

	SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI UNI CEI EN ISO/IEC 27001:2022	
	POLITICA SICUREZZA DELLE INFORMAZIONI	ALL. 1_POL_REV_00 23.10.2025

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La **presente Politica** definisce i **principi** e gli **impegni** di **MAIS S.r.l. Società Benefit** in materia di **Sicurezza delle Informazioni**, in conformità alla **UNI CEI EN ISO/IEC 27001:2022**, e costituisce il quadro di riferimento per la definizione degli obiettivi e per la guida delle azioni in materia di sicurezza.

Tale documento costituisce il quadro di riferimento per la definizione degli obiettivi e per la guida delle azioni strategiche, integrandole con la missione di responsabilità sociale e trasparenza che caratterizza la nostra natura di Società Benefit.

Scopo del documento è **tutelare il patrimonio informativo dell'azienda da minacce interne ed esterne, intenzionali o accidentali**, salvaguardando la **continuità dei servizi di manutenzione e impiantistica**, l'**integrità dei dati di laboratorio** e gli **interessi di clienti, dipendenti, partner** e della **collettività**.

La Politica **si rivolge a tutto il personale e ai collaboratori**, nonché ai **fornitori** e **soggetti terzi** che trattano informazioni per conto di **MAIS S.r.l. Società Benefit**. La **Direzione approva la presente Politica** e ne sostiene l'attuazione mettendo a disposizione risorse, competenze e strumenti adeguati.

Per sicurezza delle informazioni si intende la protezione dei tre pilastri fondamentali di **riservatezza, integrità e disponibilità (R.I.D.)** dei dati e dei sistemi che li elaborano:

- ❖ **Riservatezza:** assicurare che le informazioni siano accessibili solo al personale autorizzato;
- ❖ **Integrità:** salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione;
- ❖ **Disponibilità:** garantire che gli utenti autorizzati abbiano accesso alle informazioni e agli asset associati quando necessario.

Proteggere il patrimonio informativo significa quindi:

- ❖ mantenere il rischio entro livelli accettabili **attraverso un processo continuo di valutazione e trattamento**;
- ❖ individuare tempestivamente eventi e anomalie **mediante sistemi di monitoraggio efficaci**;
- ❖ limitare gli impatti e ripristinare i servizi nel più breve tempo possibile **in caso di incidente**.

A tal fine, **MAIS S.r.l. Società Benefit sta implementando un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)** che coordina **misure organizzative e tecniche proporzionate ai rischi e integrate nei processi aziendali** fin dalle fasi di progettazione dei servizi.

	SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI UNI CEI EN ISO/IEC 27001:2022	
	POLITICA SICUREZZA DELLE INFORMAZIONI	ALL. 1_POL_REV_00 23.10.2025

Principi di riferimento

MAIS S.r.l. Società Benefit nell'implementare il presente Sistema di Gestione, si ispira ai seguenti principi:

- ❖ **Governance e coerenza strategica.** Le misure di sicurezza sono allineate agli obiettivi di business e rispettano i requisiti normativi e contrattuali applicabili;
- ❖ **Proporzionalità basata sul rischio.** I controlli sono selezionati a valle di una valutazione del rischio con criteri di accettazione definiti, bilanciando costi e benefici;
- ❖ **Centralità delle persone.** La sicurezza coinvolge tutti: consapevolezza, comportamenti responsabili e rispetto delle policy sono parte del lavoro quotidiano;
- ❖ **Semplicità operativa.** Le misure sono chiare, proporzionate e applicabili, per garantirne l'effettiva adozione;
- ❖ **By design & by default.** La sicurezza è pianificata e integrata in ogni fase del ciclo di vita di processi, servizi e sistemi;
- ❖ **Minimo privilegio.** Le autorizzazioni seguono il principio del "need-to-know" e sono oggetto di verifica periodica;
- ❖ **Monitoraggio e miglioramento.** Eventi ed incidenti sono rilevati, gestiti e analizzati per alimentare il miglioramento continuo del sistema;
- ❖ **Sicurezza nella catena di fornitura.** I rischi derivanti da fornitori e partner sono gestiti attraverso requisiti di sicurezza chiari e verifiche periodiche;
- ❖ **Resilienza operativa.** L'azienda pianifica e si prepara a gestire le interruzioni per garantire la continuità del business anche in situazioni di crisi.

Obiettivi

In coerenza con i principi sopra esposti, l'azienda persegue i seguenti obiettivi strategici:

- ❖ **Garantire** la conformità alle normative applicabili (Reg. UE 2016/679 GDPR, D.Lgs. 231/2001, normativa metrologica D.M. 93/2017), ai requisiti contrattuali e di settore;
- ❖ **Mantenere** un sistema di sicurezza certificato secondo standard internazionali, a garanzia della fiducia delle parti interessate;
- ❖ **Proteggere** le informazioni critiche, inclusi i dati del Laboratorio Metrologico, da accessi non autorizzati;
- ❖ **Promuovere** una solida cultura della sicurezza attraverso programmi di formazione e consapevolezza continui per tutto il personale;

	SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI UNI CEI EN ISO/IEC 27001:2022	
	POLITICA SICUREZZA DELLE INFORMAZIONI	ALL. 1_POL_REV_00 23.10.2025

- ❖ **Assicurare** la resilienza operativa e la capacità di rispondere efficacemente agli incidenti di sicurezza per minimizzare i danni;
- ❖ **Perseguire** il miglioramento continuo del SGSI per mantenere un livello di protezione adeguato all'evoluzione delle minacce e del business.

Attuazione del sistema

Il SGSI definisce ruoli e responsabilità, procedure e controlli, piani di trattamento del rischio e indicatori di performance. La Direzione ne assicura l'efficacia promuovendo formazione, verifiche periodiche (audit) e conducendo il **Riesame della Direzione** a intervalli pianificati per valutare prestazioni, rischi ed opportunità di miglioramento.

Responsabilità e Impegno

La sicurezza delle informazioni è una responsabilità condivisa che richiede l'impegno attivo di tutto il personale, dei collaboratori e delle terze parti. Ciascuno è tenuto a rispettare le policy e le procedure aziendali, a proteggere gli asset informativi affidati e a segnalare ogni anomalia o potenziale minaccia.

Segnalazioni

Eventuali violazioni o incidenti di sicurezza, intenzionali o dovuti a negligenza, **devono essere prontamente segnalati** tramite i seguenti canali ufficiali:

- **Email:** giusyresta@maissrl.com
- **Posta ordinaria:** sede legale in Via Campania S.N. (Lotto 49 Z.I.), 70021 Acquaviva delle Fonti (BA).

La Direzione.

