

Regole e standard per un utilizzo responsabile dell'Intelligenza Artificiale Policy di Gruppo - Estratto

 Banco di Desio e della Brianza S.p.A.

1. Impegno del Gruppo Banco Desio sull'AI Responsabile

Il Gruppo Banco Desio adotta un modello di **AI Governance** volto a garantire un utilizzo dell'Intelligenza Artificiale **responsabile, etico, trasparente e sicuro**, in coerenza con i valori aziendali, gli obiettivi strategici e la normativa applicabile.

La Policy di AI Governance del Gruppo definisce **principi, regole, ruoli, processi e strumenti** per assicurare una gestione solida lungo l'intero ciclo di vita dei sistemi di IA, con particolare attenzione alle soluzioni di **AI generativa**.

2. Approvazione ed endorsement

La Policy di Gruppo "Regole e standard per un utilizzo responsabile dell'Intelligenza Artificiale" è stata **approvata dal Comitato Esecutivo** (CE) ed aggiornata in data **25/02/2026**.

3. Principi

Rispetto della privacy e protezione dei dati

Il Gruppo Banco Desio utilizza e sviluppa sistemi di IA nel rispetto della normativa privacy applicabile (incluso il GDPR) e delle disposizioni aziendali interne. È vietato condividere dati personali (specialmente i dati "particolari") con strumenti di IA non autorizzati; prima di fornire input a sistemi di IA è obbligatorio verificare l'eventuale presenza di dati personali e considerare ogni input come potenziale comunicazione a terzi.

Protezione della cybersecurity dei sistemi IA

Il Gruppo adotta presidi di robustezza, sicurezza e protezione dei sistemi di IA lungo tutto il loro ciclo di vita, anche tramite processi di test, monitoraggio, gestione log e tracciabilità, e in integrazione con i presidi di sicurezza informatica e di governance IT.

Prevenzione di *bias* e discriminazioni

Il Gruppo promuove un uso dell'IA ispirato a principi di **etica, equità e non discriminazione**. I sistemi devono essere progettati e utilizzati minimizzando errori e *bias*, prevenendo impatti discriminatori e pregiudizi ingiusti. Sono previsti controlli e verifiche su output e performance, anche per intercettare distorsioni o contenuti discriminatori.

Supervisione umana (“human in the loop”) e possibilità di intervento

È richiesto che l'IA **supporti le decisioni umane** e non le sostituisca. Gli output dei sistemi di IA non devono automatizzare decisioni senza verifica umana, in particolare quando coinvolgono dati personali. Il Gruppo prevede attività di supervisione umana rendicontata sugli esiti dei modelli, anche a campione, garantendo tracciabilità e dimostrabilità delle verifiche effettuate.

Trasparenza e comprensione

Il Gruppo promuove l'uso dell'IA in modo trasparente: le persone devono comprendere quando interagiscono con un sistema di IA e devono essere adottate misure per rendere comprensibili logiche, limiti e motivazioni degli output. Per i contenuti diffusi esternamente è obbligatorio attribuire chiaramente i contenuti generati dall'IA e segnalare in modo evidente contenuti visivi/audio/video generati o modificati dall'IA.

Accountability: responsabilità chiare sugli esiti prodotti dall'IA

La responsabilità dell'utilizzo e della diffusione degli output prodotti da sistemi di IA resta in capo al richiedente/utente, che è tenuto a verificarne accuratezza e appropriatezza. Il Gruppo ha definito un **framework organizzativo** (Centro di Eccellenza – CoE AI) con ruoli di business, compliance/etica, governance e tecnici per garantire responsabilità e presidi lungo l'intero ciclo di vita.

Confini chiari: cosa l'IA può e non può fare (uso consentito/vietato)

I sistemi di IA devono essere utilizzati esclusivamente per le finalità per cui sono stati progettati e secondo istruzioni del fornitore. Sono vietati comportamenti e utilizzi non autorizzati, tra cui: uso di credenziali aziendali su strumenti pubblici non approvati, installazione di plug-in/API non approvati, uso di codice generato da GenAI nei sistemi aziendali, utilizzo con terze parti senza autorizzazione contrattuale.

Divieto di sistemi proibiti (AI Act): manipolazione, sfruttamento vulnerabilità, social scoring, biometric surveillance non autorizzata

La Policy recepisce i **comportamenti vietati** previsti dall'AI Act, includendo divieti su sistemi manipolativi/subliminali/ingannevoli, sfruttamento vulnerabilità, classificazioni con trattamenti pregiudizievoli, *scraping* indiscriminato per riconoscimento facciale, deduzione emozioni sul lavoro (salvo sicurezza), categorizzazione biometrica su attributi sensibili e uso di sistemi biometrici in tempo reale in aree pubbliche per fini di sicurezza pubblica.

4. Programmi di Responsible AI

Limitazione accesso a capacità AI sensibili (es. *facial recognition*, sorveglianza)

Il Gruppo adotta un modello di governance e autorizzazione che limita l'impiego di capacità AI potenzialmente sensibili (es. biometria, sorveglianza, funzionalità ad alto impatto sui diritti) ai soli casi consentiti dalla normativa e previa valutazione del rischio, approvazione e tracciamento delle responsabilità.

Etichettatura/*labeling* di contenuti generati da AI ed esiti di decisioni AI-driven

La Policy prevede obblighi di **attribuzione** per contenuti generati dall'IA destinati all'esterno e segnalazione evidente per contenuti multimediali generati/modificati da IA. Questo soddisfa il requisito di *labeling* per contenuti.

Ove applicabile, il Gruppo si impegna a garantire adeguata trasparenza quando un esito/valutazione che impatta clienti o *stakeholder* sia significativamente supportato da sistemi di IA, coerentemente con i requisiti normativi e con i presidi di supervisione umana.

Meccanismi per rilevare e correggere “drift” o degrado delle performance nel tempo

La Policy prevede monitoraggio periodico delle performance per evitare degrado nel tempo e azioni correttive; inoltre, prevede ricalibrazione continua dei modelli e gestione strutturata delle segnalazioni/anomalie.

Processo di ricorso/contestazione (*appeals*) per utenti o terzi impattati da decisioni AI

Il Gruppo ha previsto presidi organizzativi e canali interni di segnalazione che consentono il riesame, con supervisione umana, di eventuali anomalie o criticità rilevate nell'utilizzo di sistemi di Intelligenza Artificiale a supporto dei processi aziendali interni, garantendo tracciabilità e responsabilità nella gestione degli esiti.

Formazione dei dipendenti su uso etico e/o sicurezza dell'AI

La Policy prevede un principio esplicito di alfabetizzazione e competenza nell'uso dell'AI. È obbligatorio garantire che le persone coinvolte nella progettazione, adozione o utilizzo dei sistemi di IA siano adeguatamente formate sui rischi, i limiti, le responsabilità e i principi etici applicabili.

Nell'ambito di tale principio, la Policy richiede inoltre che i fornitori mettano a disposizione materiali informativi e formativi sui sistemi forniti, e che tali contenuti siano recepiti prima dell'attivazione delle soluzioni.

Verifica esterna del sistema di gestione AI

Il Gruppo Banco Desio ha definito il proprio modello di AI Governance facendo riferimento a standard e framework riconosciuti a livello internazionale, utilizzati come linee guida metodologiche per la progettazione e il rafforzamento dei presidi organizzativi, di controllo e di gestione dei rischi legati all'Intelligenza Artificiale.

Allo stato attuale, il sistema di gestione dell'Intelligenza Artificiale **non è oggetto di certificazione né di verifica esterna indipendente**, ferma restando la presenza di presidi interni di governance, monitoraggio e controllo in coerenza con il framework adottato.

5. Governance, processi e controlli

Modello organizzativo e ruoli

Il Gruppo ha formalizzato la governance dell'Intelligenza Artificiale attraverso l'**evoluzione dell'organigramma aziendale**, introducendo specifici ruoli dedicati, che coprono ambiti di Business, Governance, Compliance/Etica e Tecnici.

Nell'ambito di tale assetto organizzativo sono stati definiti responsabilità e presidi lungo l'intero ciclo di vita dei sistemi di IA, mediante l'istituzione di ruoli specialistici (tra cui AI Strategy Manager, AI Delivery Manager, AI Developer, Data Engineer, Data Quality Specialist, AI Compliance/Risk/Legal & DPO Specialist e Utente Richiedente), integrati nei processi aziendali esistenti.

Strumenti: checklist di classificazione del rischio AI

È previsto l'uso di una **Checklist di Classificazione del Rischio AI** obbligatoria in fase di richiesta per iniziative con uso di AI e in caso di modifiche rilevanti su sistemi in esercizio (evolutive, nuove finalità, *retraining*, migrazione infrastrutturale), per classificare il rischio (proibito/alto/limitato/minimo), identificare il ruolo del Gruppo e attivare gli adempimenti di compliance.

Monitoraggio, logging, ticketing, documentazione e miglioramento continuo

Il Gruppo adotta misure strutturate di monitoraggio e controllo, in particolare per sistemi ad alto rischio: supervisione umana rendicontata, integrazione nel *ticketing*, valutazioni

periodiche di efficienza operativa, ricalibrazione continua, analisi interazioni tra sistemi, conservazione e gestione log, documentazione tecnica aggiornata e auditabile.

6. Regole per l'acquisto responsabile e gestione fornitori

Il Gruppo richiede test e verifiche dei sistemi AI (privacy, riservatezza, proprietà intellettuale, sicurezza, coerenza con finalità, assenza di distorsioni/allucinazioni/contenuti discriminatori/illegali). È inoltre richiesto monitoraggio delle performance nel tempo e azioni correttive se necessario.

Per soluzioni AI che comportino trattamento di dati personali, si applicano i requisiti di conformità privacy (incluse valutazioni di impatto ove necessarie) e formalizzazione del rapporto con i fornitori anche tramite nomine ex art. 28 GDPR quando applicabile. I rapporti con i fornitori devono essere formalizzati con accordi/licenze che disciplinino obblighi, responsabilità e diritti di risoluzione.

7. Contatti, segnalazioni e gestione violazioni

La Policy prevede che le funzioni di controllo e, per i profili di competenza, il DPO di Gruppo monitorino l'implementazione e possano effettuare verifiche per individuare violazioni; le violazioni possono comportare procedimenti disciplinari e azioni legali a tutela della società.

Per richieste di chiarimento, segnalazioni o contestazioni relative a sistemi di IA, è possibile utilizzare i canali di contatto e assistenza del Gruppo, che attiveranno il processo di presa in carico e riesame con le funzioni competenti, in coerenza con i presidi di governance e supervisione umana.