SEGE

SISTEMA DI GESTIONE INTEGRATO
ISO 9001:2015 -27001:2022

MSGI - ALLEGATO 1B

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

REV. 06

DATA 30.06.2025

Revisione	Data	Motivazione
01	28.06.2020	Prima emissione
02	30.09.2022	Aggiornato a seguito dello spostamento dei server su Cloud AWS
03	28.02.2023	Aggiornamento alla nuova versione della ISO 27001:2022
04	19.07.2023	Versione integrata 9001-27001
05	19.07.2024	Aggiornamento per estensioni 27017 e 27018 e AMD 1:2024 cambiamento climatico
06	30.06.2025	Aggiornamento con riferimento a NIS 2 e D.Lvo 138/2024

Redatto in conformità alle Norme UNI EN ISO 9001:2015 e UNI EN ISO/IEC 27001:2022 da parte di SEGE srl - P.IVA 03008050969

Sede Legale e Operativa: Piazza Sicilia 6 - 20146 Milano (MI) - Italia

REDATTO DA Ing. **Stefano Cribellati**
Presidente e Legale Rappresentante SEGE - RSGI

Ing. **Giuseppe Ruscitti**
Consultant Auditor

Dott.ssa **Agata Regeni**
Internal Auditor

VERIFICATO DA Ing. **Stefano Pacchiarini**
CTO SEGE

APPROVATO DA Ing. **Stefano Cribellati**
Presidente e Legale Rappresentante SEGE

DISTRIBUZIONE Il presente documento controllato viene mantenuto sul server aziendale nella cartella destinata ai documenti del **Sistema di Gestione Integrato Qualità e Sicurezza dei dati** in modalità esclusiva di sola lettura.

RISERVATEZZA Il presente documento è **pubblico**.
È permessa la divulgazione all'esterno dell'azienda.

1. SCOPO E OBIETTIVI

La Politica Aziendale impone che, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali sia impostata con le regole proprie dell'applicazione del Sistema di gestione secondo la norma ISO/IEC 27001:2022.

La Direzione di SEGE ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.

Lo scopo della presente Politica è di garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001:2022 e dalle linee guida contenute nello standard ISO/IEC 27002:2022.

2. CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.

L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSD).

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

3. POLITICA SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda, nel cloud (SaaS) e nei sistemi on premises dei clienti.

È necessario assicurare:

- la confidenzialità delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato;
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione;
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

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

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 e dei sistemi cloud. 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 risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

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

- Deve esistere un catalogo costantemente aggiornato degli asset aziendali , inclusi i sitemi cloud, 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.
- 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 con evidenza degli aspetti architetturali e di responsabilità condivisa per i servizi cloud.
- 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 e sui servizi erogati sul cloud in qualità di CSP.
- 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. Consapevole dell'importanza per i clienti della garanzia della catena di fornitura per operatori essenziali, SEGE s'impegna ad allineare procedure e controlli in opera per rispondere ai requisiti indicati dalla Direttiva (UE) 2022/2555 8NIS 2) e al Decreto L.vo 138/2024

4. RESPONSABILITA' DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:

1. Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione. Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
2. Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda. Devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione che, nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali;
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;

– verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

5. RIESAME

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.

Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.

Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.

Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

6. IMPEGNO DELLA DIREZIONE

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 SGSD;
– fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSD;
– controllare che il SGSD sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
– 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.

Milano, lì 19.07.2024

Ing. Stefano Cribellati
Presidente e Legale Rappresentante