PMI Digital Lab

GUIDA OPERATIVA 2026

AI Policy Aziendale

Guida operativa per definire regole chiare sull'utilizzo dell'Intelligenza Artificiale nelle PMI

Una guida modulare, un modello completo di Policy e sette strumenti pronti per l'adozione.

PARTE DEL SISTEMA PMI DIGITAL LAB

Collegata al Registro AI, ai registri operativi e alla Guida AI Act per PMI.

Identificazione della AI Policy

Dati essenziali per riconoscere, approvare e distribuire la versione in uso.

NOME AZIENDA

CODICE DOCUMENTO

POL-AI-001

VERSIONE

1.0

RESPONSABILE

APPROVATO DA

DATA DI EMISSIONE

ENTRATA IN VIGORE

CLASSIFICAZIONE

Uso interno / Riservato

NUMERO PAGINE

50

COLLOCAZIONE E DESTINATARI AUTORIZZATI

CONTROLLO DOCUMENTALE

Aggiornare versione, data e approvazione quando cambia la Policy. Registrare distribuzione e revisioni nelle appendici A6 e A7.

DATA COMPILAZIONE

RESPONSABILE

PROSSIMO RIESAME

Guida operativa

Diciannove capitoli per progettare, adottare e mantenere la Policy.

Dalla governance all’adozione

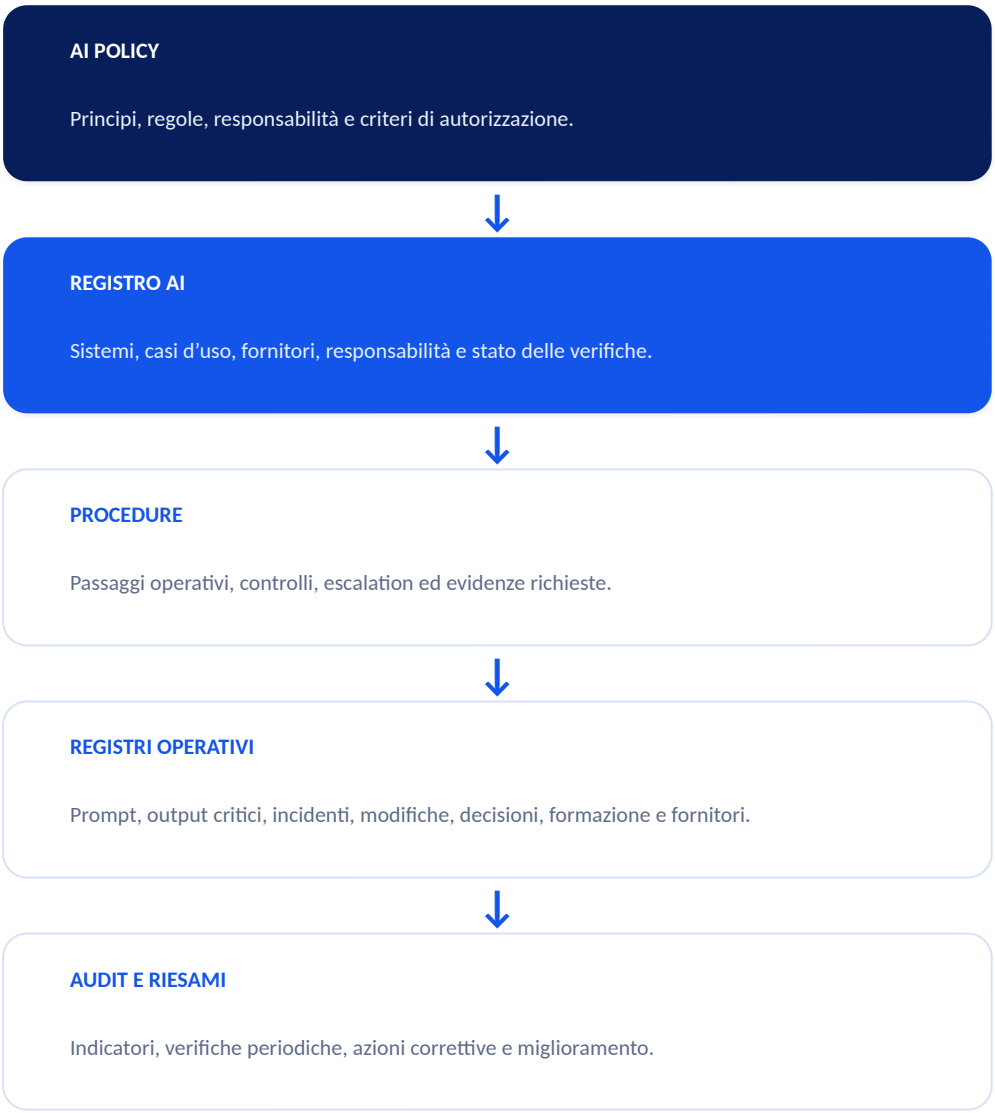
La guida precede il modello completo e i moduli pronti all’uso.

POLICY MODULARE

Obbligatorio: base comune. Consigliato: utile in molti contesti. Da valutare: applicare solo quando pertinente a processi, dati e rischi dell’impresa.

Dalle regole alle evidenze

Cinque livelli collegano governo, attività operative e controllo.



DA RICORDARE

La Policy stabilisce la regola; Registro, procedure e registri operativi dimostrano come viene applicata.

Perché ogni PMI dovrebbe avere una AI Policy

L'AI entra nei processi prima che l'organizzazione abbia definito regole condivise.

01

Diffusione reale

Chat, suite d'ufficio, CRM, selezione, marketing e automazioni integrano già funzioni AI.

02

Vantaggi

Velocità, coerenza, analisi e supporto operativo, se l'uso è progettato e controllato.

03

Rischi

Dati esposti, output errati, decisioni opache, dipendenza dai fornitori e Shadow AI.

04

Governance

La Policy chiarisce ciò che è consentito, chi decide e dove vengono registrate le evidenze.

ESEMPIO PMI

Un commerciale usa un assistente AI per offerte: la Policy stabilisce dati vietati, verifica obbligatoria e prompt approvati.

Una Policy stabilisce regole, non descrive ogni singolo passaggio

Documenti diversi hanno funzioni diverse e devono lavorare insieme.

01

AI Policy

Principi, divieti, responsabilità, controlli e criteri di autorizzazione.

02

Regolamento interno

Regole generali di comportamento e organizzazione del lavoro.

03

Procedura

Sequenza operativa, responsabilità, input, output ed evidenze.

04

Istruzione / Codice etico

Dettaglio tecnico oppure principi di condotta e valori aziendali.

ERRORE DA EVITARE

Inserire nella Policy istruzioni destinate a cambiare ogni mese. I dettagli variabili vanno in procedure e registri.

La Policy serve quando l’AI entra nel lavoro quotidiano

Non è necessario attendere un sistema complesso o ad alto rischio.

01

Account aziendali

L’impresa acquista o autorizza strumenti con funzioni AI.

02

Uso diffuso

Più reparti utilizzano chatbot, copiloti o funzioni integrate.

03

Dati e persone

Gli output riguardano clienti, dipendenti, candidati o informazioni riservate.

04

Automazioni

L’AI alimenta email, CRM, decisioni, classificazioni o flussi automatici.

DA RICORDARE

Anche una microimpresa può adottare una Policy breve: poche regole chiare sono migliori di nessuna regola.

Cinque obiettivi operativi e un risultato comune

La Policy deve permettere alle persone di lavorare con l'AI senza improvvisare.

01

Uso responsabile

Finalità lecite, comprensibili e coerenti con il ruolo.

02

Tutela dei dati

Classificazione semplice e divieti chiari.

03

Qualità

Verifica proporzionata all'importanza dell'output.

04

Supervisione

Una persona mantiene autorità e possibilità di correzione.

05

Conformità

AI Act, GDPR, sicurezza e regole interne coordinate.

06

Tracciabilità

Decisioni e verifiche collegate al Registro AI.

BUONA PRATICA

Definire pochi obiettivi misurabili: strumenti censiti, persone formate, riesami eseguiti e incidenti chiusi.

Chi deve rispettare la Policy

L’ambito segue l’accesso ai sistemi e ai dati, non il tipo di contratto della persona.

01

Dipendenti

Tutte le persone che usano strumenti e account aziendali.

02

Collaboratori

Professionisti e collaboratori che operano sui processi.

03

Consulenti

Soggetti esterni con accesso a dati o sistemi.

04

Fornitori

Quando gestiscono attività AI per conto dell’impresa.

05

Stagisti

Con autorizzazioni e supervisione adeguate.

06

Amministratori

Anche la direzione è soggetta a regole, approvazioni e tracciabilità.

ESEMPIO PMI

L’agenzia marketing esterna deve rispettare le stesse regole sui dati applicate al team interno.

Un glossario riduce interpretazioni incoerenti

Usare gli stessi termini nella Policy, nel Registro AI e nelle procedure.

01

Sistema AI

Sistema che genera contenuti, previsioni, raccomandazioni o decisioni.

02

Caso d’uso

Attività concreta nella quale il sistema viene impiegato.

03

Prompt

Istruzione o contesto fornito al sistema.

04

Output

Risultato prodotto dal sistema AI.

05

Supervisione umana

Controllo esercitato da una persona competente e autorizzata.

06

Shadow AI

Uso di strumenti o funzioni AI non conosciuti o autorizzati.

DA RICORDARE

Il glossario completo del Registro AI resta il riferimento terminologico della collana.

Ruoli applicabili anche senza funzioni dedicate

Nelle microimprese più ruoli possono coincidere, purché le responsabilità siano esplicite.

01

Direzione

Approva Policy, strumenti rilevanti, eccezioni e sospensioni.

02

Responsabile del processo

Definisce finalità, controlli, utenti e risultati attesi.

03

Utilizzatore

Rispetta regole, verifica output e segnala problemi.

04

Amministratore piattaforma

Gestisce configurazioni, account, accessi e log.

05

Referenti privacy e sicurezza

Supportano le valutazioni quando presenti o necessari.

06

HR / Qualità / Compliance

Formazione, distribuzione, audit e miglioramento.

BUONA PRATICA

Indicare un solo responsabile del risultato per ogni caso d'uso.

Matrice delle responsabilità

Compilare in base alla struttura reale. Una persona può ricoprire più ruoli.

ATTIVITÀ	ESEGUE	RISPONDE	VERIFICA	APPROVA
Nuovo strumento				
Nuovo caso d'uso				
Verifica output critico				
Gestione incidente				
Formazione				
Riesame Policy				
Autorizzazione eccezione				

DA RICORDARE

Non tutte le attività richiedono quattro persone diverse. Il controllo deve essere proporzionato alla criticità.

Sei principi per guidare le decisioni non previste

La Policy deve aiutare anche quando emerge un uso nuovo.

01

Trasparenza

Dichiarare l'uso dell'AI quando necessario e non attribuirle capacità che non possiede.

02

Supervisione

Mantenere controllo umano su output e decisioni rilevanti.

03

Responsabilità

La responsabilità resta alle persone e all'organizzazione.

04

Sicurezza

Proteggere accessi, dati, configurazioni e integrazioni.

05

Proporzionalità

Aumentare i controlli quando crescono impatto e rischio.

06

Qualità

Verificare accuratezza, completezza, fonte e adeguatezza.

RIFERIMENTO

L'AI Act adotta un approccio basato sul rischio: finalità e contesto determinano le regole applicabili.

Usi ordinari consentiti con controlli proporzionati

Gli esempi devono essere adattati ai dati e al processo aziendale.

01

Marketing

Bozze, varianti, calendari e sintesi, con revisione prima della pubblicazione.

02

Commerciale

Email e offerte, senza delegare prezzi, clausole o approvazioni.

03

Amministrazione

Classificazione e sintesi, senza automatizzare pagamenti o registrazioni non verificate.

04

Customer care

Bozze e ricerca, con escalation per reclami o casi delicati.

05

Produzione

Analisi e supporto documentale, senza sostituire controlli di sicurezza.

06

HR

Supporto redazionale e organizzativo; usi su candidati e lavoratori richiedono valutazione specifica.

BUONA PRATICA

Autorizzare casi d'uso specifici, non un prodotto in modo generico.

Matrice di autorizzazione

Usa tre livelli per evitare sia permissività generica sia divieti inutili.

ATTIVITÀ	LIVELLO	CONTROLLO	DOVE SI DOCUMENTA
Bozze interne	Obbligatorio	Revisione dell'utilizzatore	Registro AI
Contenuti pubblici	Obbligatorio	Approvazione prima della pubblicazione	Output critici
Analisi documenti	Consigliato	Controllo di fonti e dati	Scheda sistema
Automazione di flussi	Consigliato	Test, log ed eccezioni	Modifiche / Incidenti
Valutazioni su persone	Da valutare	Analisi specialistica e supervisione	Decisioni / Riesami
Nuovo fornitore	Obbligatorio	Valutazione prima dell'uso	Valutazione fornitori

ESEMPIO PMI

La bozza di una newsletter è consentita; la pubblicazione automatica senza revisione non lo è.

Divieti comprensibili e collegati al motivo

Un divieto funziona solo se la persona capisce il rischio e conosce l'alternativa.

01

Credenziali

Mai inserire password, token, chiavi API o codici di accesso.

02

Segreti e dati riservati

Evitare servizi non autorizzati: perdita di controllo e divulgazione.

03

Decisioni autonome

Non delegare assunzioni, licenziamenti, credito, pagamenti o sanzioni.

04

Identità ingannevole

Non creare contenuti che simulano persone senza autorizzazione e trasparenza.

05

Elusione dei controlli

Non disattivare log, filtri o supervisione per accelerare il lavoro.

06

Strumenti non autorizzati

Non usare account personali o servizi non valutati per attività aziendali.

ATTENZIONE

Le pratiche vietate dall'AI Act devono essere escluse indipendentemente dall'approvazione interna.

Divieto, motivo e alternativa

Ogni regola deve suggerire un comportamento praticabile.

VIETATO	PERCHÉ	ALTERNATIVA
Caricare CV in un chatbot pubblico	Dati personali e valutazioni sulle persone	Usare processo e strumento autorizzati
Inviare automaticamente un contratto	Errore con conseguenze economiche e legali	Revisione e approvazione obbligatorie
Usare password condivise	Assenza di responsabilità e tracciabilità	Account nominativi e MFA
Pubblicare immagini sintetiche ingannevoli	Rischio reputazionale e trasparenza	Etichettare e approvare il contenuto
Ignorare un output palesemente errato	Perdita di qualità e ripetizione dell'errore	Correggere e segnalare
Creare un nuovo uso senza registrarlo	Manca valutazione di dati, rischio e responsabilità	Richiesta → valutazione → Registro AI

ERRORE DA EVITARE

Scrivere "è vietato usare l'AI" senza distinguere attività, dati e strumenti.

Classificazione semplice dei dati

La regola dipende sia dal dato sia dal servizio utilizzato.

CATEGORIA	INSERIMENTO NELL'AI	REGOLA
Informazioni pubbliche	Consentito	Verificare accuratezza e diritti di utilizzo.
Documenti interni non riservati	Con attenzione	Usare solo strumenti autorizzati.
Dati personali	Valutare caso per caso	Finalità, base giuridica, minimizzazione e fornitore.
Categorie particolari di dati	Evitare salvo valutazione specifica	Richiede elevata cautela e autorizzazione.
Credenziali e chiavi	Vietato	Mai inserire in prompt o allegati.
Segreti industriali	Vietato salvo autorizzazione	Protezione contrattuale e tecnica specifica.

DA RICORDARE

"Dato personale" non significa automaticamente "sempre vietato": significa che serve una valutazione concreta e documentata.

Checklist prima di inserire un dato o documento

Se una risposta non è chiara, fermarsi e chiedere al responsabile.

01

Finalità

Il dato è davvero necessario per il risultato?

02

Classificazione

È pubblico, interno, personale, particolare, riservato o segreto?

03

Strumento

Il servizio e il piano sono autorizzati?

04

Impostazioni

Il dato può essere usato dal fornitore per migliorare il servizio?

05

Destinatari

Chi vedrà l'input e l'output?

06

Conservazione

Per quanto tempo resteranno prompt, file e log?

ESEMPIO PMI

Per sintetizzare un reclamo, rimuovere dati non necessari e utilizzare solo il servizio aziendale approvato.

Regole per i prompt aziendali

I prompt riutilizzabili sono patrimonio operativo e devono essere controllati.

01

Condivisi

Modelli utili messi a disposizione dei team.

02

Approvati

Prompt verificati per processi ripetibili o delicati.

03

Vietati

Prompt che richiedono credenziali, dati non autorizzati o elusione dei controlli.

04

Modifiche

Solo persone designate aggiornano prompt controllati.

05

Conservazione

Repository aziendale con versione e responsabile.

06

Collegamento

Prompt rilevanti registrati nel Registro Prompt.

BUONA PRATICA

Separare istruzioni, dati variabili e criteri di verifica.

Ciclo di vita del prompt approvato

Un prompt controllato viene trattato come una piccola istruzione operativa.

FASE	ATTIVITÀ	RESPONSABILE	EVIDENZA	ESITO
1	Proposta e finalità		Richiesta	
2	Test con casi normali ed errori		Risultati test	
3	Verifica dati e limitazioni		Checklist	
4	Approvazione e versione		Registro Prompt	
5	Distribuzione agli utenti		Repository	
6	Monitoraggio e revisione		Riesame	

ERRORE DA EVITARE

Copiare prompt da Internet e usarli in processi aziendali senza verificarne dati, istruzioni e risultati.

La supervisione deve essere reale, non simbolica

Chi controlla deve avere competenza, tempo e autorità per correggere o fermare.

01

Quando sempre

Persone, denaro, obblighi, sicurezza, contenuti esterni e decisioni rilevanti.

02

Chi controlla

Responsabile del processo o persona formalmente incaricata.

03

Che cosa verifica

Dati, logica, fonti, completezza, tono, conseguenze ed eccezioni.

04

Come documenta

Esito nel Registro Output critici o nella prova prevista dal processo.

DA RICORDARE

Una firma automatica o un clic senza tempo per il controllo non costituiscono supervisione efficace.

Matrice di controllo degli output

Impostare il livello minimo e aumentarlo quando crescono rischio o incertezza.

TIPO DI OUTPUT	CONTROLLO MINIMO	ISTRUZIONE
Email interna ordinaria	A campione	Verificare almeno quando contiene dati o impegni.
Offerta commerciale	Sempre	Prezzi, condizioni, cliente e allegati.
Contratto o clausola	Sempre	Revisione competente prima dell'uso.
Contenuto marketing	Prima della pubblicazione	Fonti, claim, diritti, tono ed etichettatura.
Valutazione candidato	Sempre + valutazione specifica	Non assumere decisioni autonome.
Report direzionale	Sempre	Dati, periodo, calcoli, ipotesi e fonti.

ESEMPIO PMI

Una bozza interna può essere controllata dall'autore; un'offerta deve essere verificata dal responsabile commerciale.

Verificare, correggere e imparare dagli errori

La verifica non serve solo ad approvare: deve migliorare prompt, dati e processo.

01 Accuratezza

Fatti, numeri, nomi, date e riferimenti.

02 Completezza

Informazioni mancanti e presupposti non dichiarati.

03 Fonti

Origine, attualità e affidabilità.

04 Adeguatezza

Tono, destinatario, finalità e contesto.

05 Correzione

Modificare l'output e, se necessario, prompt o dati.

06 Registrazione

Output critici, incidenti e decisioni nei relativi registri.

BUONA PRATICA

Definire prima dell'uso i criteri di accettazione dell'output.

Valutare il servizio reale, non solo il marchio

Piano gratuito, enterprise e integrazione API possono avere condizioni diverse.

01

Privacy

Ruoli, uso dei dati, conservazione, cancellazione e trasferimenti.

02

Sicurezza

Accessi, MFA, cifratura, log, incidenti e continuità.

03

AI Act

Ruolo del fornitore, istruzioni e documentazione disponibile.

04

Contratto e uscita

Subfornitori, assistenza, portabilità, rinnovi e dismissione.

COLLEGAMENTO

Registrare il risultato nella Valutazione fornitori del Registro AI.

Checklist di approvazione

Ogni punto aperto deve avere responsabile e scadenza.

CONTROLLO	STATO	EVIDENZA	RESPONSABILE / DATA
Identità, sede e piano del fornitore	☐ ☐ ☐		
Uso dei dati per training o miglioramento	☐ ☐ ☐		
Subfornitori e trasferimenti	☐ ☐ ☐		
Accessi, sicurezza e incidenti	☐ ☐ ☐		
Documentazione AI Act disponibile	☐ ☐ ☐		
Portabilità, cancellazione e uscita	☐ ☐ ☐		
Esito complessivo	Idoneo / Condizionato / No		

STATI

☐ **Da verificare** ☐ **Verificato** ☐ **Non applicabile**

Perché nasce lo Shadow AI

Spesso nasce per risolvere un problema, non per violare consapevolmente le regole.

01

Urgenza

Lo strumento ufficiale sembra lento o non disponibile.

02

Mancanza di alternative

Le persone non conoscono servizi autorizzati.

03

Regole poco chiare

La Policy vieta senza spiegare come chiedere approvazione.

04

Account personali

Accesso immediato, ma senza controllo aziendale.

DA RICORDARE

La prevenzione richiede alternative, comunicazione e un processo rapido di regolarizzazione.

Individuare, regolarizzare o interrompere

Non trasformare ogni segnalazione in una sanzione automatica.

01 — Segnalare

La persona comunica strumento, account, finalità, dati e urgenza.

02 — Contenere

Interrompere l'inserimento di dati delicati e proteggere gli accessi.

03 — Valutare

Verificare caso d'uso, fornitore, dati e alternative.

04 — Decidere

Autorizzare, limitare, sostituire oppure vietare.

05 — Registrare

Inserire sistema, decisione, azioni ed eventuale incidente nel Registro AI.

06 — Comunicare

Spiegare esito, motivazione e soluzione autorizzata.

ESEMPIO PMI

Un account personale usato per bozze può essere regolarizzato con un piano aziendale e regole sui dati.

Procedura per gli incidenti AI

Un incidente può essere un output dannoso, una divulgazione, un uso non autorizzato o un malfunzionamento.

01 — Errore rilevato

Conservare evidenze senza diffondere ulteriormente il problema.

02 — Segnalazione

Informare il canale indicato e il responsabile del processo.

03 — Contenimento

Fermare invii, accessi, integrazioni o pubblicazioni interessate.

04 — Valutazione

Gravità, impatto operativo, privacy, economico, reputazionale e normativo.

05 — Correzione

Ripristino, nuova verifica, comunicazioni e azioni correttive.

06 — Registrazione

Registro Incidenti e, se necessario, Registro Decisioni.

07 — Lezione appresa

Aggiornare Policy, prompt, formazione, controlli o fornitore.

ATTENZIONE

Se possono essere coinvolti dati personali o sicurezza, attivare subito le procedure competenti.

Responsabilità ed escalation

Definire contatti e soglie prima che si verifichi un problema.

EVENTO	PRIMA AZIONE	INFORMARE	REGISTRARE
Output errato non utilizzato	Correggere e testare	Responsabile processo	Se ricorrente
Contenuto esterno errato	Sospendere e correggere	Direzione / comunicazione	Sempre
Dati inseriti impropriamente	Interrompere e conservare evidenze	Privacy / sicurezza	Sempre
Automazione fuori controllo	Disattivare o rollback	IT / responsabile	Sempre
Impatto su lavoratore o cliente	Fermare la decisione	Direzione / funzioni competenti	Sempre
Uso Shadow AI	Contenere e valutare	Responsabile del Registro	Decisione / incidente

DA PREPARARE

Canale di segnalazione: _____ Referente: _____ Contatto urgente: _____

Formazione proporzionata al ruolo e all’utilizzo

Non tutte le persone devono conoscere gli stessi dettagli.

01

Iniziale

Regole di base, dati, strumenti autorizzati e segnalazioni.

02

Per nuovi sistemi

Funzioni, limiti, prompt, supervisione e casi vietati.

03

Dopo incidenti

Cause, nuove misure e comportamenti attesi.

04

Per ruolo

Direzione, responsabili, utilizzatori, IT, HR e funzioni di controllo.

COLLEGAMENTO

Registrare persone, contenuti, evidenze e aggiornamenti nel Registro Formazione.

Piano formativo annuale

Poche sessioni mirate sono più efficaci di un corso generico una volta l'anno.

DESTINATARI	CONTENUTI	MODALITÀ	FREQUENZA	EVIDENZA
Tutti gli utilizzatori	Policy, dati, output, incidenti	Briefing + guida	Iniziale / annuale	Presa visione
Responsabili processo	Valutazione e supervisione	Workshop	Nuovo uso / riesame	Verbale
Amministratori piattaforma	Accessi, log, modifiche, rollback	Sessione tecnica	Nuovo sistema	Registro
HR / privacy / sicurezza	Persone, dati, escalation	Caso pratico	Quando necessario	Attestazione
Direzione	Dashboard, rischi e decisioni	Riesame	Semestrale	Verbale

BUONA PRATICA

Usare esempi tratti dai processi reali dell'impresa.

Dashboard operativa

Un esempio manageriale da alimentare con i dati del Registro AI.

SISTEMI AI CENSITI	PROMPT APPROVATI	INCIDENTI APERTI
12	18	2

INCIDENTI CHIUSI	PERSONE FORMATE	RIESAMI COMPLETATI
7	34 / 40	9 / 12

CONTROLLO	ESITO	RESPONSABILE	PROSSIMA AZIONE
Coerenza Policy e Registro			
Azioni da incidenti			
Formazione per ruolo			
Fornitori e modifiche			

DA RICORDARE

La dashboard non sostituisce le evidenze: ogni indicatore deve essere riconducibile al Registro AI o a un registro operativo.

Quando riesaminare la Policy

La frequenza programmata è il minimo, non l'unico momento di revisione.

01

Nuovi sistemi AI

Nuove finalità, utenti o integrazioni.

02

Incidenti rilevanti

Errori, divulgazioni o impatti sulle persone.

03

Modifiche organizzative

Ruoli, processi, sedi o responsabilità.

04

Aggiornamenti normativi

AI Act, GDPR, indicazioni delle autorità.

05

Cambiamenti dei fornitori

Modelli, termini, dati, subfornitori o sicurezza.

06

Audit e reclami

Non conformità, segnalazioni e azioni correttive.

FREQUENZA

Riesame programmato: almeno annuale, salvo frequenza diversa definita dall'impresa. Riesame straordinario dopo gli eventi indicati.

AI Policy aziendale

Testo pronto da personalizzare, approvare e distribuire. Eliminare le opzioni non pertinenti.

COME PERSONALIZZARE

1. Compilare i campi tra parentesi quadre.
2. Selezionare i moduli Obbligatorio, Consigliato e Da valutare.
3. Collegare il Registro AI aziendale.
4. Approvare, distribuire e raccogliere la presa visione.
5. Registrare versione, formazione e riesami.

LIVELLI

OBBLIGATORIO — base comune. CONSIGLIATO — utile in molti contesti. DA VALUTARE — attivare solo se pertinente.

AZIENDA

CODICE / VERSIONE

APPROVATA DA

ENTRATA IN VIGORE

1. Scopo e campo di applicazione

Sezioni obbligatorie.

1 — SCOPO [OBBLIGATORIO]

La presente AI Policy definisce le regole per l'adozione e l'utilizzo responsabile dei sistemi di Intelligenza Artificiale presso [Nome azienda]. La Policy mira a tutelare persone, dati, qualità, sicurezza e continuità operativa, mantenendo una supervisione umana proporzionata al rischio.

2 — CAMPO DI APPLICAZIONE [OBBLIGATORIO]

La Policy si applica ad amministratori, dipendenti, collaboratori, stagisti, consulenti e fornitori che utilizzano sistemi AI per conto dell'azienda o accedono a dati, account e processi aziendali. Si applica a strumenti autonomi, funzioni integrate, API e automazioni con componenti AI.

2.1 — ECCEZIONI [DA VALUTARE]

Eventuali esclusioni devono essere motivate, approvate dalla Direzione, registrate e riesaminate entro una data definita. Nessuna eccezione può autorizzare pratiche vietate dalla legge o l'elusione dei controlli di sicurezza.

COLLEGAMENTO

Ogni sistema e caso d'uso rientrante nell'ambito deve essere censito nel Registro AI.

3. Definizioni e riferimenti

Usare lo stesso glossario del Registro AI.

3 — DEFINIZIONI [OBBLIGATORIO]

Ai fini della Policy: “Sistema AI” indica un sistema che genera contenuti, previsioni, raccomandazioni o decisioni; “Caso d’uso” l’attività concreta supportata; “Prompt” l’istruzione fornita; “Output” il risultato generato; “Supervisione umana” il controllo esercitato da una persona competente e autorizzata; “Shadow AI” l’uso non conosciuto o non autorizzato.

4 — RIFERIMENTI [OBBLIGATORIO]

La Policy è coordinata con il Regolamento (UE) 2024/1689, il Regolamento (UE) 2016/679, le indicazioni delle autorità competenti, le regole interne su sicurezza, privacy, lavoro e gestione documentale e, come riferimento organizzativo, ISO/IEC 42001.

4.1 — PREVALENZA DELLE NORME [OBBLIGATORIO]

In caso di conflitto prevalgono le disposizioni di legge e le istruzioni aziendali più restrittive applicabili al caso concreto.

5. Principi e responsabilità

Regole comuni per ogni utilizzo.

5 — PRINCIPI AZIENDALI [OBBLIGATORIO]

L'azienda utilizza l'AI secondo trasparenza, responsabilità, proporzionalità, qualità, sicurezza e supervisione umana. L'AI supporta le persone e non trasferisce al sistema la responsabilità professionale o decisionale.

6 — RUOLI [OBBLIGATORIO]

La Direzione approva Policy, usi rilevanti ed eccezioni. Il Responsabile del processo definisce finalità e controlli. Gli utilizzatori rispettano le regole, verificano gli output e segnalano problemi. Gli amministratori della piattaforma gestiscono accessi e configurazioni. Privacy, sicurezza, HR, qualità o compliance supportano le valutazioni quando pertinenti.

6.1 — APPROVAZIONE DI NUOVI STRUMENTI [OBBLIGATORIO]

Dipendente individua lo strumento → presenta richiesta → valutazione del caso d'uso e del fornitore → approvazione → inserimento nel Registro AI → formazione → utilizzo.

7. Utilizzi consentiti e vietati

Autorizzare attività precise, non prodotti generici.

7 — UTILIZZI CONSENTITI [OBBLIGATORIO]

Sono consentiti i casi d'uso autorizzati e registrati, svolti con account approvati, dati ammessi e controlli definiti. Possono includere bozze, sintesi, analisi, ricerca, classificazione e supporto operativo, purché l'output sia verificato in modo proporzionato.

8 — UTILIZZI VIETATI [OBBLIGATORIO]

È vietato inserire credenziali; utilizzare strumenti non autorizzati per dati aziendali; delegare decisioni rilevanti senza supervisione; eludere controlli e log; pubblicare contenuti ingannevoli; utilizzare l'AI per finalità incompatibili con legge, ruolo o istruzioni aziendali.

8.1 — SHADOW AI [OBBLIGATORIO]

Gli usi non autorizzati devono essere segnalati. L'azienda valuta se regolarizzare, limitare, sostituire o interrompere lo strumento e registra la decisione nel Registro AI.

9. Dati, prompt e sicurezza

Proteggere input, documenti, account e configurazioni.

9 — GESTIONE DEI DATI [OBBLIGATORIO]

Prima di inserire dati o documenti, l'utilizzatore verifica classificazione, necessità, strumento e piano autorizzati. Informazioni pubbliche possono essere usate con verifica; documenti interni richiedono attenzione; dati personali richiedono valutazione; categorie particolari, segreti e informazioni altamente riservate non sono inseriti salvo autorizzazione specifica. Credenziali e chiavi sono sempre vietate.

10 — PROMPT [CONSIGLIATO]

I prompt condivisi o riutilizzabili devono avere finalità, versione, responsabile, dati vietati e criteri di verifica. I prompt rilevanti sono conservati in un repository controllato e collegati al Registro Prompt. Solo persone autorizzate modificano i prompt approvati.

10.1 — SICUREZZA [OBBLIGATORIO]

Sono utilizzati account nominativi, privilegi minimi e misure di autenticazione previste. È vietato condividere credenziali o disattivare controlli senza autorizzazione.

11. Supervisione, output e fornitori

Controlli proporzionati alle conseguenze.

11 — SUPERVISIONE UMANA [OBBLIGATORIO]

Gli output che possono incidere su persone, denaro, obblighi, sicurezza o comunicazioni esterne sono verificati da una persona competente prima dell'uso. La persona deve poter correggere, respingere, sospendere o sottoporre il caso a escalation.

12 — VERIFICA DEGLI OUTPUT [OBBLIGATORIO]

La verifica considera accuratezza, completezza, fonti, tono, dati, destinatario e conseguenze. Gli output critici sono registrati quando previsto. Errori ricorrenti comportano revisione di prompt, dati, configurazione o processo.

13 — FORNITORI [OBBLIGATORIO]

Prima dell'adozione sono verificati servizio, piano, privacy, sicurezza, uso dei dati, subfornitori, trasferimenti, documentazione AI Act, continuità e uscita. L'esito è registrato nella Valutazione fornitori.

14. Formazione, incidenti e riesame

Chiusura approvabile dalla Direzione.

14 — FORMAZIONE [OBBLIGATORIO]

Le persone ricevono formazione iniziale e aggiornamenti proporzionati al ruolo, agli strumenti e ai rischi. Nuovi sistemi, incidenti e modifiche rilevanti possono richiedere formazione aggiuntiva. Le attività sono annotate nel Registro Formazione.

15 — INCIDENTI ED ECCEZIONI [OBBLIGATORIO]

Errori, divulgazioni, usi non autorizzati e malfunzionamenti sono segnalati, contenuti, valutati, corretti e registrati. Eccezioni motivate possono essere approvate dalla Direzione con durata, responsabile, condizioni e riesame.

16 — MONITORAGGIO, RIESAME ED ENTRATA IN VIGORE [OBBLIGATORIO]

La Policy è monitorata tramite Registro AI, dashboard, riesami e audit. È riesaminata almeno annualmente e dopo nuovi sistemi, incidenti rilevanti, modifiche organizzative, normative o dei fornitori. Entra in vigore il [data] ed è comunicata a tutti i destinatari.

APPROVAZIONE

Approvata da: _____ **Data:** _____ **Firma:** _____

Prima della pubblicazione interna

Verificare testo, allegati, riferimenti e processo di distribuzione.

Regolamento (UE) 2024/1689
eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1689

Commissione europea — AI Act
digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

EDPB — Documenti e linee guida
edpb.europa.eu/our-work-tools/our-documents_en

Garante Privacy — AI
garanteprivacy.it/temi/intelligenza-artificiale

ISO/IEC 42001:2023
iso.org/standard/42001

CHECKLIST DI ADOZIONE

☐ Personalizzata ☐ Approvata ☐ Distribuita ☐ Presa visione raccolta ☐ Registro AI aggiornato ☐ Formazione pianificata

DA RICORDARE

La Policy è un documento dinamico. Nuovi sistemi, processi, incidenti, fornitori o norme devono attivare una verifica.

DATA COMPILAZIONE	RESPONSABILE	PROSSIMO RIESAME

Presa visione della AI Policy

Conferma di ricezione, comprensione e impegno a rispettare le regole.

NOME E COGNOME

RUOLO / REPARTO

VERSIONE POLICY

DATA RICEZIONE

DICHIARAZIONE

Dichiaro di aver ricevuto e letto la AI Policy, di conoscere strumenti autorizzati, regole sui dati, controlli sugli output e canale di segnalazione.

DOMANDE O CHIARIMENTI RICHIESTI

FIRMA DEL DESTINATARIO

FIRMA / VERIFICA AZIENDALE

NOTA

La presa visione non sostituisce la formazione necessaria per ruolo e sistemi utilizzati.

VERSIONE	RESPONSABILE	DATA	PROSSIMO RIESAME	NOTE

Richiesta nuovo sistema o caso d’uso AI

La richiesta precede valutazione, approvazione, registrazione e formazione.

RICHIEDENTE / REPARTO

DATA / PRIORITÀ

SISTEMA, FORNITORE E PIANO

FINALITÀ E RISULTATO ATTESO

DATI E DOCUMENTI PREVISTI

PERSONE INTERESSATE

UTENTI E INTEGRAZIONI

ALTERNATIVA ATTUALE

ESITO / CONDIZIONI / ID DECISIONE

FLUSSO

Richiesta → valutazione → approvazione → Registro AI → formazione → utilizzo.

VERSIONE	RESPONSABILE	DATA	PROSSIMO RIESAME	NOTE

Segnalazione incidente AI

Segnalare rapidamente anche quando tutte le informazioni non sono ancora disponibili.

DATA E ORA

SEGNALATO DA

ID SISTEMA / CASO

EVENTO OSSERVATO

GRAVITÀ E TIPO DI IMPATTO

PERSONE / DATI COINVOLTI

CONTENIMENTO IMMEDIATO

RESPONSABILE E AZIONI

ESCALAZIONE / NOTIFICHE

ESITO, CHIUSURA E LEZIONE APPRESA

VERSIONE	RESPONSABILE	DATA	PROSSIMO RIESAME	NOTE

Richiesta di eccezione

Un’eccezione è temporanea, motivata, controllata e riesaminata.

RICHIEDENTE / REPARTO

REGOLA INTERESSATA

MOTIVAZIONE E RISULTATO NECESSARIO

DURATA RICHIESTA

SISTEMA / CASO D’USO

RISCHI E PERSONE INTERESSATE

MISURE COMPENSATIVE

ESITO E CONDIZIONI

APPROVATA DA

SCADENZA / RIESAME

ATTENZIONE

Nessuna eccezione può autorizzare pratiche vietate o l’elusione dei controlli di sicurezza.

VERSIONE	RESPONSABILE	DATA	PROSSIMO RIESAME	NOTE

Verbale revisione AI Policy

Documentare evidenze, decisioni e azioni del riesame.

ID VERBALE / DATA

VERSIONE ESAMINATA

RESPONSABILE

PARTECIPANTI E FUNZIONI

EVIDENZE ESAMINATE: REGISTRO AI, INCIDENTI, FORMAZIONE, FORNITORI, AUDIT

DECISIONI E MODIFICHE APPROVATE

AZIONI, RESPONSABILI E SCADENZE

APPROVAZIONE E PROSSIMO RIESAME

CHECKLIST AUDIT INTERNO

☐ Policy applicata ☐ Registro coerente ☐ Formazione aggiornata ☐ Incidenti chiusi ☐ Azioni monitorate

VERSIONE	RESPONSABILE	DATA	PROSSIMO RIESAME	NOTE

Distribuzione e storico revisioni

Conservare chi ha ricevuto la Policy e come il documento è cambiato.

A6 — REGISTRO DISTRIBUZIONE

DESTINATARIO	RUOLO	VERSIONE	DATA / CANALE	PRESA VISIONE

A7 — STORICO REVISIONI

VERSIONE	DATA	MODIFICHE	REDATTA DA	APPROVATA DA

CHIUSURA

Conservare la versione superata e distribuire sempre quella vigente.

VERSIONE	RESPONSABILE	DATA	PROSSIMO RIESAME	NOTE