

	Politica Anticorruzione	All. 5.2 Rev. 01 del 24/04/2024
---	--------------------------------	---------------------------------------

Politica per la Sicurezza delle Informazioni

1. PREMESSA

Il **Consorzio Stabile LGA** è consapevole dell'importanza di garantire la protezione delle informazioni aziendali, la riservatezza dei dati e l'integrità delle risorse digitali. Questa Politica per la Sicurezza delle Informazioni formalizza l'impegno dell'Organizzazione a conformarsi ai requisiti della ISO/IEC 27001, garantendo un ambiente operativo sicuro e resiliente contro minacce interne ed esterne. L'Organizzazione si impegna a gestire la sicurezza delle informazioni attraverso un approccio basato sul rischio, assicurando trasparenza nei processi, prevenzione delle minacce e continuità operativa.

2. CAMPO DI APPLICAZIONE

Questa politica si applica a:

- **Tutti i dipendenti** e collaboratori del **Consorzio Stabile LGA**.
- **Fornitori, consulenti e terze parti** che trattano dati o accedono ai sistemi informatici dell'Organizzazione.
- **Infrastrutture IT**, risorse digitali, dispositivi aziendali e sistemi di gestione delle informazioni.
- **Tutte le informazioni trattate**, siano esse elettroniche, cartacee o trasmesse attraverso qualsiasi altro mezzo.

L'obiettivo è garantire la protezione delle informazioni aziendali da minacce come accessi non autorizzati, fughe di dati, attacchi informatici e altri rischi che potrebbero comprometterne la riservatezza, l'integrità e la disponibilità.

3. PRINCIPI GENERALI

Infine, Il **Consorzio Stabile LGA** si impegna a rispettare i seguenti **principi fondamentali della sicurezza delle informazioni**:

- **Riservatezza** – Proteggere le informazioni aziendali da accessi non autorizzati.
- **Integrità** – Prevenire alterazioni non autorizzate dei dati e garantire la loro affidabilità.
- **Disponibilità** – Assicurare che le informazioni siano accessibili agli utenti autorizzati quando necessario.
- **Compliance** – Conformità alle normative di settore, in particolare **ISO 27001, GDPR e altre disposizioni regolamentari**.

Per garantire un ambiente operativo sicuro, il **Consorzio Stabile LGA** adotta misure che includono:

	Politica Anticorruzione	All. 5.2 Rev. 01 del 24/04/2024
---	--------------------------------	---------------------------------------

- ✚ **Definizione chiara dei ruoli e delle responsabilità**, con separazione delle funzioni per evitare conflitti di interesse.
- ✚ **Procedure di gestione degli accessi**, garantendo che solo il personale autorizzato possa accedere a informazioni sensibili.
- ✚ **Controlli di sicurezza fisici e logici**, per proteggere le informazioni aziendali e prevenire violazioni.
- ✚ **Monitoraggio e auditing**, con revisioni periodiche dei processi di sicurezza.
- ✚ **Formazione continua**, per aumentare la consapevolezza dei dipendenti sui rischi e sulle best practice in materia di sicurezza informatica.

4. OBIETTIVI

Il **Consorzio Stabile LGA** stabilisce i seguenti **obiettivi strategici**:

- ◆ **Protezione delle informazioni aziendali** da accessi non autorizzati, manipolazioni e divulgazione illecita.
- ◆ **Gestione dei rischi IT**, identificando minacce e adottando misure preventive adeguate.
- ◆ **Garantire la conformità normativa**, assicurando il rispetto delle leggi e regolamenti in materia di sicurezza informatica.
- ◆ **Promuovere la cultura della sicurezza**, attraverso la formazione e la sensibilizzazione del personale.
- ◆ **Gestire incidenti di sicurezza**, attraverso procedure di rilevamento, segnalazione e risposta rapida a eventi critici.
- ◆ **Mantenere la continuità operativa**, implementando strategie di **disaster recovery** e backup periodici.
- ◆ **Monitoraggio costante**, per migliorare continuamente l'efficacia del SGSI.

5. GESTIONE DEGLI INCIDENTI DI SICUREZZA

La Il **Consorzio Stabile LGA** ha implementato un **sistema di gestione degli incidenti** che include:

- **Monitoraggio degli eventi di sicurezza** attraverso strumenti di auditing e logging.
- **Canali di segnalazione degli incidenti** per permettere ai dipendenti di comunicare tempestivamente eventuali anomalie.
- **Processi di risposta agli incidenti** per contenere e mitigare gli effetti di un attacco informatico o di una violazione dei dati.
- **Valutazione e miglioramento continuo** delle procedure di sicurezza in base agli incidenti segnalati.

	Politica Anticorruzione	All. 5.2 Rev. 01 del 24/04/2024
---	--------------------------------	---------------------------------------

6. MONITORAGGIO E REVISIONE

Per garantire la continua efficacia della Politica, sono previste modalità di monitoraggio regolare e revisioni periodiche volte ad adeguare il documento a eventuali cambiamenti normativi, organizzativi o di contesto, assicurandone la coerenza con l'evoluzione delle esigenze aziendali.

Data di aggiornamento: 01710/2024

Firma
