BRAINPULL

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI ISO 27001:2022

PREMESSA

BRAINPULL soc. coop. è una società che ha come attività prevalente *la consulenza e il supporto al marketing e alla comunicazione, la coordinazione di campagne pubblicitarie su spazi reali e virtuali (lancio, comunicazione istituzionale, comunicazione promozionale)*. Data la natura delle proprie attività, **BRAINPULL soc. coop** considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo.

BRAINPULL soc. coop pone particolare attenzione ai temi riguardanti la sicurezza dei dati durante il ciclo di vita di progettazione e sviluppo dei propri prodotti/servizi, che devono essere ritenuti un bene primario dell'azienda.

Su tali basi **BRAINPULL soc. coop** ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma **ISO/IEC 27001:2022.**

OBIETTIVI

Il Sistema Informativo (inclusivo delle risorse tecnologiche, hardware, software, informazioni in qualsiasi formato, dati, documenti, reti telematiche e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi di **BRAINPULL soc. coop**, in considerazione della criticità dei processi aziendali che dipendono da esso. Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi e la policy sulla sicurezza delle informazioni al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni attraverso il rispetto delle seguenti proprietà:

- **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- **Integrità:** salvaguardare la consistenza dell'informazione da modifiche e cancellazioni non autorizzate;
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
- **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- **Autenticità:** garantire una provenienza affidabile dell'informazione.
- **Privacy:** garantire la protezione ed il controllo dei dati personali.

L'osservanza dei livelli di sicurezza stabiliti da **BRAINPULL soc. coop** attraverso l'implementazione dell'SGSI, permette di:

- preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi di sicurezza dei dati

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI ISO 27001:2022

- rispondere pienamente alle indicazioni della normativa vigente e cogente e degli standard internazionali di sicurezza dei dati.

AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni adottata da **BRAINPULL soc. coop** si applica indistintamente a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolti. La Politica della sicurezza delle informazioni adottata da **BRAINPULL soc. coop** deve costituire un approccio Sistematico alla sicurezza delle informazioni per tutti i componenti dell'organizzazione che – a qualsiasi Titolo – possono intervenire su qualsiasi informazione presente all'interno dell'Azienda, nell'ambito dei servizi erogati.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di **BRAINPULL soc. coop** rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

Il patrimonio informativo della **BRAINPULL soc. coop** da tutelare è costituito dall'insieme delle informazioni localizzate nella sede dell'azienda.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- ☐ Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- ☐ Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- ☐ Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- ☐ Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- ☐ Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.

BRAINPULL

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI ISO 27001:2022

- ☐ È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- ☐ Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- ☐ Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- ☐ Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- ☐ Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'attività di **BRAINPULL soc. coop**, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine aziendale.

RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.
- attuare, sostenere e verificare periodicamente la presente Politica, a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa;

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI ISO 27001:2022

- riesaminare periodicamente gli obiettivi e la Politica per la sicurezza delle informazioni per accertarne la continua idoneità.

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa Politica e della segnalazione di anomalie di cui dovesse venire a conoscenza.

Il responsabile della sicurezza delle informazioni RSI si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- verificare l'evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni a tutela della sicurezza e continuità delle attività di **BRAINPULL soc. coop**;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni che intrattengono rapporti con **BRAINPULL soc. coop**, devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso sottoscrizione di una nomina e/o una clausola contrattuale all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

RIESAME DELLA POLITICA

La presente Politica Aziendale della Sicurezza sarà revisionata periodicamente sia in caso di eventi esterni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi e sulla sicurezza delle informazioni.

La presente Politica verrà comunque riconfermata e sottoscritta con cadenza annuale. La sua sottoscrizione avverrà durante l'attività di Riesame della Direzione del SGSI.

Data, 08/05/2025

Direzione

BRAIN PULL
Società Cooperativa
Sede Legale
via Torino 44 - 70014 Conversano (BA)
P.I. e C.F. 07359120727