

L'obiettivo della **DRAS S.r.l.** nell'ambito del "Commercio all'ingrosso specializzato di componenti e ricambi per il settore industriale", è il pieno raggiungimento della soddisfazione del cliente e di tutte le parti interessate (*Stakeholders*).

La direzione **DRAS S.r.l.** ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.

Lo scopo della presente policy è di garantire la massima soddisfazione del cliente nella fruizione dei nostri servizi e la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle nostre attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda. È necessario assicurare:

- **la riservatezza delle informazioni:** ovvero le informazioni devono essere accessibili solo a chi è autorizzato.
- **l'integrità delle informazioni:** ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- **la disponibilità delle informazioni:** ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

I Ns. principi della gestione della sicurezza delle informazioni abbracciano i seguenti aspetti:

1. **ASSET INVENTORY SEMPRE AGGIORNATO** - Garantire un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
2. **VALUTAZIONE DEI RISCHI DELLE INFORMAZIONI AGGIORNATA** - La valutazione dei rischi delle informazioni viene aggiornata almeno una volta all'anno in occasione del riesame della direzione o nel caso si presentino eventi avversi o nel caso vi sia un adeguamento dell'asset inventory.
3. **ACCESSO AI SISTEMI SICURO** - Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto ad una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita e devono essere periodicamente sottoposte a revisione.
4. **UTILIZZO SICURO DEI BENI AZIENDALI** - Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
5. **FORMAZIONE CONTINUA DEL PERSONALE** - Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
6. **GESTIONE TEMPESTIVA DI EVENTI AVVERSI** - Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
7. **PROTEZIONE FISICA ADEGUATA DELLE SEDI AZIENDALI** - È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
8. **GESTIONE DELLA COMPLIANCE CONTRATTUALE CON LE TERZE PARTI** - Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
9. **SIMULAZIONI DEL PIANO DI CONTINUITA' AZIENDALE** - Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
10. **SICUREZZA INFORMATICA BY DESIGN** - Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
11. **AGGIORNAMENTO LEGISLATIVO CONTINUO** - Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.
12. **PENETRATION TEST PERIODICI** - Devono essere eseguiti penetration test periodici nelle infrastrutture e negli applicativi per valutare la resilienza dei sistemi ad attacchi esterni ed evincere eventuali vulnerabilità e consentirne il successivo fixing.

L'osservanza e l'attuazione delle policy sono responsabilità di:

- a) **Tutto il personale** che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.  
Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
- b) **Tutti i soggetti esterni** che intrattengono rapporti e collaborano con l'azienda. Devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione che, nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio,
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali,
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi,
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni,
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite ed in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del Sistema di gestione ISO 27001;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di gestione ISO 27001;
- controllare che il Sistema di gestione ISO 27001 sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della qualità e sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Per la definizione degli obiettivi e pianificazione annuale per l'SGI, si rimanda ai documenti di sistema *Riesame della Direzione e Piano di Miglioramento*.