ISMS

Information Security Management System

Doc. **NI-ISMS.01** Rev. **00** del **15/07/2025**

Classificazione: **C1 – PUBLIC**

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Industrie LISA s.r.l.

Sede legale e operativa: Corso Susa, 23 10040 Caselette (TO) Italy
P.IVA C.F/Registro imprese: 02545750016 - CCIAA Torino 565935
Iscritta al Trib. di Torino al n° 3309/79, Cap. Soc. € 10.400 int. Vers.
PEC : industrielisa@pecsoci.ui.torino.it
Telefono Tel. +39 0119688722 - +39 0119688959

1 SCHEDA DEL DOCUMENTO

Elenco delle revisioni

Rev.	Emissione	Modifiche apportate	Approvazione	
0	ISM	Prima Edizione nel ISMS	Direzione	15/07/2025

Riferimenti normativi

D.Lgs. 138/2024 – Decreto attuazione direttiva 2555/2022 NIS 2
Regolamento EU 2016/679 - General Data Protection Regulation
TISAX VDA ISA 6.03 - 1.1.1
ISO/IEC 27001:2022 - A5.1

Documenti collegati

2 ELENCO DEI CONTENUTI

3 PREMESSA

Industrie LISA S.r.l. (di seguito anche "organizzazione") è un'azienda specializzata nello stampaggio a freddo della lamiera per il mercato dei componenti automobilistici, in grado di realizzare internamente stampi e attrezzature grazie alla presenza di un consolidato reparto di attrezzeria. In un contesto industriale sempre più caratterizzato da digitalizzazione dei processi, integrazione tra impianti e sistemi informativi e crescente esposizione a minacce informatiche complesse, la sicurezza delle informazioni assume un ruolo strategico.

La protezione del patrimonio informativo – che comprende dati tecnici, commerciali, amministrativi, personali, documentazione di processo e di prodotto, nonché la proprietà intellettuale e il know-how aziendale – è un presupposto essenziale per:

1. garantire la continuità operativa e la qualità dei servizi erogati;
2. mantenere e rafforzare la fiducia di Clienti, Fornitori, Partner e altri stakeholder;
3. assicurare la conformità a norme, regolamenti e requisiti contrattuali di settore.
4.

La presente Politica nasce con l'obiettivo di definire, in modo chiaro e strutturato, l'approccio dell'organizzazione alla sicurezza delle informazioni, inserendosi in modo coerente nel sistema di gestione integrato già presente (Qualità, Ambiente, Salute e Sicurezza sul lavoro) e in particolare in un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) conforme alla norma ISO/IEC 27001 e al framework VDA ISA/TISAX.

4 SCOPO

La presente Politica definisce i principi, gli obiettivi e le linee guida generali adottati da Industrie LISA S.r.l. per impostare, attuare, mantenere e migliorare il proprio Sistema di Gestione della Sicurezza delle Informazioni (ISMS).
In particolare, la Politica:

- descrive l'approccio complessivo dell'organizzazione alla sicurezza delle informazioni e al trattamento dei rischi correlati;
- fornisce il quadro di riferimento per la definizione, il monitoraggio e il riesame degli obiettivi di sicurezza delle informazioni;
- orienta la progettazione e l'attuazione di misure tecniche e organizzative volte a prevenire accessi non autorizzati, perdite, manipolazioni, distruzioni o indisponibilità delle informazioni;
- assicura l'allineamento del sistema ai requisiti normativi e agli standard di settore (ISO/IEC 27001, VDA ISA/TISAX).

5 DEFINIZIONE DI SICUREZZA DELLE INFORMAZIONI

Per sicurezza delle informazioni si intende l'insieme delle misure, dei controlli, dei processi e delle pratiche finalizzati a proteggere le informazioni da accessi non autorizzati, modifiche indebite, perdite, distruzioni o interruzioni, assicurando il rispetto di tre requisiti fondamentali:

- Riservatezza: garantire che l'informazione sia accessibile esclusivamente ai soggetti autorizzati, prevenendo qualunque forma di divulgazione non consentita.
- Integrità: assicurare che l'informazione sia corretta, completa e protetta da alterazioni non autorizzate, sia intenzionali sia accidentali.
- Disponibilità: assicurare che l'informazione e i sistemi che la trattano siano accessibili e utilizzabili tempestivamente da parte dei soggetti autorizzati, quando necessario per lo svolgimento delle attività aziendali.

6 AMBITO DI APPLICAZIONE

La presente Politica per la Sicurezza delle Informazioni si applica a tutto il perimetro organizzativo di Industrie LISA S.r.l. e, in particolare, a:

- Tutte le informazioni trattate dall'organizzazione, indipendentemente dalla forma o dal supporto (digitale, cartaceo, verbale, fotografico, fisico o prototipale), dalla natura (tecnica, commerciale, amministrativa, personale, ecc.) e dal livello di classificazione;
- Tutti i soggetti che, a qualsiasi titolo, accedono, elaborano, trasmettono o gestiscono informazioni aziendali: dipendenti, collaboratori, consulenti, fornitori, partner commerciali e altri soggetti esterni formalmente autorizzati;
- Tutti i processi, sistemi e infrastrutture che supportano il trattamento delle informazioni, incluse applicazioni, basi dati, servizi in cloud, dispositivi mobili, postazioni di lavoro, reti aziendali e sistemi di controllo degli impianti;
- Tutte le sedi e gli spazi fisici in cui le informazioni vengono create, trattate, trasmesse o conservate, quali uffici, reparti produttivi, magazzini, archivi, ambienti in cloud o siti remoti.

L'ambito comprende anche le attività e le iniziative aziendali che comportano l'utilizzo di informazioni di Clienti, Fornitori o altre parti interessate, con l'obiettivo di garantire un livello di protezione adeguato e una continuità operativa coerente con i requisiti normativi e contrattuali.

7 OBIETTIVI

Gli obiettivi primari della sicurezza delle informazioni per Industrie LISA S.r.l. sono i seguenti:

a. Garantire la continuità operativa e la resilienza dei processi e dei sistemi aziendali, minimizzando il rischio di interruzioni dovute a incidenti informatici o a eventi avversi;
b. Proteggere la proprietà intellettuale e il know-how aziendale, con particolare attenzione alle informazioni tecniche e ai dati relativi a progettazione del processo, attrezzature e prototipi;
c. Prevenire e ridurre l'impatto di incidenti di sicurezza, adottando misure volte a limitare i danni e a ripristinare rapidamente la normale operatività;
d. Assicurare la conformità ai requisiti normativi, contrattuali e di settore (ISO/IEC 27001, VDA ISA/TISAX, GDPR, NIS 2 e altri regolamenti applicabili);
e. Accrescere la consapevolezza del personale in materia di sicurezza delle informazioni e di protezione dei dati personali, promuovendo comportamenti corretti e responsabili;
f. Dimostrare in modo trasparente l'impegno dell'organizzazione nei confronti dei propri stakeholder, fornendo evidenze di un sistema di gestione della sicurezza strutturato e affidabile.

8 STRATEGIE OPERATIVE

Per il raggiungimento degli obiettivi sopra indicati, l'organizzazione adotta un insieme coerente di strategie operative, tra cui:

- l'implementazione e il mantenimento di un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla ISO/IEC 27001:2022 e, ove pertinente, al framework VDA ISA 6.x / TISAX;
- lo svolgimento di analisi periodiche dei rischi legati alla sicurezza delle informazioni, con l'identificazione e la valutazione delle minacce e delle vulnerabilità, nonché la definizione delle misure di trattamento più idonee;
- l'adozione di controlli tecnici e organizzativi basati sulla classificazione delle informazioni e sulla criticità dei processi che le trattano;

- la realizzazione di attività di formazione e sensibilizzazione continua del personale, finalizzate a diffondere una cultura orientata alla sicurezza e alla responsabilità individuale;
- il monitoraggio degli eventi di sicurezza e la gestione strutturata degli incidenti, mediante procedure documentate e canali di comunicazione dedicati;
- l'esecuzione di audit interni e verifiche periodiche, allo scopo di valutare l'efficacia delle misure implementate e individuare aree di miglioramento.

9 PRINCIPI GUIDA

La gestione della sicurezza delle informazioni e della protezione dei dati personali presso Industrie LISA S.r.l. si basa sui seguenti principi guida fondamentali, che orientano la definizione delle misure di controllo e delle procedure operative:

9.1 Classificazione delle informazioni

Le informazioni sono classificate in base al loro livello di sensibilità, al valore per l'organizzazione e alla criticità rispetto ai processi aziendali. A ciascuna classe di informazioni viene associato un livello di protezione adeguato, che tiene conto dei requisiti di riservatezza, integrità e disponibilità. La classificazione consente di applicare controlli proporzionati al rischio e di garantire un trattamento coerente su tutto il perimetro aziendale.

9.2 Controllo degli accessi

L'accesso alle informazioni avviene secondo il principio del "need-to-know", garantendo che solo i soggetti debitamente autorizzati possano accedere ai dati pertinenti al proprio ruolo. I diritti di accesso sono definiti, concessi, rivisti e revocati in modo controllato, al fine di minimizzare il rischio di utilizzi impropri o non autorizzati delle informazioni.

9.3 Crittografia

L'uso della crittografia è previsto per la protezione delle informazioni classificate ad alto rischio o particolarmente sensibili. Tali informazioni devono essere cifrate quando vengono memorizzate su supporti digitali o trasmesse attraverso reti interne o esterne, con l'obiettivo di prevenire la perdita di riservatezza e l'intercettazione non autorizzata dei dati.

9.4 Integrità e disponibilità delle informazioni

L'organizzazione adotta misure tecniche e organizzative – quali sistemi di backup regolari, infrastrutture ridondanti, controlli di coerenza e verifiche periodiche – per garantire che le informazioni siano autentiche, integre e disponibili quando necessario. Vengono inoltre previste procedure per la manutenzione preventiva e correttiva dei sistemi informativi, al fine di ridurre il rischio di guasti e interruzioni.

9.5 Conservazione e distruzione delle informazioni

Le informazioni vengono conservate per periodi di tempo definiti sulla base di obblighi normativi, contrattuali o esigenze operative. Al termine del ciclo di vita, i dati sono eliminati o anonimizzati in modo sicuro e controllato, secondo procedure documentate, allo scopo di tutelare la riservatezza e garantire la conformità alle leggi vigenti.

9.6 Adeguatezza e proporzionalità delle misure

Le misure di sicurezza sono progettate e implementate in modo proporzionato al livello di rischio associato ai processi e alle informazioni trattate. Ciò significa che controlli particolarmente rigorosi sono applicati alle informazioni ad alta criticità, mentre per le informazioni meno sensibili si adottano soluzioni equilibrate, evitando oneri eccessivi rispetto al rischio concreto.

10 IMPEGNO DELLA DIREZIONE

La Direzione di Industrie LISA S.r.l. riconosce che le informazioni rappresentano un patrimonio strategico e fondamentale per la continuità e il successo dell'azienda. Per questo motivo si impegna formalmente a:

- riesaminare periodicamente gli obiettivi e le politiche di sicurezza delle informazioni, assicurandone la coerenza con la strategia aziendale, il contesto normativo e le aspettative delle parti interessate;
- mettere a disposizione le risorse necessarie (economiche, tecnologiche, organizzative e professionali) per l'attuazione efficace delle misure previste dalla presente Politica e dal sistema di gestione (ISMS);
- promuovere e sostenere una cultura aziendale orientata alla sicurezza, attraverso attività di formazione e sensibilizzazione rivolte al personale interno e ai collaboratori esterni coinvolti nel trattamento delle informazioni;
- verificare periodicamente l'efficacia delle misure di sicurezza implementate, tramite audit, monitoraggi e riesami, individuando tempestivamente eventuali criticità e predisponendo azioni correttive e di miglioramento continuo;
- attribuire ruoli e responsabilità chiari in materia di sicurezza delle informazioni, assicurando che ogni funzione aziendale contribuisca attivamente al raggiungimento degli obiettivi;
- rispettare rigorosamente tutte le normative applicabili, incluse le disposizioni in materia di protezione dei dati personali (Regolamento (UE) 2016/679 – GDPR), le prescrizioni NIS 2, gli standard tecnici TISAX e gli ulteriori regolamenti nazionali e internazionali rilevanti.

La Direzione assicura che tale impegno sia diffuso, compreso e condiviso a tutti i livelli dell'organizzazione, al fine di garantire il massimo livello di protezione del patrimonio informativo e delle informazioni personali gestite.

11 RESPONSABILITÀ

All'interno dell'organizzazione, le responsabilità relative alla sicurezza delle informazioni sono distribuite in modo chiaro e coerente con la struttura organizzativa.

- Responsabile della Sicurezza delle Informazioni (ISM): coordina il Sistema di Gestione della Sicurezza delle Informazioni, promuove l'attuazione delle misure di controllo, monitora la conformità alle politiche adottate, gestisce le segnalazioni di incidenti e supporta la Direzione nel riesame periodico dell'ISMS.
- Process owner: sono responsabili dell'implementazione, del mantenimento e del monitoraggio delle misure di sicurezza all'interno dei processi di propria competenza. Devono assicurare che le attività di processo rispettino le politiche aziendali e collaborare con le altre funzioni per mitigare i rischi di sicurezza.
- Dipendenti e collaboratori: sono tenuti a rispettare integralmente le politiche, le procedure e le istruzioni operative in materia di sicurezza delle informazioni. Devono adottare comportamenti responsabili nella gestione delle informazioni, segnalare tempestivamente incidenti, vulnerabilità o comportamenti non conformi e partecipare alle attività di formazione e sensibilizzazione previste.
- Fornitori e terze parti: devono attenersi ai requisiti di sicurezza definiti negli accordi contrattuali e nelle politiche aziendali. È loro responsabilità garantire che le attività svolte e i sistemi utilizzati non compromettano la sicurezza delle informazioni di Industrie LISA S.r.l., segnalando tempestivamente eventuali incidenti, violazioni o anomalie tramite i punti di contatto stabiliti.

12 ECCEZIONI

Le esenzioni o eccezioni alla presente Politica non sono, in linea generale, ammesse. Tuttavia, in situazioni straordinarie e di comprovata necessità, la Direzione può valutare e approvare specifiche deroghe, purché:

- siano adeguatamente motivate e documentate;
- includano l'analisi dei rischi derivanti dall'eccezione;
- definiscano misure compensative e limiti temporali ben precisi.

Le eccezioni approvate sono riesaminate periodicamente, al fine di verificare se sussistano ancora le condizioni che ne hanno determinato l'introduzione e, se del caso, procedere alla loro revoca.

13 VIOLAZIONI E SANZIONI

Qualsiasi violazione delle disposizioni contenute nella presente Politica o nei documenti collegati può comportare l'applicazione di misure disciplinari e/o azioni legali, in considerazione dei possibili impatti negativi derivanti da comportamenti negligenti o dolosi.

In particolare:

- le infrazioni commesse da dipendenti e collaboratori sono considerate gravi violazioni degli obblighi contrattuali e possono essere sanzionate in conformità alla normativa vigente, ai contratti di lavoro e alle policy interne;
- le violazioni imputabili a fornitori o terze parti possono comportare l'applicazione delle misure previste nei relativi contratti (ad esempio risoluzione, risarcimento danni, esclusione da future collaborazioni);
- ove necessario, l'organizzazione si riserva il diritto di segnalare i fatti alle autorità competenti, in conformità alle leggi applicabili, per la valutazione di eventuali responsabilità civili o penali.

14 SEGNALAZIONE DELLE VIOLAZIONI

Eventuali violazioni o sospette violazioni della presente politica, così come eventuali vulnerabilità, incidenti o anomalie riguardanti la sicurezza delle informazioni, devono essere segnalate senza ritardo al Responsabile della Sicurezza delle Informazioni (ISM), scrivendo all'indirizzo e-mail dedicato ism@industrielisa.it . Le segnalazioni, anche quando si riferiscano a eventi potenziali o dubbi, costituiscono un contributo fondamentale per consentire all'azienda di intervenire in modo tempestivo, limitare gli impatti negativi e migliorare continuamente l'efficacia del sistema.

15 VALIDITÀ, REVISIONE E APPROVAZIONE

La presente Politica è approvata formalmente dalla Direzione Generale di Industrie LISA S.r.l. ed entra in vigore alla data indicata nella scheda del documento. Essa è soggetta a riesame periodico almeno annuale, oppure in occasione di cambiamenti significativi nell'organizzazione, nel contesto normativo o tecnologico.

Ogni revisione della Politica:

a. viene valutata e approvata dalla Direzione;
b. è registrata nel sistema documentale aziendale con indicazione della data di emissione e della natura delle modifiche;
c. sostituisce integralmente le versioni precedenti, diventando vincolante per tutti i dipendenti, collaboratori e fornitori dell'organizzazione.

	Caselette, 15/07/2025 Ed.1.0 – Rev.0 Effective Date: **15/07/2025** Industrie LISA s.r.l Amministratore Unico **Luca MARTINI**

FINE