

Politica per la Sicurezza delle informazioni

INDICE

1. PREMESSA.....	2
2. OBIETTIVI.....	2
3. AMBITO DI APPLICAZIONE.....	3
4. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI	3
5. RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI	4
6. RIESAME DELLA POLITICA.....	4

Classificazione
<input checked="" type="checkbox"/> Pubblico
<input type="checkbox"/> Ad Uso interno
<input type="checkbox"/> Confidenziale
<input type="checkbox"/> Segreto

La Direzione Generale

1. PREMESSA

SKG Italia è una società che opera principalmente nell'Area Automotive. Data la natura delle proprie attività e dati i requisiti cliente in essere, SKG Italia considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo.

SKG Italia pone particolare attenzione ai temi riguardanti la sicurezza dei dati durante il ciclo di vita di progettazione e sviluppo dei propri prodotti, che devono essere ritenuti un bene primario dell'azienda.

Su tali basi SKG Italia ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma UNI CEI ISO/IEC 27001:2017.

2. OBIETTIVI

Il Sistema Informativo (inclusivo delle risorse tecnologiche, hardware, software, informazioni in qualsiasi formato, dati, documenti, reti telematiche e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi di SKG Italia, in considerazione della criticità dei processi aziendali che dipendono da esso. Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi e la policy sulla sicurezza delle informazioni al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni attraverso il rispetto delle seguenti proprietà:

- Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- Integrità: salvaguardare la consistenza dell'informazione da modifiche e cancellazioni non autorizzate;
- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architettonici associati quando ne fanno richiesta;
- Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- Autenticità: garantire una provenienza affidabile dell'informazione.
- Privacy: garantire la protezione ed il controllo dei dati personali.

L'osservanza dei livelli di sicurezza stabiliti da SKG Italia attraverso l'implementazione dell'SGSI, permette di:

- preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi di sicurezza dei dati
- rispondere pienamente alle indicazioni della normativa vigente e cogente e degli standard internazionali di sicurezza dei dati.

3. AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni adottata da SKG Italia si applica indistintamente a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolti. La Politica della sicurezza delle informazioni adottata da SKG Italia deve costituire un approccio Sistematico alla sicurezza delle informazioni per tutti i componenti dell'organizzazione che - a qualsiasi Titolo - possono intervenire su qualsiasi informazione presente all'interno dell'Azienda, nell'ambito dei servizi erogati.

4. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di SKG Italia rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di SKG Italia si ispira ai seguenti principi:

- Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

La politica della sicurezza delle informazioni formalizzata nell'SGSI, viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

5. RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa Politica e della segnalazione di anomalie di cui dovesse venire a conoscenza.

Il responsabile della sicurezza delle informazioni RSI si occupa assieme ad RSGI della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- verificare l'evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni a tutela della sicurezza e continuità delle attività di SKG Italia;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni che intrattengono rapporti con SKG Italia, devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

6. RIESAME DELLA POLITICA

La presente Politica Aziendale della Sicurezza sarà revisionata periodicamente sia in caso di eventi esterni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi e sulla sicurezza delle informazioni.

La presente Politica verrà comunque riconfermata e sottoscritta con cadenza annuale. La sua sottoscrizione avverrà durante l'attività di Riesame della Direzione del SGSI.