

	Codice	Revisione	Titolo	
	POL-005	01	Uso sicuro sistemi AI	
	Data		Classificazione	Uso Interno
	29/05/2025			

**GAMMA S.R.L.**  
POLITICA  
**USO SICURO DEI SISTEMI DI INTELLIGENZA  
ARTIFICIALE**

Data	Rev.	Oggetto della modifica
29/05/2025	01	Prima emissione

## 1. SCOPO E CAMPO DI APPLICAZIONE

La presente politica definisce i principi, le regole e le responsabilità per l'utilizzo sicuro dei sistemi di Intelligenza Artificiale (AI) all'interno di Gamma, in conformità a:

- ISO/IEC 27001:2022 - Controllo A.8.27 (Secure system architecture and engineering principles)
- Regolamento UE 2024/1689 (AI Act) - Requisiti per sistemi AI ad alto rischio
- GDPR (Reg. UE 2016/679) - Protezione dei dati personali
- Linee Guida AgID sull'uso dell'intelligenza artificiale nella PA

La politica si applica a:

- Tutto il personale e collaboratori di Gamma
- Collaboratori esterni e consulenti
- Qualsiasi utilizzo di sistemi AI, sia interni che esterni (cloud-based)

## 2. DEFINIZIONI

Termine	Definizione
<b>Sistema AI</b>	Sistema basato su machine learning progettato per generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali
<b>AI Generativa</b>	Sistemi AI in grado di generare testo, immagini, codice o altri contenuti (es. ChatGPT, Claude, Copilot, Midjourney, DALL-E)
<b>AI Pubblica</b>	Servizi AI accessibili via internet senza garanzie specifiche sulla riservatezza dei dati inseriti (versioni gratuite o consumer)
<b>AI Enterprise</b>	Servizi AI con accordi contrattuali che garantiscono riservatezza, non utilizzo dei dati per training, compliance GDPR
<b>Prompt</b>	Input testuale fornito a un sistema AI per ottenere una risposta o generare contenuto
<b>Allucinazione AI</b>	Output generato dall'AI che appare plausibile ma è fattualmente errato o inventato

## 3. PRINCIPI FONDAMENTALI

L'utilizzo di sistemi AI in Gamma è governato dai seguenti principi:

	<b>Codice</b>	<b>Revisione</b>	<b>Titolo</b>	
	<b>POL-005</b>	01	Usa sicuro sistemi AI	
	<b>Data</b>		<b>Classificazione</b>	Usa Interno
	29/05/2025			

### 3.1 Supervisione Umana (Human-in-the-Loop)

Ogni output generato da sistemi AI deve essere verificato e validato da personale competente prima di essere utilizzato, pubblicato o comunicato a terzi. L'AI è uno strumento di supporto, non un sostituto del giudizio umano. La responsabilità finale delle decisioni e dei contenuti rimane sempre in capo al personale che li utilizza.

### 3.2 Protezione dei Dati

È vietato inserire in sistemi AI pubblici qualsiasi dato personale, dato sensibile, informazione riservata aziendale o dato dei clienti. I dati trattati nell'ambito del servizio di conservazione digitale non devono mai essere esposti a sistemi AI esterni non autorizzati.

### 3.3 Trasparenza

Quando contenuti generati con supporto AI sono destinati a clienti o terzi, tale circostanza deve essere comunicata ove rilevante. L'utilizzo di AI nel servizio erogato deve essere dichiarato nella documentazione contrattuale se significativo.

### 3.4 Accountability

Chi utilizza sistemi AI è responsabile dell'output prodotto e delle conseguenze del suo utilizzo. L'utilizzo di AI non esime dalla responsabilità professionale né può essere invocato come giustificazione per errori o omissioni.

## 4. CATEGORIE DI UTILIZZO E REGOLE SPECIFICHE

### 4.1 Uso Interno Operativo

**Ambito:** Supporto alle attività quotidiane del personale (redazione documenti, analisi, ricerche, codice).

✓ CONSENTITO	X VIETATO
Ricerche su normative e best practice	Inserire dati personali di clienti o dipendenti
Bozze di documenti interni	Caricare documenti dei clienti
Supporto alla programmazione (codice generico)	Inserire credenziali, chiavi API, password
Sintesi di documenti pubblici	Condividere codice proprietario
Traduzione di testi non riservati	Elaborare informazioni classificate come Riservate

#### Regole operative:

1. Prima di inserire qualsiasi informazione, verificare che non contenga dati personali, dati clienti o informazioni riservate
2. Utilizzare dati fittizi o anonimizzati per testare funzionalità o ottenere esempi
3. Verificare sempre l'accuratezza degli output prima dell'utilizzo (rischio allucinazioni)
4. Non fare affidamento su citazioni, riferimenti normativi o dati numerici senza verifica indipendente

### 4.2 Uso a Supporto Commerciale e Marketing

**Ambito:** Creazione di contenuti per comunicazione esterna, materiale commerciale, presentazioni per clienti.

#### Regole operative:

1. Ogni contenuto generato con AI destinato all'esterno deve essere revisionato e approvato dal responsabile della funzione
2. I testi devono essere personalizzati e verificati: l'AI fornisce una bozza, non il prodotto finale
3. Non dichiarare capacità o caratteristiche del servizio basandosi solo su output AI non verificati
4. Le immagini generate con AI devono essere dichiarate come tali se utilizzate in documenti ufficiali
5. Verificare che i contenuti non violino diritti di proprietà intellettuale di terzi

### 4.3 Uso nel Servizio di Conservazione

	<b>Codice</b>	<b>Revisione</b>	<b>Titolo</b>	
	<b>POL-005</b>	01	Uso sicuro sistemi AI	
	<b>Data</b>		<b>Classificazione</b>	Uso Interno
	29/05/2025			

**Ambito:** Integrazione di funzionalità AI nel sistema o nei processi di conservazione.

**Principi vincolanti:**

1. Dichiarazione preventiva: qualsiasi utilizzo di AI nel servizio erogato ai clienti deve essere comunicato nella documentazione contrattuale e nel Manuale della Conservazione
2. Nessun trattamento automatizzato: l'AI non può prendere decisioni autonome sulla validità, conformità o conservabilità dei documenti senza validazione umana
3. Protezione dei documenti: i documenti dei clienti non devono mai essere trasmessi a sistemi AI esterni; eventuali funzionalità AI devono operare in ambiente isolato
4. Tracciabilità: ogni operazione effettuata con supporto AI deve essere tracciata nei log di sistema
5. Valutazione rischi: prima dell'introduzione di funzionalità AI nel servizio, deve essere condotta una valutazione dei rischi e, se necessario, una DPIA

	<b>Codice</b>	<b>Revisione</b>	<b>Titolo</b>	
	<b>POL-005</b>	01	Uso sicuro sistemi AI	
	<b>Data</b>		<b>Classificazione</b>	Uso Interno
	29/05/2025			

## 5. SISTEMI AI AUTORIZZATI

L'utilizzo di sistemi AI è consentito esclusivamente per le piattaforme e secondo le modalità indicate nella seguente tabella:

Sistema	Tipologia	Uso Consentito	Dati Ammessi	Autorizzazione
Microsoft Copilot (M365)	Enterprise	Interno operativo, commerciale	Dati interni (no clienti)	<b>Autorizzato</b>
GitHub Copilot	Enterprise	Supporto sviluppo codice	Codice generico (no secrets)	<b>Autorizzato</b>
ChatGPT (versione gratuita)	Pubblica	Solo ricerche generiche	Nessun dato aziendale	<b>Limitato</b>
Claude (Anthropic) free	Pubblica	Solo ricerche generiche	Nessun dato aziendale	<b>Limitato</b>
Midjourney, DALL-E, etc.	Pubblica	Immagini generiche	No logo, no dati	<b>Limitato</b>
AI non elencate sopra	-	-	-	<b>Da autorizzare</b>

Per richiedere l'autorizzazione all'uso di nuovi sistemi AI, contattare il Responsabile SGSI con indicazione di: nome del sistema, fornitore, finalità d'uso, tipologia di dati da trattare.

## 6. DIVIETI ASSOLUTI

Indipendentemente dal sistema AI utilizzato, è sempre vietato:

1. Inserire dati personali di clienti, dipendenti o terzi in sistemi AI pubblici
2. Caricare documenti oggetto di conservazione digitale
3. Inserire informazioni classificate come Riservate o Strettamente Riservate
4. Condividere credenziali di accesso, chiavi API, certificati digitali, chiavi crittografiche
5. Condividere il codice sorgente proprietario di MarteWeb2
6. Utilizzare AI per prendere decisioni automatizzate che producono effetti giuridici su persone fisiche
7. Utilizzare output AI senza verifica per comunicazioni ufficiali, pareri legali o attestazioni
8. Generare contenuti ingannevoli, diffamatori o che possano violare diritti di terzi

## 7. RESPONSABILITÀ

Ruolo	Responsabilità
<b>Direzione Generale</b>	Approvazione della politica, allocazione risorse per formazione, decisioni strategiche sull'adozione di AI nel servizio
<b>Responsabile SGSI</b>	Gestione dell'elenco sistemi AI autorizzati, valutazione richieste nuovi sistemi, monitoraggio conformità, aggiornamento politica
<b>DPO</b>	Valutazione impatto privacy (DPIA) per nuove AI, verifica conformità GDPR, gestione richieste interessati
<b>IT Manager</b>	Configurazione sicura degli strumenti AI enterprise, controllo accessi, monitoraggio tecnico, protezione prompt/modelli
<b>Tutto il Personale</b>	Rispetto della politica, verifica output AI, segnalazione incidenti o dubbi al Responsabile SGSI

## 8. FORMAZIONE E SENSIBILIZZAZIONE

Tutto il personale che utilizza sistemi AI deve ricevere adeguata formazione su:

- Contenuti della presente politica e relative responsabilità
- Rischi specifici dell'AI: allucinazioni, bias, violazioni privacy
- Tecniche per formulare prompt efficaci senza esporre dati sensibili
- Modalità di verifica e validazione degli output AI

La formazione viene erogata: al momento dell'assunzione, annualmente come refresh, ad ogni modifica significativa della politica o introduzione di nuovi strumenti AI.

## 9. GESTIONE INCIDENTI E VIOLAZIONI

In caso di violazione della presente politica o incidente legato all'uso di AI:

1. Segnalare immediatamente al Responsabile SGSI tramite email o canale dedicato
2. Documentare: sistema AI coinvolto, dati potenzialmente esposti, azioni intraprese

	<b>Codice</b>	<b>Revisione</b>	<b>Titolo</b>	
	<b>POL-005</b>	01	Uso sicuro sistemi AI	
	<b>Data</b>		<b>Classificazione</b>	Uso Interno
	29/05/2025			

3. Il Responsabile SGSI valuta se l'incidente configura un data breach e attiva la procedura PRO-002 se necessario

4. Se coinvolti dati personali, il DPO valuta l'obbligo di notifica al Garante entro 72 ore

Le violazioni intenzionali o reiterate della politica possono comportare provvedimenti disciplinari secondo il regolamento interno.

## 10. REVISIONE E AGGIORNAMENTO

La presente politica è soggetta a:

- Revisione annuale ordinaria
- Aggiornamento straordinario in caso di: nuove normative (es. AI Act), incidenti significativi, introduzione di nuovi sistemi AI, cambiamenti nei servizi erogati