POLITICA SISTEMA

DI GESTIONE INTEGRATO

Rev.	Data	Motivazione	Redazione	Approvazione
0	*24/08/2026*	*Prima emissione*	Comitato Guida	Amministratore Unico
1	*10/09/2026*	*Aggiornamento*	Comitato Guida	Amministratore Unico

Broxlab S.r.l., in qualità di sub-holding digitale del Gruppo Taiga, riconosce nella qualità dei servizi erogati, nella sicurezza delle informazioni trattate, nella tutela dei dati personali degli interessati e nella parità di genere i pilastri fondamentali della propria operatività e del proprio posizionamento di mercato come *Growth Makers per le PMI e le organizzazioni italiane*.

La presente Politica Integrata si applica all'intero perimetro del **Sistema di Gestione Integrato (SGI)** di Broxlab, conforme alle norme **ISO 9001:2015**, **ISO/IEC 27001:2022**, **ISO/IEC 27017:2015**, **ISO/IEC 27018:2025** e **ISO/IEC 27701:2019**, e ai requisiti della prassi di riferimento **UNI/PdR 125:2022** per la parità di genere.

L'architettura certificativa adottata è **3+2**: tre norme certificabili in regime accreditato (ISO 9001 + ISO/IEC 27001 + ISO/IEC 27701) presso un OdC accreditato ESYD/EA-MLA, e due codici di pratica (ISO/IEC 27017 + ISO/IEC 27018:2025) integrati nel SoA dell'ISMS 27001 e oggetto di certificato di conformità senza marchio di accreditamento, in linea con il loro statuto normativo di Code of Practice. La certificazione di parità di genere secondo **UNI/PdR 125:2022** è mantenuta come sistema autonomo integrato nella presente Politica (OdC: **Si Cert Italy s.r.l.**).

A. IMPEGNI GENERALI

La DIR si impegna a:

1. **Soddisfare le esigenze e le aspettative** dei propri clienti — imprese private e pubbliche amministrazioni — erogando servizi conformi ai requisiti contrattuali, normativi e cogenti applicabili.
2. **Migliorare con continuità** l'efficacia del SGI mediante il ciclo Plan-Do-Check-Act, l'analisi dei rischi e delle opportunità, la valutazione delle prestazioni e l'attuazione di azioni correttive.
3. **Operare nel rispetto** di tutta la normativa applicabile, ivi inclusi GDPR (Reg. UE 2016/679), AI Act (Reg. UE 2024/1689), NIS2 (D.lgs. 138/2024), CCNL Telecomunicazioni, Codice degli Appalti, e di ogni altra prescrizione cogente.
4. **Conseguire e mantenere** le certificazioni del SGI presso l'OdC **ISONIKE Ltd** (sede registrata Paphos · sede operativa Atene · accreditato ESYD #1177 in regime EA-MLA + IAF-MLA), per le tre norme certificabili in modo accreditato (ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019). Per i codici di pratica ISO/IEC 27017:2015 e ISO/IEC 27018:2025, integrati nel SoA dell'ISMS, ottenere certificati di conformità dedicati emessi da ISONIKE senza marchio di accreditamento.

B. IMPEGNI SPECIFICI — QUALITÀ (ISO 9001:2015)

1. Mettere il **cliente al centro** di ogni decisione operativa, garantendo focus sui requisiti, gestione delle non conformità e accrescimento della soddisfazione.
2. Industrializzare e documentare i processi delle **6 Business Unit** (Consulenza Strategica, Tecnologia AI, Digital Marketing, Brand & Comunicazione, Formazione, BPO via HICS) per garantire ripetibilità, misurabilità e indipendenza dalla singola persona.

3. Definire **obiettivi misurabili (KPI)** per ciascun processo, riesaminarli almeno annualmente e perseguire la loro continua ottimizzazione.

C. IMPEGNI SPECIFICI — SICUREZZA DELLE INFORMAZIONI (ISO/IEC 27001:2022)

1. Proteggere **Riservatezza, Integrità e Disponibilità (CIA)** di tutte le informazioni gestite, indipendentemente dal supporto, dalla forma e dalla fase del loro ciclo di vita.
2. Adottare un approccio **risk-based** alla sicurezza delle informazioni, condurre risk assessment periodici e mantenere uno **Statement of Applicability** aggiornato sui 93 controlli dell'Annex A.
3. Garantire una **cultura della sicurezza** mediante programmi continuativi di awareness e formazione per tutto il personale (AL-SGI-03).
4. Gestire gli **incidenti di sicurezza** con processi definiti di rilevamento, contenimento, eradicazione, recovery e *lesson learned* (controlli A.5.24-A.5.28).
5. Assicurare la **continuità operativa** dei processi critici e la *ICT readiness* per la business continuity (controllo A.5.30).

D. IMPEGNI SPECIFICI — CLOUD AIDAHUB (ISO/IEC 27017:2015 + ISO/IEC 27018:2025)

1. Per il servizio SaaS **AidaHub**, di cui Broxlab è Cloud Service Provider con server in Unione Europea, garantire: segregazione tenant dei dati cliente · hardening delle componenti virtuali · logging e monitoraggio delle attività amministrative · restituzione integrale dei dati al cliente in caso di exit (entro 30+30 gg) · protezione delle PII conformemente a ISO/IEC 27018:2025 (Code of Practice for PII Processor allineato a 27002:2022) e GDPR.
2. Integrare i controlli di ISO/IEC 27017:2015 e ISO/IEC 27018:2025 nello Statement of Applicability dell'ISMS 27001 (vedi ALL.E e ALL.F), garantendone l'auditabilità in regime accreditato come parte dell'audit ISO 27001.

E. IMPEGNI SPECIFICI — PRIVACY (ISO/IEC 27701:2019 + GDPR)

1. Trattare i dati personali in conformità ai principi di **liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e accountability** (GDPR art. 5).
2. Mantenere un **Registro delle attività di trattamento (ROPA)** aggiornato (GDPR art. 30) per i trattamenti effettuati in qualità di Controller e Processor.
3. Garantire l'esercizio dei **diritti degli interessati** (GDPR artt. 15-22) con procedure formalizzate (PG-PRV-03).
4. Effettuare **DPIA** (GDPR art. 35) per i trattamenti ad alto rischio, in particolare per i sistemi basati su AI integrati nei servizi (PG-PRV-02).

5. Gestire le **violazioni di dati personali** con notifica al Garante entro 72 ore e comunicazione agli interessati ove richiesto (GDPR artt. 33-34 · PG-PRV-04).
6. Designare un **DPO esterno indipendente** (GDPR art. 37) come ulteriore garanzia di compliance e tutela degli interessati (PG-PRV-06).

F. IMPEGNI SUPPLY CHAIN E RAPPORTI CON HICS

1. Per i servizi di **BU06 — Business Process Outsourcing**, erogati attraverso il subappaltatore strategico **HICS S.r.l.**, garantire il pieno presidio della catena del valore mediante: contratto intercompany con clausole di sicurezza e privacy, audit fornitore periodico, monitoraggio KPI di servizio e DPA conforme a GDPR art. 28.
2. Selezionare i propri fornitori critici sulla base di **criteri verificabili di affidabilità, sicurezza e conformità** (controlli A.5.19-A.5.23 · PG-SGI-04).

G. COINVOLGIMENTO DELLE PERSONE

1. Promuovere il **benessere organizzativo**, la **parità di genere** (certificata UNI/PdR 125:2022 — vedi §H) e il rispetto della diversità.
2. Investire nella **formazione continua** e nello sviluppo delle competenze (PG-HR-02).
3. Mantenere canali di **comunicazione bidirezionale** con tutto il personale per la segnalazione di rischi, incidenti, opportunità di miglioramento, incluso il canale whistleblowing conforme a D.Lgs. 24/2023 (PG-HR-08).

H. IMPEGNI SPECIFICI — PARITÀ DI GENERE E PARI OPPORTUNITÀ (UNI/PdR 125:2022)

Broxlab S.r.l. promuove la parità di genere come valore strategico e assume gli impegni di seguito indicati, nel rispetto del D.Lgs 198/2006 (Codice delle pari opportunità), del D.Lgs 105/2022 in materia di conciliazione vita-lavoro, della Convenzione OIL n. 190/2019, del D.Lgs 24/2023 (whistleblowing) e del D.Lgs 81/2008.

Il presidio del sistema è affidato al **Comitato Guida per la parità di genere**, composto dal Responsabile del Sistema di Gestione per la Parità di Genere (RSGPG) e dalla funzione HR, con approvazione della Direzione (AU).

L'organizzazione presidia le 6 aree previste dalla prassi UNI/PdR 125:2022:

1. **Cultura e strategia** — integrare la parità di genere nella visione, nei valori e negli obiettivi aziendali, con un piano strategico dedicato.
2. **Governance** — assicurare presidio, ruoli e responsabilità definiti tramite il Comitato Guida.
3. **Processi HR** — garantire selezione, valutazione, sviluppo e formazione privi di discriminazioni di genere.

4. **Opportunità di crescita e inclusione delle donne** — favorire pari accesso a percorsi di crescita e responsabilità.
5. **Equità remunerativa per genere** — monitorare e ridurre eventuali divari retributivi a parità di ruolo.
6. **Tutela della genitorialità e conciliazione vita-lavoro** — adottare misure di flessibilità, congedi e sostegno alla genitorialità coerenti con il D.Lgs 105/2022.

Broxlab si impegna a prevenire e contrastare ogni forma di molestia e discriminazione, attraverso il **Regolamento aziendale di contrasto alle molestie** e un **canale di segnalazione dedicato**, accessibile tramite apposito pulsante pubblicato sul sito aziendale, nel rispetto della riservatezza e del divieto di ritorsione (D.Lgs 24/2023).

L'organizzazione definisce obiettivi misurabili, ne monitora l'andamento tramite KPI e comunica i risultati agli stakeholder interni ed esterni secondo il piano di comunicazione, garantendo la pubblicazione della presente Politica sul sito aziendale.

I. RIESAME

La presente Politica è riesaminata almeno **annualmente** nell'ambito del Riesame di Direzione ed è soggetta a **revisione straordinaria** in caso di modifiche significative del contesto, dello scope, della normativa applicabile o dell'esito di incidenti rilevanti.

La Direzione (DIR) — Broxlab S.r.l.