POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E LA PROTEZIONE DEI DATI PERSONALI (S06)

CONTROLS REFERENCES

VDA ISA 5.1	**1.1.1**		
ISO/IEC 27001:2022	**5.1**		

MATRICE DELLE REVISIONI

Rev.	Data	Descrizione	Redatto	Verificato	Approvato
1	22/05/2024	Aggiunto framework VDA/ISA 5.1 ai requisiti per il ISMS (§.6)	ISM	QSM	GM
0	25/09/2023	Emissione	ISM	QSM	AD

RIFERIMENTI NORMATIVI

Titolo	Note
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
Regolamento EU 2016/679	General Data Protection Regulation (GDPR)
VDA/ISA 5.1	VDA Information Security Assessment Ver. 5.1

1 PREMESSA

Raicam Driveline s.r.l. è un'azienda specializzata nella progettazione, sviluppo e produzione di frizioni e attuatori per l'industria automobilistica. L'azienda attribuisce primaria importanza alla sicurezza delle informazioni, soprattutto in un contesto caratterizzato da una costante evoluzione tecnologica e da incessanti sfide relative alla protezione dei dati. Offrendo soluzioni a produttori originali (OEM) e al mercato aftermarket, l'azienda è pienamente consapevole che la fiducia accordata dai propri clienti e partner non risiede unicamente nella qualità dei prodotti forniti, ma altresì nella capacità di assicurare l'integrità, la confidenzialità e la disponibilità delle informazioni trattate.

2 SCOPO

L'obiettivo di questa politica è garantire la protezione delle informazioni aziendali gestite nell'ambito della progettazione, produzione e sviluppo di frizioni e attuatori per l'industria automobilistica contro tutte le minacce, sia interne che esterne, sia intenzionali che accidentali.

3 AMBITO DI APPLICAZIONE

Questa politica si applica a tutto il personale, sia interno che esterno (es. fornitori), coinvolto nei processi di progettazione, produzione e commercializzazione dei nostri prodotti, nonché ai servizi, alle risorse tecniche, alle infrastrutture e ai processi aziendali coinvolti, anche indirettamente, nella progettazione, produzione e commercializzazione di tali prodotti.

L'ambito di applicazione include sia le informazioni aziendali che quelle trattate per conto dei nostri clienti, indipendentemente dalla loro natura o forma (digitale, cartacea, verbale, etc.).

La politica si applica a tutti i luoghi, le attività e i processi in cui svolgiamo le attività di progettazione, produzione o di supporto.

Tutti i dipendenti, collaboratori e fornitori coinvolti nella attività di progettazione, produzione e commercializzazione dei nostri prodotti sono tenuti ad applicare questa politica e a contribuire alla sua attuazione e al raggiungimento degli obiettivi per la sicurezza delle informazioni in essa stabiliti.

4 DEFINIZIONE DELLA SICUREZZA DELLE INFORMAZIONI

Per la nostra organizzazione la sicurezza delle informazioni consiste nel proteggere le informazioni e i sistemi informativi di supporto da accessi non autorizzati, utilizzi impropri, divulgazioni indesiderate, interruzioni, modifiche o distruzioni.

5 OBIETTIVI

L'obiettivo generale è di assicurare la sicurezza delle informazioni trattate, garantendo su base permanente le seguenti proprietà delle informazioni:

- **Confidenzialità:** assicurando che le informazioni siano accessibili solo a coloro che sono autorizzati ad accedervi.
- **Integrità*:*** preservando l'accuratezza e la completezza delle informazioni e dei processi di elaborazione.
- **Disponibilità*:*** garantendo che gli utenti autorizzati possano accedere alle informazioni e alle risorse pertinenti quando necessario.

Inoltre, la nostra organizzazione si pone i seguenti ulteriori obiettivi:

5.1 Sicurezza delle informazioni.

- **Asset tecnologici:** preservare la sicurezza degli asset tecnologici che supportano il trattamento delle informazioni;
- **Conformità e legalità:** assicurare e garantire la conformità con le leggi, i regolamenti e gli obblighi contrattuali;
- **Business Continuity:** garantire la continuità delle attività aziendali in caso di incidenti di sicurezza;
- **Personale**: promuovere la consapevolezza sulla sicurezza delle informazioni tra i dipendenti e le parti interessate esterne.
- **Servizi aziendali:** garantire affidabilità e sicurezza di tutte le componenti che supportano i servizi aziendali;
- **Comunicazioni:** garantire la sicurezza dei canali attraverso cui vengono trasferite le informazioni;
- **Rischio:** gestire e tenere sotto controllo i rischi per la sicurezza delle informazioni contenendoli entro livelli accettabili;
- **Certificazioni:** garantire ai clienti e gli altri stakeholder il nostro impegno costante per la protezione delle loro informazioni attraverso il raggiungimento di specifiche certificazioni (es. TISAX);
- **Collaborazione:** supportare i clienti e nella gestione dei rischi di sicurezza, sia nelle attività formali/documentali, sia in quelle sostanziali legate alla prevenzione dei rischi stessi;
- **Progettazione e sviluppo:** sviluppare i processi aziendali sulla base di standard riconosciuti, metodologie consolidate, obbligazioni contrattuali, leggi e regolamenti applicabili.

5.2 Protezione dei dati personali

- **Consapevolezza e formazione:** garantire che tutti i dipendenti siano consapevoli dei requisiti del GDPR e siano adeguatamente formati per trattare correttamente i dati personali.
- **Design e privacy by default**: integrare la privacy fin dalle prime fasi di progettazione dei prodotti e dei servizi, adottando misure tecniche e organizzative adeguate per garantire la protezione dei dati personali.
- **Responsabile della protezione dei dati (DPO**): Valutare regolarmente le condizioni per la nomina obbligatoria come stabilito dall'articolo 37 del Regolamento UE

2016/679 e, se necessario, nominare un Responsabile della protezione dei dati (RPD).

- **Consenso informato:** ottenere se previsto il consenso esplicito e informato degli interessati prima di raccogliere o trattare i loro dati personali, fornendo informazioni chiare e trasparenti sulle finalità e sulle modalità di trattamento.
- **Trasferimenti internazionali di dati**: garantire che i trasferimenti di dati personali al di fuori dello Spazio economico europeo (SEE) siano effettuati conformemente alle disposizioni del GDPR, ad esempio mediante l'utilizzo di clausole contrattuali tipo o di meccanismi di certificazione.
- **Protezione dei dati particolari e giudiziari:** trattare le categorie particolati e giudiziarie di dati personali in conformità alle restrizioni previste dal GDPR, adottando misure di sicurezza adeguate a prevenire l'accesso, la divulgazione o l'uso non autorizzato di tali dati.
- **Diritti degli interessati:** rispettare e facilitare l'esercizio dei diritti degli interessati, come il diritto di accesso, il diritto alla rettifica, il diritto all'oblio, il diritto alla portabilità dei dati e il diritto all'opposizione al trattamento.
- **Sicurezza dei dati:** implementare misure di sicurezza adeguate a proteggere i dati personali da perdite, accessi non autorizzati, alterazioni o divulgazioni illecite, tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, della portata, del contesto e delle finalità del trattamento.
- **Valutazione dell'impatto sulla protezione dei dati (DPIA):** condurre, quando necessario, le valutazioni dell'impatto sulla protezione dei dati (DPIA) per valutare e mitigare i rischi associati alle attività di trattamento dei dati personali, specialmente quando il trattamento potrebbe comportare rischi elevati per i diritti e le libertà degli interessati.
- **Notifica delle violazioni dei dati:** notificare tempestivamente le violazioni dei dati personali alle autorità di controllo competenti e, se del caso, agli interessati, conformemente agli obblighi di notifica previsti dal GDPR.
- **Conservazione dei dati:** conservare i dati personali solo per il tempo necessario per raggiungere le finalità per le quali sono stati raccolti, rispettando i limiti di conservazione previsti dalla legge e assicurandosi che i dati vengano eliminati in modo sicuro una volta scaduto il periodo di conservazione.
- **Privacy nelle comunicazioni di marketing**: rispettare le norme del GDPR per le attività di marketing, ad esempio ottenendo il consenso degli interessati per l'invio di comunicazioni di marketing e fornendo loro la possibilità di revocare il consenso in qualsiasi momento.
- **Responsabilità dei fornitori di servizi**: garantire che i fornitori di servizi che trattano dati personali per conto dell'azienda siano adeguatamente selezionati, valutati e sottoposti a contratti vincolanti che stabiliscano gli obblighi di conformità al GDPR.
- **Monitoraggio e audit**: implementare meccanismi di monitoraggio e audit interni per verificare la conformità al GDPR, identificare potenziali violazioni e adottare le misure correttive appropriate.

- **Consapevolezza della privacy degli interessati**: informare gli interessati sui loro diritti in materia di privacy, a fornire loro informazioni chiare sulla gestione dei loro dati personali e a rispondere alle loro richieste e preoccupazioni in modo tempestivo ed efficace.

6 STRATEGIE

Per il raggiungimento dei nostri obiettivi sono adottate le seguenti strategie operative:

- operare sempre nel rispetto degli accordi contrattuali e normativi;
- promuovere lo sviluppo professionale e la professionalità dei nostri collaboratori attraverso attività di formazione e aggiornamento continuo.
- garantire che tutte le attività siano svolte con serietà, competenza e professionalità.
- implementare un sistema di gestione integrato per la sicurezza delle informazioni e la protezione dei dati personali basato sulle linee guida ISO/IEC 27001:2022 e conforme al framework VDA/ISA 5.1, in grado di fornire strumenti e processi di controllo per migliorare continuamente metodi e risultati.
- coinvolgere e sensibilizzare il personale ad operare in conformità con la presente politica e ad agire in conformità con i requisiti stabiliti dal sistema di gestione e a segnalare eventuali violazioni di sicurezza delle informazioni di cui venga a conoscenza.

7 REQUISITI DEL SISTEMA DI GESTIONE

Il sistema di gestione integrato per la sicurezza delle informazioni e la protezione dei dati personali risponde ai seguenti requisiti minimi:

- monitoraggio costante dei processi e delle misure di sicurezza delle informazioni.
- registrazione, analisi e investigazione tempestive di eventuali non conformità. violazioni e incidenti di sicurezza, identificando le cause e definendo le adeguate azioni di mitigazione.
- condotta di audit interni e audit da parte di organismi indipendenti per verificare l'efficacia dei controlli per la sicurezza delle informazioni e delle contromisure.
- indirizzamento ottimale degli investimenti in base alla tipologia di informazioni trattate e alle esigenze di sicurezza espresse dagli stakeholder.
- fornitura di adeguata formazione alla personale diffusione della cultura della sicurezza delle informazioni.

8 PRINCIPI GUIDA PER LA SICUREZZA DELLE INFORMAZIONI E DEI DATI PERSONALI

I principi guida per tutte le attività relative alla sicurezza delle informazioni sono i seguenti:

- **Classificazione e protezione:** Tutte le informazioni sono asset di valore e devono essere classificate in base alla loro sensibilità e adeguatamente protette in funzione della loro criticità;

- **Accesso alle Informazioni:** L'accesso alle informazioni deve essere basato sul principio del bisogno di conoscenza (c.d. "*need-to-know*") e controllato sulla base di una specifica politica di controllo degli accessi.
- **Misure di sicurezza:** Le misure di sicurezza devono essere proporzionali al rischio.
- **Crittografia:** Le informazioni più sensibili devono essere sottoposte a cifratura durante la trasmissione e quando sono memorizzate su dispositivi portatili o sistemi esterni.
- **Integrità delle Informazioni:** Devono essere prese misure per garantire l'integrità delle informazioni.
- **Conservazione delle Informazioni:** Le informazioni devono essere conservate per il periodo richiesto dalla legge o dalla politica interna dell'azienda.
- **Distruzione delle Informazioni:** Le informazioni devono essere distrutte in modo sicuro quando non sono più necessarie.

9 IMPEGNO A SODDISFARE I REQUISITI APPLICABILI

Raicam Driveline si impegna a rispettare tutte le leggi, i regolamenti e gli altri requisiti applicabili alla sicurezza delle informazioni. Questo include, ma non è limitato a, la protezione dei dati personali, la proprietà intellettuale, le leggi sulla diffamazione, il diritto penale e i contratti con clienti e fornitori e le altre parti interessate.

10 RESPONSABILITÀ

Ogni soggetto coinvolto direttamente o indirettamente nella progettazione, produzione e sviluppo di frizioni e attuatori per l'industria automobilistica è responsabile di comprendere e aderire a questa politica, nonché di segnalare eventuali violazioni o potenziali rischi per la sicurezza delle informazioni.

11 SANZIONI

La mancata osservanza dei requisiti per la sicurezza delle informazioni e la protezione dei dati personali stabiliti da questa politica o dal sistema di gestione integrato, può comportare sanzioni disciplinari, fino alla cessazione del rapporto lavorativo o contrattuale.

12 DIREZIONE

La direzione si impegna a migliorare continuamente il sistema di gestione integrato per la sicurezza delle informazioni e la protezione dei dati personali attraverso la revisione regolare delle politiche, dei controlli, dell'efficacia delle misure di sicurezza e del rispetto delle leggi e dei regolamenti applicabili.

13 GESTIONE DELLE ESENZIONI ED ECCEZIONI

Le esenzioni ed eccezioni alla politica aziendale per la sicurezza delle informazioni e la protezione dei dati personali sono ammesse, previa approvazione della Direzione Generale,

solo in casi straordinari e di estrema necessità. Le eccezioni devono essere adeguatamente documentate, e riviste regolarmente per garantire che siano ancora necessarie.

14 CONFORMITÀ

Questa politica viene mantenuta costantemente in linea con i requisiti legislativi, normativi e contrattuali applicabili.

15 VALIDITA' APPROVAZIONE E MODIFICHE

La presente politica per la sicurezza delle informazioni è approvata dalla Direzione Generale. Tutte le modifiche a questa politica devono essere approvate dalla Direzione Generale prima dell'implementazione.

La politica è valida dalla data di approvazione

Mondovì, 22/05/2024

Raicam Driveline s.r.l
F.to General Manager
Andrea BLENGINO

Firmato digitalmente da:
Blengino Andrea Nicola
Firmato il 26/06/2024 16:43
Seriale Certificato: 3193617
Valido dal 16/01/2024 al 16/01/2027
InfoCamere Qualified Electronic Signature CA