

DOCUMENTO DI POLITICA PER LA SICUREZZA DELLE INFORMAZIONI di IMQ Group S.r.l., CSI S.p.A. e IMQ S.p.A.

PO-SGS/00

IMQ GROUP S.R.L.
CAPOGRUPPO GRUPPO IMQ

Sede legale
Italia
20138 Milano
via Quintiliano 45

tel. (+39) 02 5073 1
fax (+39) 02 5099 1550
imgroup@legalmail.it
www.imgroup.it



Le società IMQ Group S.r.l., CSI S.p.A. e IMQ S.p.A. (nel seguito, congiuntamente, "Organizzazione") hanno adottato un Sistema di Gestione per la Sicurezza delle Informazioni (nel seguito, "SGSI"), che consente di garantire e dimostrare la conformità ai requisiti applicabili in materia di sicurezza delle informazioni.

La presente politica stabilisce gli indirizzi e gli obiettivi strategici per la sicurezza delle informazioni trattate dall'Organizzazione nello svolgimento delle proprie attività e nell'erogazione dei propri servizi.

Tutto il personale dell'Organizzazione, indipendentemente dalla posizione e dalle mansioni svolte, è informato, reso consapevole, tenuto a rispettare ed applicare la presente politica nonché le ulteriori politiche specifiche e procedure del SGSI che da essa derivano e si ispirano.

Governance

IMQ Group S.r.l., in qualità di Capogruppo, esercita funzioni di direzione, indirizzo strategico e coordinamento in materia di sicurezza delle informazioni, assicurando un governo centralizzato degli aspetti inerenti alla protezione e alla gestione delle informazioni.

La presente politica, applicabile all'intera Organizzazione, assicura che la sicurezza delle informazioni sia affrontata e gestita in modo uniforme, coerente, consistente e sistematico all'interno dell'Organizzazione.

Informazioni da proteggere

Le informazioni trattate dall'Organizzazione, incluse nel perimetro del SGSI, comprendono, a titolo esemplificativo ma non esaustivo:

- Informazioni dell'Organizzazione: dati, documenti o altre informazioni di carattere trasversale all'Organizzazione (ad es., dati del personale, dati finanziari e commerciali, strategie aziendali, ecc.) oppure correlati ai servizi erogati dall'Organizzazione (ad es., risultati e documentazione delle attività di test, certificazione, ispezione e valutazione, ecc.);
- Informazioni dei clienti: prodotti, prototipi, dati e documenti progettuali, documentazione tecnica e commerciale, risultati e documentazione delle attività di test, certificazione, ispezione, valutazioni, ecc.;
- Informazioni di soggetti terzi: dati, documenti o altre informazioni di soggetti terzi (diversi dai clienti) o afferenti alle relazioni con essi, che devono essere protetti in virtù di obblighi legali, contrattuali o di copyright.

Tali informazioni rappresentano le *informazioni che devono essere protette dall'Organizzazione* mediante l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate alle minacce e ai relativi rischi identificati e valutati dall'Organizzazione attraverso il processo di gestione del rischio.

Principi fondamentali e obiettivi strategici

L'Organizzazione stabilisce i seguenti obiettivi strategici per la sicurezza delle informazioni, declinati rispetto ai principi fondamentali:

- **Riservatezza:** garantire che le informazioni siano accessibili esclusivamente ai soggetti autorizzati, applicando il principio “*need to know*”.
La riservatezza delle informazioni deve essere protetta sia per adempiere ai requisiti legislativi, normativi e contrattuali in materia di riservatezza, sia per prevenire impatti negativi sul mantenimento di accreditamenti, notifiche o riconoscimenti, sull'immagine e sulla reputazione dell'Organizzazione;
- **Integrità:** assicurare l'accuratezza, la completezza e l'autenticità delle informazioni.
L'integrità delle informazioni deve essere protetta per assicurare l'affidabilità e la validità delle informazioni nonché per prevenire impatti negativi sui processi decisionali e sulle attività operative, sul rispetto degli impegni contrattuali, sul mantenimento di accreditamenti, notifiche o riconoscimenti, sull'immagine e sulla reputazione dell'Organizzazione;
- **Disponibilità:** garantire che le informazioni necessarie e gli strumenti di supporto correlati (sistemi informativi e di rete, applicativi, ecc.) siano accessibili e utilizzabili quando richiesto dai soggetti autorizzati.
La disponibilità delle informazioni e degli strumenti di supporto correlati deve essere garantita per assicurare l'operatività dell'Organizzazione e l'erogazione dei relativi servizi nei tempi e modi previsti dai requisiti legislativi, normativi e contrattuali applicabili.
- **Conformità:** soddisfare i requisiti delle parti interessate rilevanti per la sicurezza delle informazioni, inclusi i requisiti legislativi, normativi e contrattuali applicabili all'Organizzazione.

In coerenza con i suddetti obiettivi strategici, l'Organizzazione definisce e riesamina periodicamente obiettivi specifici per la sicurezza delle informazioni, tenendo in considerazione

i requisiti applicabili, i risultati della valutazione e del trattamento del rischio, il contesto, le esigenze e le aspettative delle parti interessate e i risultati del monitoraggio dell'SGSI.

Ruoli e Responsabilità

L'Organizzazione individua i ruoli chiave per la sicurezza delle informazioni, assegnando a ciascuno responsabilità e autorità specifiche, al fine di garantire una struttura organizzativa adeguata al conseguimento degli obiettivi e dei risultati attesi del SGSI.

Formazione, competenza e consapevolezza del personale

L'Organizzazione assicura che tutto il suo personale sia consapevole delle proprie responsabilità in materia di sicurezza delle informazioni e vi adempia correttamente.

A tal fine, l'Organizzazione promuove e assicura la pianificazione e l'attuazione di programmi di informazione, formazione e addestramento, finalizzati a garantire che tutto il personale acquisisca e mantenga adeguate conoscenze delle politiche e delle procedure del SGSI, nonché competenze e qualifiche in materia di sicurezza delle informazioni coerenti con il proprio ruolo e le relative responsabilità.

L'Organizzazione mantiene adeguati contatti con gruppi specialistici o altri forum di sicurezza specializzati e associazioni professionali, al fine di:

- migliorare la conoscenza aziendale sulle “*best practices*” e mantenere l'aggiornamento in materia di sicurezza delle informazioni;
- assicurare che la comprensione delle tematiche di sicurezza delle informazioni in azienda sia aggiornata e completa;
- ricevere tempestivamente informazioni (ad es., alert, avvisi, patch da applicare) in merito a vulnerabilità, possibili attacchi e contromisure da applicare.

Conformità e miglioramento continuo

L'Organizzazione si impegna a garantire la conformità ai requisiti ad essa applicabili in materia di sicurezza delle informazioni e a migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia del SGSI. A tal fine, l'Organizzazione conduce, a intervalli regolari, audit interni, riesami di direzione, attività di monitoraggio, riesame del contesto dell'Organizzazione, valutazione dei rischi.

Fornitori e altri soggetti terzi

L'Organizzazione rende pubblicamente disponibile la presente politica affinché tutti i soggetti terzi interessati siano informati in merito alle esigenze e agli obiettivi dell'Organizzazione in materia di sicurezza delle informazioni.

L'Organizzazione si impegna ad avvalersi di fornitori preventivamente selezionati, qualificati e, qualora il loro operato possa avere un impatto sulla sicurezza delle informazioni, informati della presente politica.

I fornitori dell'Organizzazione sono tenuti ad operare nel rispetto degli accordi contrattuali sottoscritti con l'Organizzazione, comprensivi, ove applicabili, di specifici requisiti in materia di sicurezza delle informazioni.

L'Organizzazione si impegna a monitorare e riesaminare periodicamente le prestazioni dei fornitori e la loro conformità ai requisiti contrattuali.

Riesame della presente politica

La presente politica è riesaminata e, se opportuno, aggiornata periodicamente, nonché qualora si verificano cambiamenti significativi in relazione alla sicurezza delle informazioni.

Milano, 14 settembre 2026

dott. Vincenzo de Martino

Presidente e Amministratore delegato
di IMQ Group S.r.l.

Ing. Fausto Mozzarelli

Amministratore delegato

di IMQ S.p.A.

Ing. Fulvio Giorgi

Amministratore delegato

di IMQ S.p.A.