# POLITICA E PROCEDURE PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

| Rev. | Data | Descrizione | Elaborato da | Verificato da | Validato da |
|---|---|---|---|---|---|
| 1.0 | 10/03/2025 | Prima Emissione | Sara Di Silverio (Head of Management) | Daniele Angiolelli (COO) | Domenico De Monte (CEO) |

*1 Scopo* ..... *3*
*2 Ambito di applicazione* ..... *3*
*3 Definizioni* ..... *3*
*4 Riferimenti normativi e standard ISO* ..... *4*
*5 Ruoli e responsabilità* ..... *4*
*6 Principi guida per l'utilizzo dell'AI* ..... *5*
*7 Classificazione dei sistemi AI approvati* ..... *5*
*8 Requisiti di sicurezza e protezione dei dati* ..... *6*
*9 Validazione e gestione dei modelli: ChatGPT, Gemini, LLaMA* ..... *6*
**9.1 Principi comuni di validazione a carico del fornitore** ..... **6**
*10 Gestione delle eccezioni* ..... *7*
*11 Vendor Assestment & Contrattualistica* ..... *7*
*12 DPIA e Analisi dei Rischi* ..... *7*
*13 Monitoraggio, metriche e reporting* ..... *8*
*14 Incident Response per eventi AI* ..... *8*
*15 Test, Red Teaming e valutazioni di robustezza* ..... *9*
*16 Formazione e consapevolezza* ..... *9*
*17 Audit, certificazione e miglioramento continuo* ..... *9*
*18 Revisione della Policy* ..... *9*

# 1 Scopo

Questo documento integra la policy generale adottata dalla direzione e disponibile al presente link https://www.netsons.com/contratti

Definisce la politica, le procedure e i controlli necessari per **l'utilizzo** sicuro, etico e conforme alle normative applicabili alle tecnologie di Intelligenza Artificiale (AI) all'interno di Netsons.

Include requisiti specifici per la validazione e il governo di tre tecnologie AI qualificate:

- ChatGPT (OpenAI) - https://openai.com/it-IT/policies/
- Gemini (Google) - https://gemini.google/policy-guidelines/?hl=it
- LLaMA (Meta / modelli open-source) - https://ai.meta.com/llama/use-policy/

# 2 Ambito di applicazione

Il presente documento si applica a tutta l'organizzazione di Netsons che utilizza o intende utilizzare sistemi basati su AI al fine di efficientare i processi (principali e a supporto) affidati.

Per quanto al paragrafo precedente sono inclusi, a titolo esemplificativo e non esaustivo:

- comunicazione e marketing (elaborazione e ottimizzazione di testi tramite il sistema AI, copywriting assistito);
- supporto clienti (utilizzo del sistema AI per approfondire contenuti di una risposta efficacie);
- informazioni di mercato (informazioni pubbliche), ricerca e deepsearch;
- tooling per sviluppo e sicurezza (sviluppo di codice e successivo test di codice in ambiente sicuro).

Sono esclusi sistemi sperimentali privi di impatti operativi e prototipi non destinati alla produzione, a meno che non vengano esplicitamente autorizzati dal CISO (vedasi paragrafo 1).

Nel caso in cui l'utilizzo dell'intelligenza artificiale coinvolga il trattamento dei dati personali è previso il coinvolgimento del DPO per le relative valutazioni.

# 3 Definizioni

**AI System / Sistema AI**: qualsiasi sistema software che utilizza tecniche di machine learning, deep learning o regole basate su modelli per effettuare predizioni, generare contenuti o supportare decisioni.

**Data Controller / Data Processor**: definizioni come da GDPR - Netsons può agire in entrambe le vesti a seconda del servizio offerto.

**DPIA (Data Protection Impact Assessment):** valutazione obbligatoria quando l'uso del sistema comporta rischi elevati per i diritti e le libertà delle persone.

**PII (Personally Identifiable Information)**: informazioni che identificano direttamente o indirettamente una persona fisica.

**FRIA (Fundamental Rights Impact Assessment):** processo formale e documentato che mira a valutare gli impatti di un sistema AI su tutti i diritti fondamentali della persona, andando oltre la sola privacy.

# 4 Riferimenti normativi e standard ISO

Documenti e standard di riferimento:

- ISO 9001 Qualità
- ISO 14001 Ambiente
- ISO 27001 Sicurezza delle informazioni (tenendo conto delle ISO 27017 e ISO 27018)
- ISO 22301 Business Continuity
- ISO 27701 Sicurezza delle informazioni personali.
- ISO 42001 (AI management systems)
- ISO 20000 (gestione dei servizi IT)
- ISO/IEC 23894 (AI risk management)
- EU AI Act Regolamento 2024/1689
- Legge 132/2025 (ad integrazione delle norme dell'AI Act)
- GDPR (Regolamento UE 2016/679)
- NIS2 Directive

# 5 Ruoli e responsabilità

- **Direzione:** approvazione della policy AI, allocazione delle risorse e supervisione strategica.
- **Responsabile AI Governance**: stesura delle policy, gestione del registro dei casi d'uso, validazione dei modelli e review periodica.
- **CISO / Responsabile Sicurezza delle informazioni**: valutazione dei rischi tecnici, implementazione dei controlli di sicurezza, gestione incidenti.
- **Responsabile Privacy / DPO**: valutazioni DPIA, verifica della conformità GDPR, supervisione delle attività di trattamento dati.
- **Business Owner** (per use case): definizione dei requisiti di business, accettazione dei risultati e monitoraggio operativo.
- **Utenti autorizzati**: uso conforme alle policy, segnalazione di anomalie.

# 6 Principi guida per l'utilizzo dell'AI

- Legalità e conformità (GDPR, normative nazionali ed EU AI Act).
- Trasparenza e spiegabilità: ogni sistema AI in uso deve superare verifiche di trasparenza e spiegabilità (disponibilità di policy) garantite da fornitori qualificati.
- Sicurezza by design e by default: protezioni adeguate per dati e modelli.
- Human-in-the-loop per decisioni critiche e output destinati a clienti esterni: ogni output destinato a clienti/utenti non deve violare i principi riconducibili alla dignità dell'individuo e possono essere adottati solo sotto supervisione umana.
- Gestione del rischio e validazione tecnica: l'utilizzo dell'AI all'interno di un processo non deve generare rischi inaccettabili piuttosto deve essere adottato come strumento di mitigazione del rischio (fare riferimento al risk managemente del SGI).
- Accountability: logging completo e tracciabilità delle decisioni AI. I sistemi AI autorizzati devono essere gestiti mediante account aziendale in modo tale da riportare ogni interazione utente/AI nel campo di applicabilità della presente policy.
- Equità e non discriminazione: monitoraggio e mitigazione dei bias; il sistema di AI non deve in alcun modo contribuire all'emarginazione di gruppo vulnerabili, all'inasprimento di pregiudizi e di discriminazioni; l'equità deve essere integrata all'interno del sistema AI utilizzato fin dalla scelta dei dati inseriti dall'utente.
- Robustezza tecnica e sicurezza: i sistemi di AI devono essere resilienti e sicuri; devono garantire il backup in caso di criticità e generare output che risultino affidabili e riproducibili.
- Privacy e governance dei dati: in linea con quanto richiesto dal GDPR, i sistemi di AI devono garantire un uso conforme del trattamento dei dati personali e proteggere i dati degli utenti utilizzatori, pertanto, devono essere garantiti adeguati meccanismi di governance dei dati.
- Benessere sociale e aspetti ambientali: i sistemi di AI devono essere uno strumento al servizio dell'utente, comprese le generazioni future; l'uso dell'AI deve essere integrato con l'ambiente circostante considerando anche l'impatto sociale e ambientale che la nuova tecnologia induce.
- Accountability e responsabilità: l'utilizzo dell'AI da parte dell'organizzazione Netsons prevede un uso responsabile e consapevole.

# 7 Classificazione dei sistemi AI approvati

Netsons ha adottato un sistema di classificazione di sistemi AI in funzione del rischio, tenendo conto dell'AI ACT al quale si rimanda per ulteriori approfondimenti.

I sistemi AI utilizzati in Netsons sono classificati per livello di impatto e sensibilità secondo il seguente schema:

- Livello 1 (Minimo o nullo): strumenti di produttività interna, suggerimenti non critici.
- Livello 2 (Limitato): assistenti per marketing, analisi dati interne, suggerimenti tecnici.

    - I sistemi AI adottati in netsons di cui al primo paragrafo sono classificati come appartenenti al livello 2; si tenga comunque in considerazione quanto definito dal paragrafo "gestione delle eccezioni".
- Livello 3 (Elevato): chatbot pubblici che possono influenzare clienti, sistemi decision support per configurazioni infrastrutturali, automazioni che impattano SLA/servizi.
- Livello 4 (Inaccettabile): è considerato inaccettabile un sistema che utilizza tecniche subliminali senza che un utente ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di influenzare il comportamento di uno o più individui.

Nel caso in cui si intendesse introdurre un nuovo sistema AI, deve essere identificato il livello di rischio associato, ivi inclusi i controlli applicabili.

# 8 Requisiti di sicurezza e protezione dei dati

In riferimento ai sistemi autorizzati di cui al paragrafo 1, i requisiti di sicurezza sono demandati al fornitore.

I requisiti comportamentali, ad integrazione di quanto definito dal regolamento informatico, per un utilizzo sicuro e consapevole dell'AI, possono essere così sintetizzati:

- Non inserire mai PII, ivi incluse credenziali, codici fiscali, nomi e cognomi o comunque informazioni personali che possono essere aggregate e riconducibili ad un individuo;
- Supervisionare ed eventualmente rielaborare e ricontestualizzare sempre l'output ricevuto dall'AI.

# 9 Validazione e gestione dei modelli: ChatGPT, Gemini, LLaMA

## 9.1 Principi comuni di validazione a carico del fornitore

Prima dell'impiego in produzione, ogni modello o servizio AI deve superare una serie di controlli che si suddividono come segue:

- Documentazione Model Card e Dataset Card (provenienza dati, limiti, metriche).
- Security & privacy review (DPIA se necessario).
- Test di accuratezza, robustezza e resistenza a prompt adversarial.
- Verifica di bias e fairness su sample rappresentativi.
- Definizione di metriche di accettazione (accuracy, precision, recall, hallucination rate, safety pass rate).
- Red-team e penetration test su componenti esposti.

# 10 Gestione delle eccezioni

In caso di necessità aziendali che comportino delle azioni non previste dalla presente policy, sarà necessario richiedere l'intervento del CISO per richiedere una preventiva autorizzazione.

Si considera un'eccezione alla policy, una circostanza non prevista o straordinaria che richiede un trattamento specifico e differenziato. Nel caso in cui si verificasse una cosiddetta "eccezione", potrà essere necessario adottare misure temporanee o transitorie o adatte esclusivamente alla situazione contingente. Le eccezioni devono permettere una gestione flessibile degli scenari senza la necessità di revisionare la policy.

Pertanto, il CISO, per la specifica eccezione, dovrà produrre una valutazione di impatto del sistema AI da utilizzare, specificando le misure di limitazione del rischio, anche temporanee, da adottare all'interno dell'organizzazione.

Nel caso in cui l'eccezione riguardasse dati personali, il CISO contatta il DPO per condividere la valutazione di impatto, prima di autorizzare l'eccezione.

# 11 Vendor Assestment & Contrattualistica

Per qualsiasi fornitore AI si intende applicare la seguente procedura minima di valutazione ai fini della contrattualizzazione.

La semplificazione della procedura di approvvigionamento è strettamente collegata al solo utilizzo dell'AI nei processi di supporto, già identificati nei paragrafi precedenti.

A tale scopo dovranno essere valutati i seguenti punti:

- Due Diligence (certificazioni: ISO27001, SOC2, evidenze di sicurezza).
- Verifica Data Processing Agreement (DPA) e appendice per sub-processors.
- Clausole su data residency e limitazioni di trattamento dati.
- SLA su availability, time-to-response per incidenti e risoluzione.
- Diritto di audit e accesso ai log (ove possibile) o reportistica periodica.
- Indennizzi e limiti di responsabilità relativi a breach e violazioni normative.

Le evidenze dell'assestment dovranno essere formalizzate mediante archiviazione o registrazione del controllo all'interno del gestionale aziendale (es. youtrack, google drive..).

# 12 DPIA e Analisi dei Rischi

Eseguire una Data Protection Impact Assessment (DPIA) per tutti i progetti AI che trattano PII o che possono avere impatti elevati sui diritti degli interessati.

Le fasi da seguire per la DPIA sono:

1. Descrizione del trattamento e scopo.

2. Valutazione della necessità e proporzionalità.
3. Identificazione dei rischi per i diritti e le libertà.
4. Misure di mitigazione proposte.
5. Valutazione residua del rischio e decisione del DPO.

L'utilizzo consentito dell'IA all'interno dell'organizzazione Netsons, non può e non deve considerare PII, pertanto si ritiene la DPIA non necessaria.

# 13 Monitoraggio, metriche e reporting

Nel caso in cui Netsons intendesse sviluppare soluzioni integrate con l'IA si prevede, in prima istanza, di definire metriche e KPIs, soggetti a monitoraggio continuo, per ogni sistema AI in produzione; a titolo esemplificativo e non esaustivo:

- performance technique: latency, throughput, error rate, availability.
- Quality metrics: accuracy, precision, recall, F1, hallucination rate (per generative).
- Fairness metrics: disparate impact, per-group performance.
- Drift detection: data drift, concept drift.
- Security metrics: anomalous access attempts, number of incidents.

Inoltre, per quanto si guarda il reporting, si prevede: rapporti mensili al CISO al quale si riconoscono i poteri in merito all'AI e review trimestrale con la Direzione.

# 14 Incident Response per eventi AI

Le procedure specifiche per incidenti legati all'utilizzo dell'AI (es. perdita di dati, output offensivi, bias rilevato) si concretizzano nelle seguenti fasi:

1) Identificazione e classificazione
2) Contenimento immediato (disabilitare modello, limitare accessi, rollback a versione safe).
3) Analisi forense e root-cause.
4) Comunicazione interna e notifiche esterne (DPO, clienti impattati, autorità competenti entro i termini GDPR se necessario).
5) Remediation, patching e preventive measures.
6) Post-incident review e aggiornamento policy.

L'incident reporting viene formalizzato sui sistemi aziendali, es. youtrack.

# 15 Test, Red Teaming e valutazioni di robustezza

Nell'eventualità della produzione di servizi integrati con l'IA, prima della messa in produzione è obbligatorio eseguire test di robustezza e operazioni di red teaming che includano:

- Prompt injection tests, adversarial inputs, stress tests.
- Test su bias con dataset rappresentativi.
- Security penetration tests su API e layer esposti.
- Report di risultati e piano di remediation obbligatorio prima del go-live.

I test, red teaming e valutazione di robustezza saranno tracciati e formalizzati sui sistemi aziendali, es. youtrack.

# 16 Formazione e consapevolezza

Netsons definisce un programma di formazione obbligatorio per tutti gli utenti autorizzati. I contenuti minimi di questo piano di formazione sono:

- Introduzione ai rischi dell'AI e principi di sicurezza nell'uso consapevole dell'IA.
- Policy aziendale e regolamento aziendale con particolare rilevanza al consapevole utilizzo dell'IA.
- Reporting di incidenti e uso responsabile.

Nel caso in cui si intendesse mettere in produzione soluzioni IA, il piano formativo tratterà anche i seguenti argomenti:

- Linee guida su prompt engineering sicuro.
- Privacy by design e trattamento dei dati personali.
- Procedura aziendale di sviluppo.

Viene definita la seguente frequenza in merito alla formazione: onboarding e refresher almeno annuale.

# 17 Audit, certificazione e miglioramento continuo

Netsons eseguirà audit interni almeno annuali e audit esterni annuali sull'utilizzo dell'AI nei processi aziendali.

Il monitoraggio del rispetto delle policy aziendali è affidato ai responsabili di funzione, con frequenza settimanale.

# 18 Revisione della Policy

In sede di Riesame della Direzione e comunque almeno una volta l'anno (tenendo conto anche dei cambiamenti del contesto o dei processi aziendali), l'Alta Direzione riesamina i contenuti della presente policy ed emette eventuali revisioni.