POLITICA AZIENDALE
PER L'INTELLIGENZA ARTIFICIALE

Artificial Intelligence Management System (AIMS) | ISO/IEC 42001:2023

Versione	1.0
Data	04 giugno 2026
Stato	Prima Versione - Approvata
Società	Soft Strategy S.p.A.
Owner	Emanuele Donati — Responsabile AI di Gruppo / AI Center Director
Approvatore previsto	Emanuele Hermes Candela — Amministratore Delegato
Sedi operative	Roma — Via Cristoforo Colombo 115 Valenzano — Strada Provinciale per Casamassima km 3, c/o Technopolis, 70010 Valenzano (BA)
Classificazione	Pubblico

La presente Politica diviene efficace a seguito della sua approvazione e pubblicazione secondo le disposizioni documentali aziendali.

Sommario

PARTE I — POLITICA GENERALE PER L'INTELLIGENZA ARTIFICIALE 3
1. Indirizzo e campo di applicazione 3
2. Principi etici e AI con ESG by Design 4
3. Governance, responsabilità e competenze decisionali 5
4. Sistemi e strumenti AI, dati, fornitori e autorizzazioni 5
5. Rischi, obblighi normativi e prevenzione degli illeciti 6
6. Ciclo di vita, supervisione, monitoraggio e incidenti 7
7. Formazione, competenze e AI Literacy 8
8. Valutazione delle prestazioni, documentazione e miglioramento 8
PARTE II — POLITICA AI PER IL PROFILO USER 9
9. Strumenti, account e informazioni trattabili 9
10. Controllo degli output, trasparenza e impieghi sensibili 10
PARTE III — POLITICA AI PER IL PROFILO DEVELOPER 11
11. Progettazione responsabile ed ESG by Design 11
12. Validazione, fornitura e presidio operativo delle soluzioni 12
PARTE IV — POLITICA AI PER IL PROFILO RESEARCHER 13
13. Governance delle sperimentazioni e integrità scientifica 13
14. Ricerca sostenibile e trasferimento dei risultati 14
DISPOSIZIONI FINALI 15
15. Applicazione, riferimenti e riesame 15

PARTE I — POLITICA GENERALE PER L'INTELLIGENZA ARTIFICIALE

1. Indirizzo e campo di applicazione

Soft Strategy S.p.A. considera l'Intelligenza Artificiale (AI) una leva strategica per l'innovazione, la qualità dei servizi professionali, la realizzazione di soluzioni tecnologiche e la Ricerca e Sviluppo. La Società ne promuove un impiego consapevole, affidabile, sicuro, trasparente e rispettoso delle persone, valorizzando i benefici per clienti, lavoratori, comunità e altri soggetti interessati.

La Direzione riconosce il principio AI con ESG by Design quale indirizzo distintivo della propria traiettoria tecnologica. La sostenibilità è considerata fin dalla concezione delle soluzioni e non soltanto come verifica successiva: l'AI è impiegata per generare valore ambientale, sociale ed economico (*AI for Sustainability*), mentre sono governati gli impatti ambientali, sociali e di governance della tecnologia stessa (*Sustainability of AI*).

Con la presente Politica la Direzione stabilisce i principi e gli impegni che orientano lo sviluppo, la fornitura e l'utilizzo di sistemi AI. Soft Strategy adotta un Artificial Intelligence Management System (AIMS) conforme alla propria organizzazione e coerente con la ISO/IEC 42001, finalizzato a governare rischi e opportunità, definire responsabilità, misurare l'efficacia dei controlli e sostenere il miglioramento continuo.

La governance dell'AI opera in raccordo con i Sistemi di Gestione e i presidi aziendali applicabili, in particolare quelli relativi a qualità, sicurezza delle informazioni, Data Protection, Modello 231, proprietà intellettuale, approvvigionamenti, risorse umane e sostenibilità. Le competenze e gli ambiti di responsabilità di ciascuna funzione restano definiti dai rispettivi assetti organizzativi.

La Politica si applica a Soft Strategy S.p.A., alle sedi operative di Roma – Via Cristoforo Colombo 115 e Valenzano – Strada Provinciale per Casamassima km 3, c/o Technopolis, 70010 Valenzano (BA), a tutte le Business Unit, all'AI Center e alle altre strutture che sviluppano, forniscono, integrano, acquisiscono, utilizzano o sperimentano AI. Si rivolge ad amministratori, dirigenti, dipendenti, collaboratori e soggetti terzi che operano per conto della Società, nei limiti dei rapporti e delle autorizzazioni applicabili.

Sono comprese le attività svolte nei processi interni, nei servizi professionali e nelle commesse cliente, nei prodotti e nelle soluzioni proprietarie o ibride, nonché nelle attività di ricerca industriale, sviluppo sperimentale, laboratorio, proof of concept (PoC), pilot, produzione, manutenzione e dismissione. Il campo comprende sistemi AI realizzati internamente, componenti open source e sistemi, modelli, API, piattaforme e servizi di terze parti, inclusi strumenti integrati in applicazioni già in uso.

L'AIMS si riferisce alla sola Soft Strategy S.p.A. Le funzioni centralizzate di Soft Strategy Group e delle altre società coinvolte nei processi di supporto operano come interfacce organizzative secondo responsabilità e accordi applicabili, senza che ciò determini l'estensione automatica del perimetro di certificazione.

Soft Strategy opera attraverso tre profili funzionali, anche cumulabili nello stesso progetto: User, quando utilizza sistemi o servizi AI; Developer, quando progetta, sviluppa, configura, integra o fornisce soluzioni AI proprie o commissionate; Researcher, quando conduce attività scientifiche, industriali o sperimentali sull'AI. Le denominazioni identificano regimi interni di governo e non sostituiscono la qualificazione giuridica dei ruoli prevista dalla normativa applicabile.

I principi della presente Politica sono comuni e inderogabili. Le disposizioni delle Parti II, III e IV definiscono, invece, obblighi, autorizzazioni, verifiche ed evidenze proporzionati al profilo, alla finalità, alla fase del ciclo di vita e al livello di rischio. Quando più profili si sovrappongono, si applicano cumulativamente le disposizioni pertinenti; in caso di requisiti differenti prevale quello maggiormente protettivo o più specifico per il contesto.

2. Principi etici e AI con ESG by Design

Soft Strategy assume i principi di legalità, tutela della persona e responsabilità professionale come riferimento permanente per tutte le attività AI. Il loro concreto esercizio è commisurato alla finalità e al rischio, mentre le garanzie fondamentali sono comuni ai tre profili. L'AI deve assistere le capacità delle persone, favorire decisioni informate e generare risultati controllabili, senza indebolire diritti, doveri professionali o presidi di governance.

- **Responsabilità, legalità e supervisione umana.** Ogni iniziativa ha un owner identificabile, rispetta gli obblighi normativi e contrattuali e dispone dei meccanismi di intervento umano appropriati. Non è consentito delegare integralmente al sistema la responsabilità di decisioni aziendali rilevanti o utilizzare l'AI per attribuire falsamente attività, dichiarazioni o evidenze.
- **Equità, inclusione e comprensibilità.** Sono valutati i rischi di bias, discriminazione e esclusione; le informazioni sul ruolo dell'AI, sulle limitazioni e sulle modalità di contestazione sono proporzionate ai destinatari e alle possibili conseguenze. Si considerano accessibilità, dignità del lavoro e bisogni di persone vulnerabili.
- **Affidabilità, protezione e sicurezza.** I dati, i modelli e gli output sono soggetti a verifiche proporzionate per accuratezza, robustezza e aggiornamento. Si tutelano privacy, informazioni riservate, proprietà intellettuale e integrità dei sistemi, prevenendo accessi abusivi, alterazioni, data leakage e vulnerabilità specifiche dell'AI.
- **Innovazione e integrità scientifica.** Ricerca e sviluppo sono favoriti in condizioni che consentano sperimentazione, verifica delle ipotesi, documentazione dei limiti e trattamento corretto dei risultati, inclusi esiti negativi. La libertà scientifica è esercitata nel rispetto delle persone, dei dati e degli accordi applicabili.
- **Sostenibilità e verificabilità.** Il valore economico è perseguito insieme all'efficienza delle risorse, alla qualità del lavoro, agli effetti su ambiente e comunità. Indicatori, calcoli GHG e dichiarazioni ESG devono essere riconducibili a dati, fonti, metodologie e validazioni adeguati, senza confondere stime e benefici effettivamente conseguiti.

Soft Strategy applica l'AI con ESG by Design come criterio di orientamento delle decisioni di investimento, selezione tecnologica, sviluppo, utilizzo e sperimentazione. L'analisi considera congiuntamente il valore generato dal sistema AI e gli impatti connessi alla sua realizzazione e al suo esercizio. Il contributo economico, l'efficienza operativa, la qualità del servizio e i risultati ambientali e sociali sono pertanto valutati come dimensioni complementari, senza assumere che il miglioramento di una compensi automaticamente il peggioramento di un'altra.

La Società considera, in modo proporzionato al caso d'uso, una duplice prospettiva: inside-out, relativa agli effetti delle decisioni tecnologiche su persone, comunità e ambiente; outside-in, relativa ai rischi e alle opportunità che aspettative degli stakeholder, disponibilità di risorse, evoluzione normativa e contesto sociale ed economico generano per la Società e i clienti. Tale prospettiva orienta il governo degli impatti AI e si raccorda, ove pertinente, con le analisi ESG dell'organizzazione, senza sostituire le metodologie e gli obblighi specifici di rendicontazione di sostenibilità.

Sul piano ambientale, nella valutazione di nuove soluzioni e nelle revisioni significative devono essere considerate l'idoneità funzionale e la proporzionalità delle risorse utilizzate: dimensione dei modelli, architetture specializzate, RAG, caching, esigenze di training e inferenza, ubicazione dell'elaborazione, infrastruttura, traffico dati, efficienza energetica, longevità e dismissione delle risorse hardware. Modelli compatti o elaborazione on-premise non sono considerati automaticamente più sostenibili: sono preferiti quando adeguati ai requisiti e sostenuti da confronti o evidenze tecniche attendibili.

Sul piano sociale, l'AI deve sostenere la capacità delle persone di comprendere, decidere, apprendere e lavorare con qualità. Si promuovono accessibilità, inclusione, formazione, attenzione agli utenti vulnerabili, disponibilità di alternative appropriate e strumenti di intervento umano. Nei processi lavorativi vengono considerati il possibile aumento della pressione produttiva, la redistribuzione dei compiti, il rischio di dipendenza dall'automazione e le opportunità di qualificazione delle competenze.

Sul piano della governance, l'AIMS favorisce sistemi verificabili e controllabili: responsabilità definite, fonti e dati tracciabili, modelli e versioni identificabili, test e limiti documentati, meccanismi di explainability e guardrail adeguati, gestione dei fornitori e trasparenza delle interazioni con stakeholder e clienti. Le dichiarazioni sui benefici ESG delle soluzioni sono formulate sulla base di indicatori, confronti e risultati effettivamente verificabili.

Questi impegni si applicano anche quando un sistema AI è concepito per finalità di sostenibilità, quali gestione delle emissioni GHG, rendicontazione ambientale, ottimizzazione dei servizi, efficienza delle risorse o accessibilità: la finalità positiva non esonera da valutazioni sulla qualità dei dati, sulla correttezza del calcolo e sugli effetti indesiderati.

3. Governance, responsabilità e competenze decisionali

L'Amministratore Delegato di Soft Strategy S.p.A., Emanuele Hermes Candela, nel quadro dei poteri societari vigenti, assume la responsabilità ultima dell'efficacia dell'AIMS, ne approva gli indirizzi fondamentali, assicura risorse adeguate e promuove la diffusione della presente Politica.

Il Responsabile AI di Gruppo / AI Center Director (Emanuele Donati) è owner della Politica e referente di coordinamento dell'AIMS. Definisce indirizzi metodologici, promuove la classificazione dei sistemi e dei relativi rischi, coordina la valutazione delle nuove iniziative e supporta le Business Unit nell'applicazione delle regole AI. L'esercizio di tale funzione di coordinamento non trasferisce a Soft Strategy Group la responsabilità ultima dell'AIMS della Società certificata.

I Direttori di Business Unit e i responsabili di progetto o commessa identificano i casi d'uso, ne verificano la coerenza con l'attività autorizzata, nominano i referenti operativi, assicurano l'applicazione delle misure e rendono disponibili le evidenze. Le funzioni IT/Information Security, Data Protection/RPD-DPO, Compliance/Legal, Acquisti/Procurement, HR, Sostenibilità/ESG, Ricerca e Sviluppo e Responsabile dei Sistemi di Gestione intervengono per i rispettivi ambiti e secondo l'organizzazione effettivamente vigente. Le responsabilità, le interfacce con funzioni Group e le autorità decisionali sono dettagliate nella documentazione AIMS applicabile.

Ogni sistema o iniziativa AI dispone di un owner individuato e di un referente per gli aspetti operativi. La responsabilità di una decisione aziendale non può essere delegata integralmente a un sistema AI.

L'assetto di responsabilità è reso operativo attraverso ruoli e deleghe, criteri di escalation, autorizzazioni e interfacce definite con le funzioni centralizzate di Gruppo. Nei progetti AI che coinvolgono più Business Unit, funzioni aziendali o società del Gruppo, la responsabilità delle decisioni e delle evidenze riferite a Soft Strategy S.p.A. resta identificabile e verificabile.

4. Sistemi e strumenti AI, dati, fornitori e autorizzazioni

La Società mantiene un registro dei sistemi e degli utilizzi AI rilevanti, comprendente strumenti di terze parti, iniziative interne, commesse, prodotti, PoC, pilot e attività di Ricerca e Sviluppo. Il registro distingue la titolarità della soluzione dalla provenienza dei modelli e componenti AI, identifica i ruoli svolti da Soft Strategy e consente di collegare owner, finalità, dati, fornitori, fase di vita, rischi, autorizzazioni, valutazioni effettuate e, quando pertinenti, impatti e indicatori ESG. Lo stato dei sistemi è aggiornato sulla base dell'effettiva operatività e dei rispettivi casi d'uso.

Soft Strategy assicura che i sistemi di Intelligenza Artificiale siano progettati, sviluppati, utilizzati e mantenuti attraverso risorse tecnologiche, informative e professionali adeguate alle rispettive finalità e ai rischi associati. A tal fine, la Società promuove l'identificazione e la tracciabilità delle principali risorse e dipendenze, comprendenti dati, modelli, strumenti, infrastrutture e competenze umane, verificandone nel tempo disponibilità, affidabilità e idoneità. Particolare attenzione è riservata alle dipendenze critiche da fornitori, tecnologie e competenze specialistiche, nonché alla capacità delle infrastrutture di sostenere le prestazioni richieste in condizioni di sicurezza, continuità operativa ed efficienza delle risorse, coerentemente con i principi di AI con ESG by Design.

L'inclusione in un censimento, il possesso di una licenza, la disponibilità di una funzionalità o la presenza di uno strumento in un ambiente cliente non costituiscono di per sé autorizzazione al suo utilizzo per ogni finalità o classe di dati. La Società definisce un catalogo controllato degli strumenti e servizi approvati, specificando, ove pertinente, tipologia di account, configurazione, utenti abilitati, funzionalità consentite, categorie di dati e condizioni d'uso.

L'acquisizione o attivazione di nuovi strumenti, modelli, API, connettori e funzionalità agentiche avviene con valutazione preventiva proporzionata, coordinata dal Responsabile AI e dalle funzioni competenti; per nuove iniziative progettuali il Direttore della BU interessata assicura la verifica dell'esigenza e dell'appropriatezza. Le modalità operative di approvazione, registrazione e gestione delle eccezioni sono definite nei processi AIMS e di approvvigionamento applicabili.

Gli strumenti e gli utilizzi attivi sono sottoposti a verifica periodica della loro ammissibilità e delle condizioni di impiego, con priorità ai servizi accessibili tramite account personali, al trattamento di dati riservati e alle integrazioni capaci di accedere o operare su ambienti aziendali. L'esito delle verifiche determina, secondo il caso, conferma, adeguamento, limitazione o revoca dell'autorizzazione.

Nella selezione e gestione di servizi e componenti AI di terzi, Soft Strategy valuta, per quanto pertinente, condizioni contrattuali, garanzie di sicurezza e privacy, subfornitori, localizzazione e trasferimento dei dati, finalità di trattamento, conservazione, riutilizzo degli input e degli output per addestramento, diritti di proprietà intellettuale, disponibilità, modifiche del servizio, auditabilità, continuità ed exit strategy. Sono inoltre valutate, quando rilevanti e documentabili, informazioni disponibili sui consumi, sulla localizzazione dell'elaborazione, sulle caratteristiche infrastrutturali e sugli impegni ambientali del provider, senza assumere equivalenza fra localizzazione del servizio, sovranità del dato e sostenibilità ambientale.

Per sistemi AI collegati ad ambienti interni o dei clienti si applicano adeguati controlli di accesso, segregazione, configurazione, logging e change management. Connettori, accesso ai repository, comandi sul sistema, utilizzo di terminali e agenti capaci di leggere, modificare, inviare o cancellare contenuti richiedono autorizzazione specifica e limitazione dei privilegi, con supervisione umana delle azioni critiche.

L'autorizzazione del provider non esaurisce la responsabilità sui dati e sugli utilizzi consentiti. Le verifiche contrattuali, di sicurezza, Data Protection e proprietà intellettuale devono riguardare la configurazione effettiva e il caso d'uso: si presta particolare attenzione all'impiego degli input per addestramento, alle modalità di conservazione e cancellazione, alla segregazione delle informazioni di clienti diversi e all'evoluzione delle condizioni del servizio.

5. Rischi, obblighi normativi e prevenzione degli illeciti

Ogni iniziativa AI è assoggettata, prima dell'uso o del rilascio appropriato alla sua natura, a uno screening che considera finalità, ruolo di Soft Strategy, utenti, dati, modello e provider, autonomia, accessi, popolazione interessata, impatti e obblighi applicabili, comprese le possibili ricadute ambientali e sociali della soluzione e le dipendenze dalla filiera tecnologica. In relazione agli esiti si svolgono l'AI Risk Assessment e, quando pertinente, l'AI Impact Assessment, secondo metodologie proprie dell'AIMS e raccordate ai processi aziendali esistenti.

Ricevono attenzione rafforzata, fra gli altri, sistemi relativi a selezione e gestione delle persone, scoring, biometria, dati sanitari e categorie particolari di dati, minori, analisi di immagini e video, servizi pubblici, infrastrutture critiche e decisioni suscettibili di effetti significativi sulle persone. La classificazione interna del rischio non coincide automaticamente con la classificazione giuridica ai fini dell'AI Act, che viene esaminata separatamente quando applicabile.

La componente Data Protection comprende, ove necessario, l'analisi di ruoli privacy, basi giuridiche, finalità, minimizzazione, categorie di interessati, conservazione, trasferimenti internazionali, accordi con responsabili e DPIA ai sensi dell'art. 35 GDPR. Una verifica privacy positiva non sostituisce la valutazione dei rischi AI; le due

analisi sono coordinate e reciprocamente richiamate. Sono inoltre gestite le prescrizioni del Modello 231 e degli altri presidi pertinenti.

La Società non ammette pratiche AI vietate dalla normativa applicabile. L'impiego di sistemi soggetti a requisiti normativi specifici, inclusi quelli eventualmente classificati ad alto rischio, è subordinato alla verifica dei relativi obblighi e al coinvolgimento delle funzioni competenti.

La Società definisce criteri per l'accettazione dei rischi residui, il trattamento, le eccezioni autorizzate, le responsabilità e il riesame al verificarsi di modifiche significative. Le valutazioni AI e quelle privacy, di sicurezza, contrattuali ed ESG possono essere raccolte in un quadro coordinato, mantenendo riconoscibili finalità, metodologie, responsabilità e basi normative di ciascuna componente.

Per sistemi che producono indicatori di sostenibilità, emissioni, valutazioni sociali o altre informazioni oggetto di rendicontazione, la valutazione comprende inoltre il rischio di errore metodologico, classificazioni improprie, informazioni incomplete, fattori di conversione non aggiornati, fonti non verificabili e dichiarazioni potenzialmente fuorvianti.

Ai fini dell'AI Act sono identificati, secondo il ruolo concretamente svolto dalla Società, gli obblighi relativi alle pratiche vietate, alle categorie di sistemi soggette a prescrizioni specifiche, alla trasparenza dei sistemi e dei contenuti sintetici e alle responsabilità dei soggetti della catena del valore. L'applicazione di requisiti e tempi è verificata sulla base della disciplina vigente; gli adempimenti propri del GDPR, del diritto del lavoro, della tutela della proprietà intellettuale e delle altre normative pertinenti conservano autonoma rilevanza.

La Società orienta i propri presidi di prevenzione anche ai rischi penali connessi a realizzazione, alterazione e impiego illecito di sistemi AI. Con riferimento al D.Lgs. 9 settembre 2026, n. 160, sono considerate in particolare le fattispecie dell'art. 437-bis c.p., relative a omissioni di misure di sicurezza o sorveglianza umana e ad alterazioni illecite nei sistemi di AI ad alto rischio nei presupposti previsti dalla legge, e dell'art. 612-quater c.p., relativo alla diffusione illecita di contenuti generati o manipolati artificialmente. La valutazione del rischio è raccordata al Modello 231 anche in relazione al nuovo art. 25-vicies del D.Lgs. 231/2001, alle competenze delle funzioni di controllo e ai canali aziendali di segnalazione.

La prevenzione degli illeciti costituisce un impegno trasversale, che si traduce in controlli effettivi e proporzionati su autorizzazioni, accessi, integrità di dati e sistemi, gestione delle modifiche, tracciabilità e supervisione umana. È vietato eludere intenzionalmente tali controlli, realizzare impersonificazioni ingannevoli o utilizzare strumenti AI per falsificare documentazione, risultanze tecniche o comunicazioni professionali.

6. Ciclo di vita, supervisione, monitoraggio e incidenti

Le iniziative AI sono governate lungo il ciclo di vita, dall'ideazione alla dismissione. Requisiti, controlli e verifiche sono differenziati tra uso standard, sviluppo, laboratorio, PoC, pilot e produzione. In particolare, il passaggio a un impiego operativo o a una consegna al cliente richiede una verifica documentata dei requisiti, del rischio residuo, delle prestazioni, della supervisione, delle responsabilità di esercizio e degli impatti ambientali e sociali rilevanti. L'esercizio, la cessazione di singole funzionalità e la dismissione complessiva sono registrati in modo coerente con gli effettivi impieghi.

Sono presidiati modifiche dei modelli e dei provider, nuove versioni, degrado delle prestazioni, feedback, accessi anomali, errori significativi, output dannosi, compromissioni di dati e incidenti riconducibili all'AI. Le segnalazioni confluiscono nei processi aziendali competenti per sicurezza, Data Protection e gestione degli incidenti, con un raccordo specifico per gli eventi AI e i relativi impatti.

La supervisione umana deve risultare effettiva e coerente con la capacità di incidere sui risultati o sulle azioni del sistema. Ove necessario, sono previsti strumenti per interpretare gli esiti, contestarli, correggerli, sospendere l'esecuzione e intervenire tempestivamente nei processi automatizzati. Per i sistemi capaci di operare mediante

strumenti, API o accessi privilegiati, tali misure comprendono restrizioni dei permessi e conferme sulle operazioni critiche.

Segnalazioni, errori gravi, vulnerabilità, comportamenti imprevisti e possibili violazioni sono esaminati dal responsabile del sistema con le funzioni interessate. Gli eventi che comportano impatti su persone, clienti, informazioni, disponibilità dei servizi o diritti dei terzi determinano, secondo necessità, contenimento, ripristino, comunicazione, rivalutazione del rischio e miglioramento dei controlli. La gestione degli incidenti AI è coordinata con i processi di sicurezza delle informazioni, Data Protection e responsabilità contrattuale.

7. Formazione, competenze e AI Literacy

Soft Strategy considera la conoscenza dei sistemi AI e dei loro limiti parte essenziale della professionalità, della qualità dei servizi e della protezione delle persone. In coerenza con l'articolo 4 dell'AI Act e con i requisiti di competenza e consapevolezza della ISO/IEC 42001, la Società adotta misure di alfabetizzazione e sviluppo delle competenze adeguate ai ruoli, alle conoscenze iniziali, agli strumenti impiegati, al contesto operativo e ai possibili effetti sui destinatari dei sistemi.

La funzione HR, in coordinamento con l'AI Center, i responsabili delle Business Unit e le funzioni di controllo competenti, promuove un piano periodico di informazione, formazione e aggiornamento. Il piano individua i destinatari, gli obiettivi formativi, i contenuti essenziali e le modalità di verifica dell'apprendimento o dell'effettiva applicazione delle conoscenze. Sono conservate evidenze adeguate delle iniziative realizzate, delle partecipazioni e delle esigenze di aggiornamento emerse.

I percorsi sono modulati rispetto ai profili operativi. Gli utilizzatori acquisiscono consapevolezza di limiti, errori, allucinazioni, trattamento dei dati, riservatezza, diritti sugli output, supervisione e segnalazioni. I Developer approfondiscono progettazione responsabile, gestione dei rischi, qualità dei dataset, prove di validazione, cybersecurity, trasparenza, requisiti normativi ed ESG by Design. I Researcher sviluppano competenze su integrità scientifica, gestione dei dati sperimentali, riproducibilità, valutazione critica di modelli e impatti, rischi emergenti e condizioni per il trasferimento alla produzione.

I responsabili di commessa, i manager e le funzioni di controllo ricevono inoltre una formazione coerente con le rispettive responsabilità di autorizzazione, sorveglianza e assunzione delle decisioni. La necessità di aggiornamento è rivalutata quando cambiano modelli, fornitori, funzionalità, processi, prescrizioni normative o livelli di rischio. L'efficacia del percorso non è misurata esclusivamente sulla frequenza ai corsi, ma anche sulla capacità di adottare correttamente i presidi richiesti nelle attività reali.

8. Valutazione delle prestazioni, documentazione e miglioramento

Il funzionamento dell'AIMS è sottoposto a obiettivi misurabili, monitoraggi, audit interni, gestione delle non conformità, azioni correttive e riesame della Direzione. Gli indicatori possono comprendere, secondo rilevanza e disponibilità dei dati, tasso di adozione e di formazione, qualità e affidabilità delle risposte, tempi di servizio, incidenti e reclami, copertura della documentazione e dei test, consumi o indicatori di efficienza delle inferenze, impatti sulla qualità del lavoro e soddisfazione degli utenti. Le misure sono accompagnate da perimetro, unità, fonte, responsabile e criteri di confronto, evitando confronti tra architetture o contesti non omogenei. La presente Politica viene riesaminata periodicamente e in occasione di cambiamenti normativi, organizzativi, tecnologici o di rischio rilevanti; la verifica della sua efficacia è svolta attraverso evidenze documentate e risultati operativi.

La Direzione, con il supporto del Responsabile AI e delle funzioni interessate, valuta periodicamente l'adeguatezza e l'efficacia dell'AIMS, tenendo conto dei risultati dei monitoraggi, delle verifiche sul rispetto della Politica, della copertura delle valutazioni di rischio, del livello di competenza del personale e delle esigenze espresse da clienti e parti interessate. I risultati confluiscono nei processi di audit, riesame e miglioramento continuo applicabili al sistema AI.

PARTE II — POLITICA AI PER IL PROFILO USER

9. Strumenti, account e informazioni trattabili

La Politica User disciplina l'impiego di sistemi, funzionalità e servizi AI di terzi nelle attività professionali di Soft Strategy, indipendentemente dalla Business Unit o dalla modalità di accesso. Si applica a chatbot, assistenti di produttività, ricerca e sintesi documentale, strumenti di trascrizione, generazione di contenuti e immagini, assistenti allo sviluppo software, applicazioni AI integrate e servizi agentici. Si applica altresì ai sistemi AI sviluppati da Soft Strategy quando utilizzati internamente come strumenti di lavoro.

L'utilizzatore mantiene la responsabilità della correttezza dell'uso e degli esiti destinati a colleghi, clienti, partner e terzi. L'AI non sostituisce il giudizio professionale, le verifiche richieste dalla commessa, le approvazioni gerarchiche e i controlli aziendali.

Per attività aziendali possono essere utilizzati esclusivamente strumenti e funzionalità autorizzati per lo specifico utilizzo, attraverso account, tenant e ambienti conformi alle condizioni stabilite dalla Società o dal cliente. L'uso lavorativo di account AI personali è vietato, salvo eccezioni motivate e autorizzate per iscritto dalle funzioni competenti, con indicazione di finalità, dati ammessi, durata e misure compensative. L'acquisto individuale di una licenza non costituisce autorizzazione.

L'abilitazione all'uso di un prodotto non implica l'abilitazione automatica a tutte le sue funzioni, estensioni, plug-in, connettori, integrazioni, modalità di condivisione o agenti. L'utente non può attivare autonomamente collegamenti a posta elettronica, calendari, repository, sistemi di ticketing, CRM, database o archivi aziendali e di commessa quando ciò non sia stato preventivamente approvato.

La gestione delle credenziali, degli accessi, delle autorizzazioni e della revoca delle utenze segue i controlli aziendali di sicurezza e i vincoli dei sistemi dei clienti.

L'inserimento di contenuti in uno strumento AI deve rispettare il principio di necessità, la classificazione delle informazioni, la titolarità dei diritti e le condizioni dell'ambiente autorizzato. Non è sufficiente che il servizio sia considerato sicuro o disponibile con licenza aziendale: la legittimità del trattamento deve essere verificata anche rispetto a cliente, contratto, informazione e finalità.

La scelta del tipo di informazione da sottoporre al sistema è parte integrante della valutazione dell'utilizzatore e deve rispettare le condizioni di autorizzazione. In particolare si applicano i seguenti criteri:

- **Contenuti pubblici o divulgabili:** possono essere trattati negli strumenti autorizzati, fermo il controllo su attendibilità, diritti d'uso e finalità.
- **Informazioni interne:** sono utilizzabili solo negli strumenti e nelle configurazioni aziendali ammesse per tale categoria, evitando trasferimenti non necessari.
- **Documenti, codice, dati e proprietà intellettuale di Soft Strategy, clienti o terzi:** richiedono specifica compatibilità con le autorizzazioni, i contratti, le licenze, la Policy IP e le condizioni del fornitore AI; devono essere protetti da usi ulteriori non autorizzati, inclusi addestramento e condivisione.
- **Dati personali:** possono essere trattati soltanto nell'ambito di finalità e strumenti autorizzati, nel rispetto delle regole Data Protection. Dati particolari, giudiziari o relativi a persone vulnerabili richiedono una valutazione specifica prima dell'inserimento.
- **Credenziali, segreti, chiavi, token e dati di autenticazione:** non devono essere immessi nei prompt o nei file trasmessi a servizi AI, salvo specifica soluzione tecnica aziendale formalmente autorizzata e protetta.

Laddove il risultato sia ottenibile con dati aggregati, anonimizzati, pseudonimizzati o sintetici, è preferibile utilizzare tali modalità in coerenza con le regole applicabili. Copiare informazioni da un ambiente del cliente a un servizio AI esterno non è consentito in mancanza del diritto e dell'autorizzazione necessari.

Le regole valgono per strumenti autonomi e per funzionalità AI incorporate in software già autorizzato: un nuovo connettore, una funzione agentica, una modalità di condivisione o un cambiamento del provider possono modificare l'esposizione dei dati e richiedere una valutazione aggiuntiva prima dell'attivazione.

10. Controllo degli output, trasparenza e impieghi sensibili

L'utente valuta criticamente la pertinenza, la completezza e l'attendibilità delle risposte e ne verifica fonti, citazioni, calcoli, riferimenti normativi, codice e dati quando il risultato è destinato a decisioni, atti, offerte o deliverable. Gli output generati con AI non sono automaticamente considerati corretti, originali o liberamente riutilizzabili.

Per attività che comportano decisioni legali, economiche, tecniche, professionali, organizzative o che incidono sulle persone, la revisione umana deve essere effettuata da soggetti competenti e secondo le autorizzazioni previste. La presenza di contenuti generati o elaborati con AI è comunicata quando richiesto da legge, contratto, istruzioni del cliente o dalla natura del rapporto con i destinatari.

L'utente non presenta come effettivamente svolte attività, verifiche, analisi di fonti o controlli che non siano stati eseguiti; non utilizza risultati AI per falsificare evidenze o attribuire a terzi dichiarazioni inesistenti.

Gli strumenti AI che operano su file locali, repository, IDE, terminali, browser, posta o piattaforme collegate devono essere utilizzati con privilegi minimi e nei soli ambienti consentiti. Le azioni capaci di pubblicare, modificare o cancellare informazioni, inviare messaggi, installare pacchetti, eseguire comandi o modificare configurazioni richiedono controllo umano e autorizzazioni proporzionate; non si attivano modalità di esecuzione autonoma non espressamente ammesse.

Il codice generato o modificato con assistenti AI è assoggettato a code review, test, analisi di sicurezza e controlli di licenza previsti dal processo di sviluppo. L'uso di strumenti AI per registrazioni, trascrizioni, sintesi di riunioni o trattamento di voce, immagini e video presuppone la verifica degli obblighi di informazione, delle basi giuridiche e delle autorizzazioni applicabili, senza attivazioni occulte o trattamenti eccedenti la finalità autorizzata.

Chi utilizza strumenti AI è tenuto a considerare non soltanto la rapidità di produzione degli output, ma anche la loro reale utilità, verificabilità e il possibile impatto sulle persone e sulle risorse. L'adozione dell'AI deve contribuire alla qualità del lavoro, non moltiplicare elaborazioni superflue, comunicazioni non verificate o decisioni non comprensibili.

L'utilizzatore privilegia modalità proporzionate allo scopo, evita impieghi computazionalmente onerosi privi di utilità riconoscibile e non attribuisce a un sistema capacità, certificazioni, risparmi energetici o benefici sociali non dimostrati. Quando gli output supportano report ESG, valutazioni GHG, questionari ambientali o comunicazioni verso stakeholder, verifica fonti, dati di base, unità di misura, assunzioni, formule e congruenza delle affermazioni prima dell'approvazione o della diffusione.

Nei servizi rivolti a utenti o cittadini, chi utilizza l'AI considera la comprensibilità delle risposte, l'accessibilità delle interfacce, eventuali barriere linguistiche e digitali e la necessità di coinvolgere operatori competenti nei casi in cui l'automazione non garantisca una tutela adeguata delle persone.

L'uso di AI per screening o valutazione di candidati, gestione o scoring del personale, inferenze su caratteristiche sensibili, sorveglianza, decisioni rilevanti o altri trattamenti potenzialmente critici non può essere avviato sulla sola iniziativa dell'utilizzatore: richiede un processo di valutazione e autorizzazione specifico, con coinvolgimento delle funzioni HR, Legal, AI e Data Protection, secondo il caso.

Gli utenti segnalano utilizzi non autorizzati, divulgazione di contenuti, output gravemente inesatti o pregiudizievoli, anomalie e incidenti tramite i canali aziendali. Ciascun utente partecipa alle iniziative di formazione previste e si mantiene aggiornato sulle istruzioni relative agli strumenti che impiega.

Quando si impiegano interfacce conversazionali o si diffondono immagini, voci, video o altri contenuti generati o manipolati mediante AI, l'utilizzatore rispetta gli obblighi di trasparenza e informazione applicabili al caso, inclusi quelli stabiliti dall'articolo 50 dell'AI Act. È in ogni caso vietato realizzare, diffondere o avallare contenuti ingannevoli o illeciti che possano ledere identità, reputazione, diritti o sicurezza delle persone.

PARTE III — POLITICA AI PER IL PROFILO DEVELOPER

11. Progettazione responsabile ed ESG by Design

La Politica Developer disciplina la progettazione, lo sviluppo, la personalizzazione, la configurazione, l'integrazione, il collaudo, la fornitura e la manutenzione di sistemi e soluzioni AI per uso interno, per il mercato o per specifici clienti. Si applica tanto ai sistemi proprietari quanto alle soluzioni ibride costruite su modelli, librerie, API, framework o servizi di terzi, incluso il fine-tuning, la costruzione di sistemi RAG e la progettazione di agenti.

Per ogni iniziativa sono chiariti ruolo effettivo di Soft Strategy, responsabilità rispetto al cliente e ai fornitori, assetti contrattuali, proprietario della soluzione e titolarità dei modelli o componenti utilizzati. Le qualificazioni rilevanti ai sensi dell'AI Act sono effettuate caso per caso, senza presumerle dalla sola denominazione del progetto o dall'uso di modelli di terzi.

La governance dei sistemi AI è integrata nella gestione di progetto e nel ciclo di vita del software. Nella definizione dei requisiti sono valutati finalità, benefici attesi, utenti, contesto d'uso, qualità e provenienza dei dati, requisiti contrattuali, rischi, supervisione umana, prestazioni attese, limiti del sistema e condizioni di dismissione.

Il responsabile della commessa, con il supporto dell'AI Center e delle funzioni competenti, assicura la presenza di un owner del sistema, di ruoli di verifica e approvazione, nonché delle informazioni necessarie al Registro AI. Per le soluzioni realizzate su specifica del cliente, la ripartizione delle responsabilità di sviluppo, fornitura, uso, monitoraggio e trattamento dei dati viene documentata contrattualmente e operativamente.

I team di sviluppo considerano gli obiettivi ESG pertinenti insieme ai requisiti funzionali e non funzionali, valutando già in fase di progettazione il valore atteso, le popolazioni potenzialmente interessate, l'accessibilità, il contributo alla qualità del lavoro e le conseguenze ambientali dell'architettura proposta.

La scelta tra modelli general-purpose, modelli compatti e verticali, componenti locali, infrastrutture del cliente, cloud e configurazioni ibride deve essere motivata in funzione di accuratezza e robustezza richieste, qualità dell'esperienza, riservatezza, disponibilità, costi complessivi e utilizzo delle risorse. L'orientamento verso modelli efficienti e infrastrutture controllabili costituisce una preferenza progettuale, non un requisito tecnologico assoluto né prova sufficiente di minore impatto ambientale.

Quando il caso d'uso lo richiede, sono definiti criteri di confronto ragionevoli — ad esempio qualità delle risposte rispetto a una baseline, latenza, throughput, consumo energetico per unità di lavoro comparabile e costi di esercizio — e sono documentate le assunzioni adottate. La raccolta di metriche non deve diventare un adempimento sproporzionato per componenti sperimentali o sistemi a rischio trascurabile, ma deve sostenere decisioni tecniche e rendicontazioni attendibili.

Nei sistemi che producono indicatori economici o ESG, la progettazione deve consentire, per quanto pertinente, di ricostruire il percorso fonte → dato → trasformazione → fattore/metodologia → calcolo → output → validazione. Le funzioni generative non sostituiscono le regole di calcolo deterministiche quando necessarie per garantire ripetibilità, verificabilità e coerenza metodologica. Testi e sintesi possono assistere gli operatori, ma i valori destinati a rendicontazione devono essere controllati in base alle responsabilità definite.

La progettazione considera inoltre inclusione e non discriminazione, feedback e contestazione degli esiti, conservazione di canali umani appropriati, autonomia e formazione degli operatori, rischio di aumento del carico cognitivo e condizioni nelle quali la soluzione deve trasferire il controllo a una persona.

Dataset e fonti informative sono selezionati e gestiti in funzione della legittimità d'uso, qualità, rappresentatività, provenienza, appropriatezza rispetto allo scopo e protezione delle informazioni. L'impiego di dati di clienti o terzi per training, fine-tuning, embeddings, indicizzazione e knowledge base deve risultare compatibile con finalità, titoli d'uso, contratti e istruzioni ricevute, senza presumere che la mera disponibilità dei dati ne autorizzi il riutilizzo.

La scelta di modelli, API, piattaforme, componenti open source e servizi esterni tiene conto di sicurezza, condizioni di licenza, compatibilità con i diritti sugli output, qualità, costi, resilienza, dipendenza dal provider, conservazione dei dati e possibilità di sostituzione. Sono registrate le versioni rilevanti dei modelli e dei componenti e sono controllati i cambiamenti capaci di modificare rischi o prestazioni.

Per i sistemi RAG si presidiano selezione, autorizzazione, segregazione e aggiornamento delle fonti, controllo degli accessi, qualità del recupero e rischio di risposta non fondata. Per i sistemi agentici sono stabiliti limiti di autonomia, strumenti accessibili, permessi, controlli sulle azioni esterne, verifiche di output e meccanismi di arresto o ripristino.

Nella progettazione dei sistemi AI sono integrati, secondo rischio e destinazione d'uso, requisiti di accessibilità, contestabilità degli esiti, tracciabilità delle decisioni, interoperabilità e riduzione delle dipendenze tecnologiche non necessarie. Lo sviluppo di applicazioni mediante modelli o servizi esterni non attenua gli obblighi che derivano a Soft Strategy dalle attività di personalizzazione, integrazione o fornitura e dal ruolo effettivamente assunto nel rapporto con il cliente.

12. Validazione, fornitura e presidio operativo delle soluzioni

Il rilascio di una soluzione AI avviene a fronte di criteri di accettazione proporzionati al rischio e al contesto, inclusi gli obiettivi di sostenibilità e qualità del servizio esplicitamente assunti nella progettazione. Tali criteri considerano, quando pertinenti, accuratezza, robustezza, allucinazioni, bias, explainability, sicurezza applicativa, privacy, tempi di risposta, tracciabilità, resilienza, monitoraggio e supervisione umana.

Le verifiche comprendono test rappresentativi degli scenari di impiego previsti, condizioni di errore e uso improprio, nonché limiti del sistema. Per applicazioni a impatto sociale rilevante sono considerate accessibilità, comportamento su gruppi e contesti differenti, possibilità di errore sistematico e ricadute sull'operatore e sull'utente finale. Per modelli generativi e agentici sono valutati, secondo il contesto, prompt injection, data leakage, uso non consentito di strumenti, affidabilità delle fonti, esecuzione di azioni e gestione delle autorizzazioni. I risultati delle verifiche, le limitazioni note e i rischi residui sono documentati con un livello di dettaglio idoneo alla decisione di rilascio.

Il passaggio in produzione o la consegna al cliente richiede una decisione riconoscibile e attribuita, con identificazione di responsabilità operative, eventuali limitazioni d'uso, istruzioni, modalità di segnalazione e condizioni di modifica o sospensione. Non è sufficiente il successo tecnico di una PoC quale evidenza di idoneità all'utilizzo produttivo.

La documentazione delle soluzioni AI descrive finalità, funzionamento essenziale, dipendenze, dati, limiti, prestazioni, modalità di supervisione e, quando rilevanti, elementi misurabili di sostenibilità ambientale e sociale in misura coerente con il destinatario e con gli obblighi applicabili. Le informazioni necessarie al cliente per utilizzare e governare il sistema sono rese disponibili secondo il contratto e la ripartizione delle responsabilità.

La Società tutela la propria Background IP, disciplina la Foreground IP e i diritti sui deliverable, identifica le componenti di terzi e verifica le condizioni di riuso, licenza, subfornitura, trasferibilità e handover nel rispetto della Policy IP aziendale. I vincoli contrattuali più restrittivi sono incorporati nelle istruzioni al team di progetto.

Quando Soft Strategy mantiene attività di esercizio o manutenzione, sono stabiliti controlli di monitoraggio, gestione dei cambiamenti, incidenti, aggiornamento dei modelli, regressioni, vulnerabilità, feedback ed eventuale ritiro della soluzione. In caso di cessazione delle responsabilità operative, vengono documentati consegna e confini del presidio residuo.

Quando il sistema ricade nel campo di applicazione di obblighi di trasparenza o delle disposizioni sui sistemi AI ad alto rischio, la documentazione di progettazione e collaudo comprende anche i requisiti normativi pertinenti, le informazioni da fornire agli utilizzatori e le misure di marcatura o comunicazione dei contenuti sintetici previste dalla legge. La valutazione verifica l'effettività delle misure di sorveglianza umana, sicurezza e integrità, anche alla luce delle specifiche disposizioni penali applicabili.

Durante le fasi di gestione e manutenzione, le modifiche di modelli, dati, prompt, fonti RAG, agenti o provider sono esaminate rispetto alle prestazioni, alla sicurezza, alla privacy e ai rischi già valutati. L'handover al cliente comprende la disponibilità delle informazioni necessarie alla corretta gestione del sistema, la definizione dei ruoli successivi alla consegna e le condizioni per l'eventuale aggiornamento, sospensione o dismissione.

PARTE IV — POLITICA AI PER IL PROFILO RESEARCHER

13. Governance delle sperimentazioni e integrità scientifica

La Politica Researcher disciplina le attività di ricerca industriale, sviluppo sperimentale, studio metodologico, addestramento e valutazione dei modelli, esplorazione di nuove architetture, proof of concept, dimostratori e pilot AI, condotti direttamente da Soft Strategy o nell'ambito di partenariati, università, organismi di ricerca e progetti finanziati.

La Società riconosce il valore della libertà di esplorazione scientifica e tecnologica, della riproducibilità, del confronto fra ipotesi e della possibilità di ottenere risultati non soddisfacenti o non confermativi. L'assenza di prestazioni mature non impedisce una sperimentazione legittima, purché le condizioni di ricerca siano proporzionate ai rischi e gli esiti non siano presentati come validati per impieghi non ancora autorizzati.

Il responsabile scientifico o di progetto identifica finalità, perimetro, componenti, dati, partner, ambienti sperimentali e criteri di passaggio alle fasi successive; coordina, quando necessario, le valutazioni con l'AI Center e le funzioni competenti.

Per le attività di R&S si applica una progressione di controlli basata sulla concreta esposizione al rischio, indipendentemente dalla denominazione utilizzata nella documentazione progettuale.

- **Ricerca e laboratorio controllato.** Esperimenti in ambienti segregati, senza coinvolgimento operativo di utenti reali e preferibilmente con dati sintetici o comunque legittimamente utilizzabili. È sufficiente una registrazione essenziale di owner, scopo, dati, modelli, provider, ambiente, vincoli e rischi principali, oltre ai controlli IT e Data Protection pertinenti.
- **PoC e pilot circoscritti.** Attività con dataset reali, interazioni limitate con utenti o integrazioni circoscritte richiedono screening dei rischi e degli impatti, autorizzazioni sui dati, criteri di prova, monitoraggio, responsabilità di supervisione e misure per arresto o contenimento.
- **Sperimentazione sul campo ad impatto elevato.** Attività che interessano persone, infrastrutture, contesti pubblici, sistemi cyber-fisici, dati sensibili o decisioni significative richiedono una valutazione rafforzata prima dell'avvio, con coinvolgimento di funzioni tecniche, sicurezza, Data Protection, Legal e altri soggetti competenti.

Le distinzioni interne di fase non sostituiscono la qualificazione giuridica delle attività di R&S, dei test in condizioni reali, della fornitura o della messa in servizio ai sensi delle disposizioni applicabili.

Le attività di ricerca sono documentate in modo sufficiente a ricostruire ipotesi, obiettivi, dati, impostazioni, versioni dei modelli, parametri significativi, prove, indicatori, risultati e limiti. Sono favoriti confronto con

baseline, separazione tra dati di sviluppo e di valutazione, controlli della riproducibilità, valutazione di errori, bias, incertezza, consumo di risorse e stabilità dei risultati quando pertinenti.

Non è consentito manipolare o rappresentare selettivamente i risultati al fine di dichiarare prestazioni non dimostrate, né attribuire ai modelli proprietà di accuratezza, sicurezza o conformità non supportate dai test svolti. La sperimentazione di modelli vulnerabili, non robusti o caratterizzati da bias è ammissibile come oggetto di analisi, ma resta confinata a condizioni controllate e non legittima automaticamente il loro utilizzo su persone o processi reali.

L'utilizzo di dataset proprietari, di clienti, partner, enti pubblici o terzi deve rispettare diritto d'uso, vincoli di progetto, licenze, riservatezza, Data Protection e condizioni per eventuali attività di training, fine-tuning o condivisione. Particolare attenzione è rivolta a video, audio, dati di localizzazione, informazioni di mobilità, immagini di persone, dati sanitari, minori e dati provenienti da sensori in contesti reali.

La disponibilità di dati per una ricerca non autorizza automaticamente il trasferimento verso servizi cloud o modelli esterni, la pubblicazione di dataset o il loro riutilizzo in progetti diversi. L'accesso ai sistemi sperimentali è limitato alle persone e ai partner autorizzati; i sistemi esterni e gli strumenti di calcolo sono sottoposti alle verifiche pertinenti.

Negli accordi con partner e clienti sono disciplinati, quando rilevanti, titolarità di dati e risultati, Background IP, Foreground IP, licenze, pubblicazioni, riservatezza, trattamento dei dati e condizioni di valorizzazione o successiva industrializzazione.

La pianificazione della ricerca comprende un confronto con le funzioni competenti quando la sperimentazione utilizza sistemi di terzi, infrastrutture o dataset condivisi, comporta l'accesso ad ambienti cliente o coinvolge direttamente soggetti interessati. La tracciabilità metodologica e contrattuale permette di distinguere le autorizzazioni della fase scientifica da quelle richieste per un impiego operativo o commerciale.

14. Ricerca sostenibile e trasferimento dei risultati

Le attività R&S sono orientate, ove coerente con gli obiettivi scientifici, a ricercare il migliore equilibrio tra capacità del modello, qualità, spiegabilità, controllabilità, risorse impiegate e benefici attesi. La sperimentazione di architetture leggere, verticali, locali o ibride è incoraggiata quale possibile soluzione ai vincoli energetici, di riservatezza e di dipendenza tecnologica, senza escludere l'uso motivato di architetture più complesse quando necessario alla ricerca.

I protocolli sperimentali definiscono, in misura proporzionata, baseline e indicatori appropriati per confrontare architetture, prestazioni e impatti: accuratezza, robustezza, capacità di generalizzazione, latenza, memoria, consumo o proxy energetici, costi di addestramento e inferenza, ripetibilità e condizioni infrastrutturali. Risultati energetici o ambientali vengono comunicati con le relative ipotesi, unità di misura, workload e limiti di trasferibilità; le stime non sono presentate come misure certificate.

La valutazione scientifica considera anche gli effetti sociali potenziali: comprensibilità del risultato, accessibilità, differenze di prestazione per utenti o situazioni differenti, rischi di esclusione, impatti sul lavoro, benefici per servizi pubblici e comunità. Nei progetti di ricerca applicata con contesti reali si raccolgono, quando appropriato, riscontri degli stakeholder interessati e si verificano eventuali effetti inattesi.

Il responsabile della ricerca valorizza risultati negativi, failure case e limiti sperimentali quali evidenze utili al miglioramento dei modelli, delle scelte progettuali e della successiva eventuale industrializzazione. Nessun beneficio ESG è dichiarato acquisito per effetto della sola finalità sostenibile del progetto.

La transizione da ricerca, prototipo o pilot a prodotto, servizio o soluzione destinata a impiego operativo costituisce un punto di controllo specifico. Prima del rilascio sono rivalutati ruolo della Società, classificazione

normativa, requisiti, dati, sicurezza, impatti, diritti di terzi, prestazioni, supervisione, responsabilità e modalità di gestione in esercizio.

Quando l'iniziativa assume caratteristiche di sviluppo o fornitura, si applica anche la Politica Developer; quando viene utilizzata come strumento interno, si applica la Politica User. La denominazione di progetto R&S o PoC non giustifica il mantenimento di un regime sperimentale dopo il passaggio a uso reale o continuativo.

La comunicazione scientifica, tecnica e commerciale dei risultati di ricerca deve distinguere chiaramente risultati sperimentali, dimostrazioni, prestazioni validate e funzionalità pronte per l'utilizzo. La pubblicazione di elaborati, dataset, codice o modelli e la presentazione di risultati a clienti, enti finanziatori o partner seguono le autorizzazioni applicabili, la tutela della proprietà intellettuale e gli impegni di riservatezza.

Il responsabile della ricerca assicura il riesame dei risultati, delle anomalie e dei rischi emersi, valorizzandoli per l'evoluzione dei processi AIMS, delle linee di ricerca e delle soluzioni industriali.

Nelle attività di collaborazione con università, enti di ricerca, imprese e amministrazioni, l'individuazione di finalità condivise e di risultati trasferibili è accompagnata dalla disciplina dei diritti di proprietà intellettuale, delle responsabilità sui dati, delle modalità di pubblicazione e delle condizioni per l'eventuale industrializzazione. Il coinvolgimento di contesti territoriali, servizi pubblici o comunità richiede inoltre una valutazione dei benefici e dei possibili effetti inattesi sulle persone e sull'ambiente.

DISPOSIZIONI FINALI

15. Applicazione, riferimenti e riesame

La Politica generale e le tre articolazioni User, Developer e Researcher costituiscono un quadro unitario di indirizzo per Soft Strategy S.p.A. e sono attuate attraverso il campo di applicazione AIMS, le attribuzioni di responsabilità, le procedure, le istruzioni e i registri pertinenti. Le disposizioni si applicano congiuntamente quando uno stesso sistema o una medesima iniziativa coinvolge più profili. Le regole operative sono rese disponibili ai destinatari secondo le modalità documentali aziendali.

La Politica si raccorda, secondo i rispettivi ambiti, ai Sistemi di Gestione aziendali, alle procedure di sicurezza e gestione dei rischi, ai presidi Data Protection, al Modello 231, alla gestione dei fornitori e dei contratti, alla documentazione di sostenibilità e alla Policy per la tutela e gestione della Proprietà Intellettuale di Soft Strategy S.p.A., versione 1.1 del 18 settembre 2026. Gli obblighi normativi e contrattuali applicabili conservano prevalenza ove impongano requisiti più restrittivi.

Costituiscono riferimenti normativi principali la ISO/IEC 42001:2023, il Regolamento (UE) 2024/1689 (AI Act), come modificato e applicabile, incluso il Regolamento (UE) 2026/1744, il Regolamento (UE) 2016/679 (GDPR), la legge 23 settembre 2025, n. 132, il D.Lgs. 9 settembre 2026, n. 160 e il D.Lgs. 8 giugno 2001, n. 231, secondo i rispettivi ambiti. La conformità dei singoli sistemi è valutata con riferimento alla specifica destinazione d'uso, al ruolo esercitato, alla normativa vigente e alle relative scadenze.

Il Responsabile AI coordina la comunicazione e il riesame della Politica, con il supporto di HR, Compliance, Legal, Data Protection, Responsabile dei Sistemi di Gestione e responsabili delle Business Unit. Il riesame avviene almeno annualmente e in presenza di variazioni significative della normativa, dei rischi, delle attività aziendali, delle tecnologie, delle risultanze di audit o degli incidenti. Le modifiche sono sottoposte all'iter di approvazione previsto dalla Società.

Approvazione: Emanuele Hermes Candela — Amministratore Delegato di Soft Strategy S.p.A.

Data: 04/06/2026 Firma: 