

- D.Lgs. 231/2001;
- Regolamento UE 679/2016 (GDPR);
- Regolamento (UE) 2024/1689 – Artificial Intelligence Act dell'Unione Europea, noto anche come EU AI Act o AI Act – entrato in vigore dal 1° agosto 2024;
- normativa su sicurezza dei prodotti e responsabilità del produttore;
- normativa generale e di settore su salute e sicurezza sul lavoro;
- normativa generale e di settore su segreti industriali e concorrenza;
- normative generale e di settore in materia di cybersecurity.

---

4. DEFINIZIONI E CLASSIFICAZIONE DEI SISTEMI IA

4.1 Definizioni

Ai fini della presente Policy IA, si applicano le seguenti definizioni operative, redatte al fine di garantire chiarezza interpretativa e uniformità applicativa all'interno dell'organizzazione aziendale:

- **Intelligenza Artificiale (IA):** qualsiasi sistema software, hardware o combinato, sviluppato o utilizzato dalla Società o dagli Utilizzatori, in grado di elaborare dati, informazioni o segnali e di generare output quali previsioni, raccomandazioni, analisi, classificazioni o contenuti, con un livello di autonomia parziale o assistita, sulla base di modelli algoritmici, statistici o di apprendimento automatico.

- **IA generativa:** sistemi di Intelligenza Artificiale progettati per generare nuovi contenuti (testi, immagini, codice, modelli, schemi concettuali) a partire da input forniti dall'utilizzatore, inclusi chatbot, assistenti virtuali e strumenti di supporto alla progettazione.

- **Sistema di IA autorizzato**: sistema di Intelligenza Artificiale che sia stato preventivamente valutato sotto il profilo tecnico, organizzativo, di sicurezza informatica e di conformità normativa, e formalmente approvato dalla Società secondo la procedura interna di autorizzazione.

- **Utilizzatore**: qualsiasi soggetto che, a qualunque titolo (dipendente, dirigente, amministratore, consulente, fornitore), utilizzi sistemi di IA nell'ambito o per finalità riconducibili all'attività della Società.

- **Dati industriali riservati**: l'insieme delle informazioni tecniche, tecnologiche, produttive e commerciali della Società, incluse a titolo esemplificativo e non esaustivo: disegni tecnici, modelli CAD, schemi elettrici, distinte base, parametri di progetto, parametri di collaudo, processi produttivi, specifiche di prodotto, know-how e informazioni strategiche.

4.2 Classificazione dei sistemi di IA in base al rischio

Al fine di garantire un utilizzo consapevole e proporzionato dell'Intelligenza Artificiale, la Società adotta una classificazione interna dei sistemi di IA basata sul livello di rischio potenziale associato al loro utilizzo, tenendo conto dell'impatto sui processi aziendali, sulla sicurezza dei prodotti e sulla responsabilità del produttore.

a) Sistemi di IA a basso rischio
Rientrano in questa categoria i sistemi di IA utilizzati per attività di supporto amministrativo, documentale o informativo, che non incidono direttamente su decisioni tecniche, produttive o di sicurezza. Tali sistemi possono essere utilizzati, previa autorizzazione espressa, nel rispetto della presente Policy IA e delle policy IT aziendali.

b) Sistemi di IA a rischio medio
Rientrano in questa categoria i sistemi di IA utilizzati come supporto alle attività tecniche, produttive o organizzative, inclusi il supporto alla progettazione concettuale, l'analisi dei dati di produzione, la manutenzione predittiva e l'analisi di trend qualitativi. L'utilizzo di tali sistemi richiede sempre supervisione e validazione umana qualificata.

c) Sistemi di IA ad alto rischio
Rientrano in questa categoria i sistemi di IA che, anche solo potenzialmente, possono incidere sulla sicurezza dei prodotti, dei lavoratori o dei clienti, sulla conformità normativa, sulla marcatura CE o sulla responsabilità del produttore. Tali sistemi non possono mai operare in modo autonomo e sono ammessi esclusivamente come strumenti di supporto informativo, previa autorizzazione rafforzata e controllo costante.

---

5. PRINCIPI GENERALI DI UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

Il presente Capitolo definisce i principi generali e inderogabili che regolano l'utilizzo dell'Intelligenza Artificiale all'interno della Società. Tali principi costituiscono il fondamento etico, tecnico e giuridico della Policy IA e devono orientare ogni decisione, scelta operativa e comportamento degli utilizzatori.

5.1 Principio di centralità e prevalenza del controllo umano

La Società riconosce che l'Intelligenza Artificiale rappresenta uno strumento di supporto all'attività umana e non può in alcun caso sostituire il giudizio, la competenza, la responsabilità e la discrezionalità dell'essere umano.

Ogni utilizzo dell'IA deve essere concepito e gestito in modo tale da garantire la presenza di un controllo umano effettivo, consapevole e qualificato, in particolare nei processi che incidono sulla progettazione, sulla produzione, sulla sicurezza dei prodotti e sulla conformità normativa.

È fatto espresso divieto di delegare a sistemi di IA decisioni autonome o automatizzate aventi effetti giuridici, tecnici o organizzativi rilevanti.

5.2 Principio di responsabilità e attribuibilità delle decisioni

Ogni attività svolta mediante l'ausilio di sistemi di IA deve essere sempre riconducibile a una o più persone fisiche chiaramente individuate, che mantengono la piena responsabilità delle decisioni assunte e degli output generati.

L'utilizzo dell'IA non esonera in alcun modo l'utilizzatore, il responsabile di funzione o la Società dalle responsabilità civili, penali, amministrative o disciplinari derivanti da errori, omissioni o violazioni.

5.3 Principio di tracciabilità e verificabilità

L'utilizzo dei sistemi di IA deve essere organizzato in modo da consentire la tracciabilità delle attività svolte, degli input forniti, degli output generati e delle decisioni adottate sulla base di tali output.
La tracciabilità costituisce requisito essenziale per:

- la verifica interna;
- l'attività di audit;
- l'adempimento degli obblighi di controllo ex D.Lgs. 231/2001;
- la gestione di eventuali contenziosi o ispezioni.

5.4 Principio di proporzionalità e precauzione industriale

L'adozione e l'utilizzo dell'IA devono essere proporzionati alla complessità, alla criticità e al rischio del processo interessato.

Nei processi industriali caratterizzati da impatti potenzialmente rilevanti sulla sicurezza dei prodotti, dei lavoratori o dei clienti, la Società applica un principio di precauzione rafforzato, limitando l'uso dell'IA a funzioni di supporto informativo e analitico.

5.5 Principio di sicurezza del prodotto e del processo

La sicurezza dei prodotti meccanici ed elettromeccanici costituisce valore primario e non negoziabile per la Società.

L'utilizzo dell'IA non può in alcun caso compromettere, ridurre o aggirare i requisiti di sicurezza, affidabilità, qualità e conformità normativa dei prodotti e dei processi produttivi.

Ogni output generato da sistemi di IA che incida, anche indirettamente, su aspetti di sicurezza deve essere sottoposto a verifica tecnica qualificata.

5.6 Principio di conformità normativa e regolamentare

L'utilizzo dell'IA deve avvenire nel rispetto di tutte le normative applicabili, incluse quelle in materia di:

- sicurezza dei prodotti e responsabilità del produttore;
- salute e sicurezza sul lavoro;
- protezione dei dati personali;
- segreti industriali e concorrenza;
- responsabilità amministrativa degli enti ex D.Lgs. 231/2001.

Ogni utilizzo dell'IA che comporti dubbi interpretativi o profili di rischio normativo deve essere preventivamente valutato con le funzioni competenti.

5.7 Principio di tutela del patrimonio informativo e industriale

La Società riconosce e difende accuratamente il valore strategico del proprio patrimonio informativo, tecnico e industriale.

L'utilizzo dell'IA deve essere strutturato in modo da **prevenire la dispersione, la perdita o l'uso improprio di dati, informazioni e know-how aziendali, adottando misure organizzative e tecniche adeguate.**

---

6. IA E PROCESSI INDUSTRIALI AZIENDALI

Il presente Capitolo disciplina in modo puntuale l'utilizzo dell'Intelligenza Artificiale nei principali processi industriali e di supporto della Società, al fine di garantire che tale utilizzo avvenga in coerenza con i principi di sicurezza, controllo umano, responsabilità e conformità normativa.

6.1 IA e progettazione dei prodotti e dei componenti

L'IA può essere utilizzata come strumento di supporto alla fase di progettazione di prodotti o componenti esclusivamente per finalità di analisi preliminare, simulazione concettuale, verifica di coerenza progettuale e supporto all'individuazione di soluzioni alternative.

In tale ambito:

- l'IA **non può essere utilizzata per la progettazione autonoma di componenti o assiemi;**
- ogni output generato dall'IA deve essere verificato, validato e approvato da personale tecnico qualificato;
- resta fermo l'obbligo di rispetto delle normative tecniche applicabili, delle specifiche di prodotto e delle procedure di progettazione aziendali.

È espressamente **vietato utilizzare sistemi di IA per sostituire il processo di validazione tecnica, la revisione progettuale o le verifiche di sicurezza.**

6.2 IA e industrializzazione del prodotto

Nella fase di industrializzazione, l'IA può essere utilizzata per supportare:

- l'analisi dei processi produttivi;
- l'ottimizzazione dei flussi;
- la valutazione preliminare di alternative di processo.

L'IA non può in alcun caso sostituire le decisioni di industrializzazione che restano di esclusiva competenza delle funzioni apicali aziendali preposte.

6.3 IA e produzione

Nel processo produttivo, l'IA può essere impiegata per:

- analisi dei dati di produzione;
- individuazione di anomalie o inefficienze;
- supporto alla pianificazione della produzione.

È vietato affidare a sistemi di IA il controllo diretto e autonomo di macchinari, impianti o linee produttive senza adeguati presidi di sicurezza e supervisione umana.

6.4 IA e qualità, collaudo e certificazioni

L'IA può supportare le attività di qualità e collaudo attraverso l'analisi di dati storici, la rilevazione di trend e il supporto alla gestione documentale.

In nessun caso l'IA può:

- sostituire test fisici obbligatori;
- validare in modo automatico i risultati di collaudo;
- essere utilizzata come unico strumento per attestare la conformità del prodotto;
- incidere autonomamente sulla marcatura CE o sul fascicolo tecnico.

6.5 IA e manutenzione

L'IA può essere utilizzata per la manutenzione predittiva e preventiva, al fine di supportare l'individuazione di possibili guasti o criticità.

Le decisioni operative relative agli interventi di manutenzione **restano in ogni caso di competenza del personale tecnico qualificato.**

6.6 IA e gestione dei dati tecnici

L'utilizzo dell'IA per l'analisi e la gestione dei dati tecnici deve avvenire nel rispetto delle policy IT e delle misure di sicurezza adottate dalla Società.

È vietato utilizzare sistemi di IA che comportino la diffusione non controllata di dati tecnici, disegni o informazioni riservate.

6.7 IA, Sistemi informativi e Cybersecurity

Ogni sistema di IA deve essere valutato preventivamente sotto il profilo della sicurezza informatica. L'integrazione dell'IA nei sistemi informativi aziendali deve garantire:

- segregazione degli accessi;
- tracciabilità delle operazioni;
- protezione da accessi non autorizzati;
- possibilità di audit.

---

7. AMBITI CONSENTITI, LIMITATI E VIETATI DI UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

Il presente Capitolo individua in modo chiaro e tassativo gli ambiti di utilizzo dell'Intelligenza Artificiale consentiti, soggetti a limitazione e vietati all'interno della Società, al fine di prevenire utilizzi impropri, ridurre il rischio operativo e garantire il rispetto dei principi di sicurezza, controllo umano e responsabilità.

7.1 Ambiti di utilizzo consentiti

È consentito l'utilizzo di sistemi di IA, previa autorizzazione e nel rispetto della presente Policy IA, per le seguenti finalità:

- **Supporto documentale e informativo:** redazione di bozze di documenti interni, sintesi normative, supporto alla predisposizione di procedure e manuali, fermo restando che la versione finale deve essere sempre verificata e approvata da personale competente.

- **Analisi di dati storici:** analisi di dati di produzione, qualità, manutenzione e logistica al fine di individuare trend, correlazioni e possibili aree di miglioramento.

- **Supporto concettuale alla progettazione:** utilizzo dell'IA per attività di brainstorming tecnico, analisi preliminare di soluzioni progettuali, valutazioni concettuali non vincolanti.

- **Manutenzione predittiva:** supporto all'individuazione di potenziali guasti o criticità, senza sostituzione delle decisioni operative del personale tecnico.

- **Supporto alla pianificazione**: analisi di scenari produttivi, pianificazione delle risorse e supporto alle decisioni organizzative.

7.2 Ambiti di utilizzo soggetti a limitazione

Gli utilizzi di IA che incidono, anche indirettamente, su processi tecnici o industriali rilevanti sono soggetti a specifiche limitazioni e controlli rafforzati.

Rientrano in questa categoria:

- **Progettazione tecnica:** l'IA può essere utilizzata solo come supporto informativo; ogni output deve essere sottoposto a verifica e validazione tecnica qualificata.
- **Qualità e collaudo:** l'IA può supportare l'analisi dei dati di collaudo, ma non può validare risultati né attestare la conformità del prodotto.
- **Produzione**: l'IA può analizzare dati di processo, ma non può controllare autonomamente macchinari o linee produttive.
- **Gestione dei dati tecnici**: l'utilizzo dell'IA è consentito solo su sistemi autorizzati e con dati adeguatamente protetti.

Per tali ambiti è obbligatoria la supervisione costante da parte di personale qualificato.

7.3 Ambiti di utilizzo vietati

È fatto **espresso e inderogabile divieto di utilizzare sistemi di IA per**:

- progettare autonomamente componenti meccanici o elettromeccanici safety-critical;
- sostituire test fisici, prove obbligatorie o collaudi prescritti;
- validare automaticamente la conformità normativa dei prodotti;
- incidere in modo autonomo sulla marcatura CE o sul fascicolo tecnico;
- aggirare o eludere controlli di qualità, sicurezza o conformità;
- **effettuare l'upload, l'inserimento o la condivisione di qualsiasi documentazione aziendale**, ed in particolare disegni tecnici, modelli CAD, risultati di prove tecniche o di test, report di collaudo, verbali di verifica e documentazione CE;
- utilizzare l'IA per valutazioni disciplinari, di performance o di selezione del personale;
- utilizzare l'IA in modo contrario al Codice Etico o alla normativa vigente.

7.4 Conseguenze delle violazioni

Ogni utilizzo dell'IA in violazione del presente Capitolo costituisce grave violazione della Policy IA e comporta l'applicazione delle sanzioni disciplinari previste, fatta salva ogni ulteriore responsabilità civile, penale o amministrativa.

---

8. TUTELA DEI DATI, DEL KNOW-HOW E CYBERSECURITY

Il presente Capitolo disciplina le misure e le regole finalizzate alla tutela dei dati personali, dei dati industriali e del know-how aziendale nell'ambito dell'utilizzo dell'Intelligenza Artificiale, nonché i presìdi di sicurezza informatica necessari a prevenire rischi di perdita, diffusione indebita o compromissione delle informazioni.

8.1 Protezione dei dati personali

L'utilizzo di sistemi di IA che comporti il trattamento di dati personali deve avvenire nel pieno rispetto della normativa in materia di protezione dei dati personali, inclusi il Regolamento UE 679/2016 (GDPR) e le disposizioni interne aziendali.

In particolare:

- è vietato inserire nei sistemi di IA dati personali non necessari rispetto alle finalità perseguite;
- ove possibile, i dati devono essere preventivamente anonimizzati o pseudonimizzati;
- ogni utilizzo di IA che comporti trattamenti nuovi o ad alto rischio deve essere preventivamente valutato sotto il profilo privacy, anche mediante valutazione d'impatto (DPIA), ove applicabile;
- i ruoli e le responsabilità in materia di protezione dei dati devono essere chiaramente individuati.

8.2 Tutela del know-how e dei segreti industriali

La Società riconosce il valore strategico del proprio patrimonio tecnico, industriale e documentale e adotta un **principio di divieto assoluto di caricamento (upload) di documentazione aziendale su sistemi di Intelligenza Artificiale non espressamente autorizzati.**

È fatto **espresso, generale e inderogabile divieto** di effettuare l'upload, l'inserimento o la condivisione, anche parziale, su qualsiasi sistema di IA (inclusi sistemi cloud, piattaforme esterne, chatbot e strumenti di IA generativa) di:

- disegni tecnici, modelli CAD, schemi meccanici ed elettromeccanici;
- risultati di prove tecniche, test di laboratorio, collaudi, verifiche funzionali o di sicurezza;
- report di prova, verbali di collaudo, analisi di affidabilità;
- parametri di progetto, specifiche tecniche, distinte base;
- documentazione del fascicolo tecnico e documentazione relativa alla marcatura CE;
- procedure produttive, processi industriali e know-how aziendale;
- qualsiasi altra documentazione aziendale riservata o non pubblica.

Il divieto si applica **indipendentemente**:

- dal formato del documento (testo, immagine, file CAD, screenshot, foto);
- dal dispositivo utilizzato (aziendale o personale);
- dalla finalità dichiarata dell'utilizzo.

È altresì vietato utilizzare sistemi di IA che prevedano l'utilizzo dei dati caricati per finalità di addestramento, apprendimento o miglioramento del modello, anche in forma aggregata.

Ogni violazione del presente divieto è considerata **grave violazione della Policy IA**, del Codice Etico e degli obblighi di riservatezza ed espone il responsabile a sanzioni disciplinari e a ulteriori responsabilità previste dalla legge.

8.3 Sicurezza informatica e protezione dei sistemi

L'adozione e l'utilizzo di sistemi di IA devono avvenire nel rispetto delle policy di sicurezza informatica della Società e delle best practice in materia di cybersecurity.

In particolare:

- i sistemi di IA devono garantire adeguati livelli di sicurezza, autenticazione e controllo degli accessi;
- devono essere previste misure di protezione contro accessi non autorizzati, perdita di dati e attacchi informatici;
- l'integrazione dell'IA nei sistemi informativi aziendali deve essere preventivamente valutata dalla funzione IT;
- devono essere garantite la tracciabilità delle operazioni e la possibilità di audit.

8.4 Gestione degli incidenti e segnalazioni

Eventuali incidenti di sicurezza, violazioni dei dati o utilizzi impropri dell'IA devono essere segnalati tempestivamente secondo le procedure aziendali, al fine di consentire l'adozione di misure correttive e preventive.

La mancata segnalazione di incidenti o violazioni costituisce violazione della presente Policy IA.

---

9. GOVERNANCE INTERNA DELL'INTELLIGENZA ARTIFICIALE

Il presente Capitolo definisce il sistema di governance interna dell'Intelligenza Artificiale adottato dalla Società, individuando ruoli, responsabilità, processi decisionali e meccanismi di controllo volti a garantire un utilizzo dell'IA conforme, sicuro, tracciabile e coerente con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001.

9.1 Principi di governance

La governance dell'Intelligenza Artificiale si fonda sui seguenti principi:

- chiara attribuzione di ruoli e responsabilità;
- separazione delle funzioni decisionali e di controllo;
- supervisione continua e controllo umano;
- integrazione con il sistema di controllo interno e con il Modello 231;
- documentazione e tracciabilità delle decisioni.

9.2 Organi e funzioni coinvolte

Nell'ambito della governance dell'IA sono coinvolti, ciascuno per le rispettive competenze, i seguenti soggetti:

- **Consiglio di Amministrazione:** approva la presente Policy IA e ne assicura l'adeguatezza rispetto alla strategia aziendale e al profilo di rischio.

- **Alta Direzione:** garantisce l'attuazione operativa della Policy IA e l'integrazione dell'IA nei processi aziendali in modo conforme.

- **Responsabile Compliance / Modello 231:** presidia i profili di rischio normativo e di responsabilità amministrativa dell'ente connessi all'uso dell'IA.

- **Organismo di Vigilanza (OdV):** vigila sull'efficace attuazione della Policy IA e riceve i flussi informativi previsti.

- **Funzione IT e Cybersecurity:** valuta i sistemi di IA sotto il profilo tecnico e di sicurezza informatica.

- **Responsabili di funzione (Tecnico, Produzione, Qualità, ecc.)**: garantiscono l'utilizzo dell'IA nei rispettivi ambiti nel rispetto della presente Policy IA.

9.3 Processo di autorizzazione all'utilizzo dell'IA

L'utilizzo di sistemi di Intelligenza Artificiale è consentito esclusivamente previa autorizzazione formale, secondo la procedura aziendale.

Il processo di autorizzazione prevede, di norma:

- richiesta motivata da parte della funzione interessata;
- valutazione tecnica e di sicurezza informatica;
- valutazione dei profili di rischio normativo e 231;
- eventuale coinvolgimento dell'OdV;
- registrazione del sistema IA autorizzato.

9.4 Registro dei sistemi di IA

La Società istituisce e mantiene un registro aggiornato dei sistemi di Intelligenza Artificiale autorizzati, contenente almeno:

- descrizione del sistema;
- finalità di utilizzo;
- livello di rischio;
- funzioni coinvolte;
- data di autorizzazione e riesame.

9.5 Monitoraggio e audit

L'utilizzo dei sistemi di IA è soggetto a monitoraggio periodico e, ove necessario, ad audit interni.
Il monitoraggio è finalizzato a:

- verificare la conformità alla presente Policy;
- individuare utilizzi impropri o non autorizzati;
- valutare l'adeguatezza dei presidi di controllo.

9.6 Gestione delle non-conformità

Eventuali non conformità, violazioni o utilizzi impropri dell'IA devono essere gestiti tempestivamente mediante l'adozione di misure correttive e preventive, in coordinamento con le funzioni competenti e, ove applicabile, con l'Organismo di Vigilanza.

---

10. FORMAZIONE, RESPONSABILITÀ E SISTEMA DISCIPLINARE

Il presente Capitolo disciplina gli obblighi di formazione, le responsabilità individuali e il sistema disciplinare connessi all'utilizzo dell'Intelligenza Artificiale, al fine di garantire l'effettiva applicazione della presente Policy e la sua integrazione nel sistema di controllo interno e nel Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001.

10.1 Formazione e sensibilizzazione

La Società riconosce che la corretta comprensione dei rischi e delle opportunità connesse all'Intelligenza Artificiale costituisce presupposto essenziale per un utilizzo consapevole e conforme degli strumenti IA.

A tal fine, la Società assicura:

- programmi di formazione periodica obbligatoria per i dipendenti e i dirigenti coinvolti nell'utilizzo dell'IA;
- specifici moduli formativi per le funzioni tecniche, produttive, di qualità, IT e compliance;
- attività di sensibilizzazione sui rischi legali, organizzativi e di sicurezza connessi all'uso improprio dell'IA;
- aggiornamenti formativi in occasione di modifiche normative, tecnologiche o organizzative rilevanti.

La partecipazione alle attività formative costituisce obbligo lavorativo e deve essere adeguatamente tracciata.

10.2 Responsabilità individuali

Ogni soggetto destinatario della presente Policy IA è tenuto a:

- conoscere e rispettare le disposizioni della Policy IA;
- utilizzare esclusivamente sistemi di IA autorizzati;
- attenersi alle procedure aziendali e alle indicazioni delle funzioni competenti;
- collaborare alle attività di controllo e audit;
- segnalare tempestivamente eventuali anomalie, violazioni o utilizzi impropri dell'IA.

La violazione degli obblighi sopra indicati comporta responsabilità individuale e non può essere giustificata dall'utilizzo di strumenti di IA o dall'affidamento su output generati automaticamente.

10.3 Sistema disciplinare

Il mancato rispetto della presente Policy costituisce violazione degli obblighi contrattuali e può dar luogo all'applicazione delle sanzioni disciplinari previste dal sistema disciplinare aziendale e dal Modello 231, in misura proporzionata alla gravità della violazione.

A titolo esemplificativo, possono costituire violazioni disciplinari:

- l'utilizzo di sistemi di IA non autorizzati;
- la violazione dei divieti previsti dalla Policy IA;
- la mancata segnalazione di incidenti o utilizzi impropri;
- l'inserimento nei sistemi di IA di dati riservati o protetti;
- l'elusione dei controlli previsti.

Restano ferme le ulteriori responsabilità civili, penali e amministrative nei casi previsti dalla legge.

---

11. INTEGRAZIONE NEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/2001

Il presente Capitolo disciplina l'integrazione della Policy Aziendale per l'Utilizzo dell'Intelligenza Artificiale nel Modello di Organizzazione, Gestione e Controllo adottato dalla Società ai sensi del D.Lgs. 231/2001, quale Parte Speciale finalizzata alla prevenzione dei rischi di responsabilità amministrativa dell'ente connessi all'utilizzo dell'IA.

11.1 Valenza della Policy IA nel sistema 231

La presente Policy IA costituisce parte integrante del Modello 231 e concorre, unitamente al Codice Etico, al sistema disciplinare e alle procedure aziendali, a prevenire la commissione dei reati presupposto potenzialmente connessi all'utilizzo dell'Intelligenza Artificiale.

L'adozione e l'effettiva attuazione della Policy IA rappresentano presidi organizzativi idonei a dimostrare la volontà dell'ente di governare consapevolmente i rischi emergenti derivanti dall'innovazione tecnologica.

11.2 Mappatura dei processi sensibili

In relazione all'utilizzo dell'IA, sono individuati come processi sensibili ai fini del D.Lgs. 231/2001, in particolare:

- progettazione e sviluppo di componenti meccanici ed elettromeccanici;
- industrializzazione e produzione;
- qualità, collaudo, certificazione e marcatura CE;
- gestione dei dati tecnici e industriali;
- sistemi informativi e cybersecurity;
- gestione dei fornitori tecnologici.

Tali processi sono soggetti a specifici presidi di controllo e monitoraggio.

11.3 Reati presupposto rilevanti

L'uso improprio o non conforme dell'Intelligenza Artificiale può esporre la Società al rischio di commissione, tra gli altri, dei seguenti reati presupposto:

- reati colposi in materia di salute e sicurezza sul lavoro (art. 25-septies);
- reati colposi connessi alla sicurezza dei prodotti e alla responsabilità del produttore;
- reati informatici e trattamento illecito di dati (art. 24-bis);
- delitti contro l'industria e il commercio;
- violazione di segreti industriali.

11.4 Presidi di controllo specifici

Al fine di prevenire i rischi di cui al presente Capitolo, la Società adotta i seguenti presidi:

- chiara regolamentazione dell'utilizzo dell'IA mediante la presente Policy IA;
- processo formale di autorizzazione e registrazione dei sistemi di IA;
- segregazione dei ruoli tra chi utilizza, chi autorizza e chi controlla;
- obbligo di validazione tecnica umana degli output IA;
- monitoraggio periodico e audit;
- formazione obbligatoria del personale;
- sistema disciplinare efficace.

11.5 Flussi informativi verso l'Organismo di Vigilanza

Devono essere tempestivamente comunicati all'Organismo di Vigilanza:

- utilizzi dell'IA non autorizzati o non conformi;
- incidenti o anomalie rilevanti;
- violazioni della Policy IA;
- esiti degli audit interni sull'utilizzo dell'IA.

L'OdV valuta le segnalazioni ricevute e propone, ove necessario, l'adozione di misure correttive.

11.6 Coordinamento con gli altri strumenti di controllo

La presente Policy si coordina con:

- il Codice Etico;
- il DVR;
- il sistema di gestione della qualità;
- le procedure IT e cybersecurity;
- il sistema disciplinare.

Tale coordinamento garantisce un approccio integrato alla gestione dei rischi IA.

---

12. ALLEGATI OPERATIVI

Allegato 1 – Comunicazione ai Dipendenti
Allegato 2 – Impegno e presa visione dipendenti