ISMS

Information Security Management System

POLICY
Doc. **PO-ISMS.001** Rev. 0 del **10/01/2025**
Classificazione: **C1 – PUBLIC**

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Giobert **S.p.A.**
Sede legale e operativa: via Pavia 82, Rivoli (Italia)
P.IVA C.F/Registro imprese: 09948100012- Cod. REA: TO – 1093620
PEC giobert@pec.giobertgroup.com
Telefono +39 011 9548711

1 SCHEDA DEL DOCUMENTO

Elenco delle revisioni

Rev.	Emissione	Modifiche apportate	Approvazione	
0	RSI	Prima Edizione nel ISMS	Direzione Centrale Giobert S.p.A.	10/01/2025

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
TISAX VDA ISA 6.03 - 1.1.1

Documenti collegati

2 ELENCO DEI CONTENUTI

3 PREMESSA

Giobert SpA (di seguito organizzazione) è un'azienda specializzata nella progettazione e produzione di componenti meccatronici per il settore automotive, in particolare sistemi di blocco e chiavi per veicoli.
In un contesto caratterizzato da crescente digitalizzazione e minacce informatiche complesse, l'organizzazione attribuisce massima importanza alla protezione delle informazioni aziendali, al fine di salvaguardare la competitività e la fiducia di clienti, partner e stakeholder.

4 SCOPO

Questa politica definisce l'approccio dell' organizzazione alla sicurezza delle informazioni, con l'obiettivo di prevenire accessi non autorizzati, perdite, manipolazioni, distruzioni o indisponibilità delle informazioni gestite, tutelando il patrimonio informativo dell'azienda e di tutti i suoi stakeholder.

5 DEFINIZIONE DI SICUREZZA DELLE INFORMAZIONI

La sicurezza delle informazioni è l'insieme delle misure, dei controlli e delle pratiche finalizzate a proteggere le informazioni da accessi non autorizzati, modifiche indebite, perdite, distruzioni o interruzioni, al fine di garantire:

- Riservatezza: assicurare che l'informazione sia accessibile esclusivamente ai soggetti autorizzati, impedendo ogni forma di divulgazione non autorizzata.
- Integrità: garantire che l'informazione sia corretta, completa e protetta da alterazioni non autorizzate, intenzionali o accidentali.
- Disponibilità: assicurare che l'informazione e i sistemi che la trattano siano accessibili e utilizzabili tempestivamente quando richiesto dai soggetti autorizzati.

6 AMBITO DI APPLICAZIONE

La presente Politica per la Sicurezza delle Informazioni si applica a:

- Tutte le informazioni trattate da Giobert S.p.A., indipendentemente dalla loro forma o supporto (digitale, cartaceo, verbale), dalla natura (tecnica, commerciale, amministrativa, personale, ecc.) e dalla classificazione;
- Tutti i soggetti che, a qualsiasi titolo, accedono, elaborano, trasmettono o gestiscono informazioni aziendali, inclusi dipendenti, collaboratori, consulenti, fornitori, partner commerciali e ogni altro soggetto esterno formalmente autorizzato;
- Tutti i processi, sistemi informativi, applicazioni, infrastrutture tecnologiche, dispositivi e sedi fisiche – inclusi uffici, reparti produttivi, archivi, ambienti in cloud o sedi remote – nei quali le informazioni vengano create, trattate, trasmesse o conservate.

L'ambito si estende inoltre a tutte le attività e iniziative aziendali che comportano l'utilizzo di informazioni, al fine di garantire un livello adeguato di protezione e continuità operativa, in coerenza con i requisiti normativi, contrattuali e organizzativi applicabili

7 OBIETTIVI

Gli obiettivi primari della sicurezza delle informazioni per Giobert S.p.A. includono:

- Garantire continuità operativa e resilienza dei sistemi aziendali;
- Proteggere la proprietà intellettuale e il know-how aziendale;
- Prevenire e ridurre l'impatto di incidenti informatici;
- Assicurare la conformità a requisiti normativi, contrattuali e di settore (es. ISO 27001, TISAX, VDA/ISA);
- Favorire la consapevolezza del personale in materia di sicurezza;
- Dimostrare l'impegno dell'organizzazione per la sicurezza delle informazioni verso i propri stakeholder.

8 STRATEGIE OPERATIVE

Per il raggiungimento degli obiettivi, l'organizzazione adotta le seguenti strategie:

- Implementare e mantenere un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma ISO/IEC 27001:2022 e, ove pertinente, al framework VDA/ISA 6.0.3;
- Formazione e sensibilizzazione continua del personale;
- Analisi periodica dei rischi legati alla sicurezza delle informazioni;
- Implementazione di controlli tecnici e organizzativi basati sulla classificazione delle informazioni;
- Monitoraggio degli eventi di sicurezza e risposta strutturata agli incidenti;
- Audit regolari per verificare l'efficacia delle misure adottate.

9 PRINCIPI GUIDA

La gestione della sicurezza delle informazioni e della protezione dei dati personali presso Giobert S.p.A. si basa sull' insieme dei seguenti principi guida fondamentali:

1. **Classificazione delle informazioni**
   Tutte le informazioni vengono classificate in base al loro livello di sensibilità, valore e criticità per l'organizzazione, assegnando un livello di protezione adeguato al tipo di informazione trattata.
2. **Controllo degli accessi**
   L'accesso alle informazioni è regolato secondo il principio del "need-to-know" garantendo che solo i soggetti debitamente autorizzati possono accedere alle informazioni pertinenti al proprio ruolo, minimizzando il rischio di accessi non autorizzati o impropri.
3. **Crittografia**
   L'uso della crittografia è obbligatorio per la protezione delle informazioni classificate ad alto rischio, sia quando sono archiviate su supporti digitali o fisici, sia durante la loro trasmissione attraverso reti interne o pubbliche, garantendo un presidio fondamentale contro la perdita di riservatezza e l'intercettazione non autorizzata dei dati.
4. **Integrità e disponibilità delle informazioni**

Sono adottate misure tecniche e organizzative volte ad assicurare l'autenticità, l'inalterabilità e l'affidabilità dei dati. Tali misure includono sistemi di backup regolari, infrastrutture ridondanti, procedure per la verifica periodica dell'autenticità e correttezza dei dati trattati, nonché interventi di manutenzione preventiva sui sistemi informativi.

5. **Conservazione e distruzione delle informazioni**
   Le informazioni sono conservate per un periodo definito in base agli obblighi normativi, contrattuali o operativi, e vengono eliminate in modo sicuro al termine del ciclo di vita. Le modalità di conservazione e distruzione sono stabilite da procedure documentate, volte a garantire la tutela della riservatezza e la conformità alle normative vigenti.
6. **Adeguatezza e proporzionalità delle misure di sicurezza**
   Le misure di sicurezza sono progettate e implementate in modo adeguato e proporzionato al livello di rischio associato al trattamento delle informazioni.

10 IMPEGNO DELLA DIREZIONE

La Direzione di Giobert S.p.A. riconosce che le informazioni rappresentano un patrimonio strategico e fondamentale per la continuità e il successo dell'azienda e si impegna formalmente a garantire un adeguato livello di sicurezza delle informazioni attraverso:

- La revisione degli obiettivi e delle politiche di sicurezza delle informazioni, assicurandone la coerenza con le strategie aziendali e con il contesto normativo applicabile;
- La messa a disposizione delle risorse economiche, tecnologiche e organizzative necessarie per l'attuazione efficace delle misure previste dalla presente politica e dal sistema di gestione della sicurezza delle informazioni adottato (ISMS);
- La promozione e il sostegno di una cultura aziendale basata sulla consapevolezza della sicurezza, tramite formazione periodica e sensibilizzazione continua di tutto il personale e dei collaboratori esterni coinvolti nel trattamento delle informazioni;
- La verifica periodica dell'efficacia delle misure di sicurezza implementate, tramite audit e riesami periodici, al fine di identificare tempestivamente eventuali criticità e intraprendere opportune azioni correttive o di miglioramento continuo;
- L'assegnazione di ruoli e responsabilità chiari e ben definiti in materia di sicurezza delle informazioni, garantendo che ogni soggetto aziendale partecipi attivamente al raggiungimento degli obiettivi fissati;
- Il rispetto rigoroso di tutte le normative applicabili, incluse ISO/IEC 27001:2022, TISAX, Regolamento (EU) 2916/69 GDPR, D-Lgs 138/2024 NIS e ulteriori regolamenti nazionali e internazionali rilevanti.
- La Direzione assicura che tale impegno venga diffuso, compreso e adottato da tutta l'organizzazione, al fine di garantire il massimo livello di protezione del patrimonio informativo aziendale e delle informazioni personali gestite.

11 RESPONSABILITÀ

All'interno dell' organizzazione le responsabilità per la sicurezza delle informazioni sono distribuite come segue:

- **Process owner**: Hanno il compito di implementare, mantenere e monitorare le misure di sicurezza delle informazioni all'interno dei processi aziendali di competenza. Devono garantire che i processi e i servizi siano conformi alle politiche aziendali e collaborare con altre funzioni o servizi per mitigare i rischi di sicurezza.
- **Dipendenti e Collaboratori**: Sono tenuti a rispettare integralmente le politiche e le procedure aziendali in materia di sicurezza delle informazioni. Devono adottare comportamenti responsabili nella gestione delle informazioni e segnalare tempestivamente eventuali incidenti di sicurezza, vulnerabilità o comportamenti non conformi.
- **Fornitori e Terze Parti**: Devono aderire rigorosamente ai requisiti di sicurezza definiti negli accordi contrattuali e nelle politiche per la sicurezza delle informazioni. È loro responsabilità garantire che le proprie attività e i propri sistemi non compromettano la sicurezza delle informazioni aziendali di Giobert S.p.A segnalando tempestivamente incidenti , violazioni o anomalie attraverso i punti di contatto stabiliti.

12 ECCEZIONI

Le esenzioni ed eccezioni alla presente politica non sono generalmente ammesse. Tuttavia, in casi straordinari e di estrema necessità la Direzione Generale di Giobert S.p.a. può approvare eccezioni. Le eccezioni vengono documentate e riviste regolarmente per verificare la sussistenza nel tempo del principio di estrema necessità che le ha determinate.

13 VIOLAZIONI E SANZIONI

Qualsiasi violazione delle disposizioni contenute nel presente documento o nei suoi allegati potrà comportare l'applicazione di misure disciplinari e/o azioni legali, in considerazione dei possibili impatti negativi derivanti da comportamenti negligenti o dolosi. In particolare, ogni infrazione commessa da dipendenti, collaboratori o soggetti terzi operanti per conto dell'organizzazione sarà considerata una grave violazione degli obblighi contrattuali e potrà essere sanzionata in conformità alle normative applicabili, ai contratti di lavoro vigenti e alle policy interne. Ove necessario, l'organizzazione si riserva il diritto di segnalare le violazioni alle autorità competenti, in conformità con le leggi locali e internazionali, al fine di valutare eventuali implicazioni 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 al Responsabile della Sicurezza delle Informazioni (ISM), scrivendo all'indirizzo e-mail dedicato: ism@giobert.com. Tali segnalazioni consentono all'azienda di intervenire con rapidità, limitando eventuali impatti negativi e contribuendo al miglioramento continuo del sistema di gestione della sicurezza delle informazioni.

15 VALIDITÀ, REVISIONE E APPROVAZIONE

La presente politica è approvata formalmente dalla Direzione Generale ed è soggetta a riesame periodico, almeno annuale, o in occasione di cambiamenti rilevanti nell'organizzazione, nella normativa o nel contesto operativo e tecnologico. Ogni modifica deve essere approvata formalmente prima della sua entrata in vigore, e tutte le versioni aggiornate della politica sono comunicate tempestivamente ai soggetti interessati. La versione aggiornata sostituisce integralmente quella precedente, diventando immediatamente vincolante per tutti i dipendenti, collaboratori e fornitori dell'organizzazione.

Data: 10/01/2025
Firma Direzione Generale
Giobert S.p.A.

FINE