

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

In un mondo digitale costantemente connesso e con attacchi in continuo sviluppo, investire nella sicurezza informatica della propria azienda significa porre un freno a scenari catastrofici di attacchi informatici che potrebbero comportare danni alla reputazione, ai clienti e al profitto dell'azienda. Proprio per questo la Dusty S.r.l. ha implementato un sistema di gestione della sicurezza delle informazioni (SGSI) in conformità alla norma ISO/IEC 27001:2022, per garantire e proteggere i dati, le informazioni proprie, dei propri clienti, fornitori e le risorse informative da tutte le minacce o incidenti, esterni e/o interni, accidentali e/o intenzionali, che possono compromettere l'erogazione dei servizi. In applicazione di tale impegno, l'organizzazione attua la politica per la sicurezza delle informazioni e dei dati personali in modo da:

- Adottare un sistema di gestione delle informazioni conforme ai requisiti specificati delle Norme UNI CEI EN ISO/IEC 27001:2022
- Nominare formalmente il responsabile della sicurezza delle informazioni e il DPO;
- Assicurare che tutto il personale interno dell'organizzazione siano adeguatamente informati e formati sui temi relativi alla sicurezza delle informazioni al fine di minimizzare i rischi derivanti dalle minacce.
- Mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI.
- Garantire la sicurezza incorporata come elemento essenziale delle reti, dei sistemi informativi, delle operazioni e degli accessi alle informazioni in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.

E' obiettivo di Dusty S.r.l. salvaguardare la sicurezza del proprio sistema informativo attraverso il rispetto dei seguenti principi:

1. **RISERVATEZZA DEI DATI:** Garantire che i dati e le informazioni siano preservati dal possibile utilizzo o accesso da parte di soggetti non autorizzati e siano utilizzate esclusivamente dai soggetti autorizzati.
2. **INTEGRITA' DEI DATI:** Garantire che ogni informazione sia realmente quella originariamente inserita nel sistema informatico mantenendo la veridicità garantendo che non siano in alcun modo modificati o cancellati, se non ad opera di soggetti autorizzati.
3. **DISPONIBILITA' DEI DATI:** Assicurare che gli utenti autorizzati abbiano accesso alle informazioni
4. **AUTENTICITA':** Garantire che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.
5. **CONTROLLO DEI DATI:** Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati.
6. **PRIVACY:** Garantire la protezione ed il controllo dei dati personali.

La Politica aziendale impone che, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali sia impostata con le regole proprie dell'applicazione del Sistema di gestione secondo la norma ISO/IEC 27001:2022.

La direzione di Dusty 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 tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27001 nelle loro ultime versioni.

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda. L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione (SGSD). L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

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 confidenzialità delle informazioni: ovvero le informazioni devono essere accessibili solo da 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.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo.

La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- Deve esistere 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.
- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a 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.
- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- 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.
- 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.
- 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.
- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- 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.
- 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.
- 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.

L'osservanza e l'attuazione della presente policy sono responsabilità di:

1- 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.

2-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 e 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.

Il Responsabile del Sistema di Gestione ha la responsabilità del riesame della politica.

Il riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.

Dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

La direzione sostiene attivamente la sicurezza delle informazioni in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

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 SGSD;
- Fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGSD;
- Controllare che il SGSD 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 sicurezza delle informazioni;
- Attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Catania, 30/11/2022

Amministratore Unico

