POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

INFORMATION SECURITY POLICY

Sommario

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI / INFORMATION SECURITY POLICY

Da Lio S.p.A. ha approvato la presente politica per la sicurezza delle informazioni.

Da Lio S.p.A. è consapevole che, per lo sviluppo del proprio mercato, il SGSI riveste un ruolo di assoluto rilievo strategico e rappresenta un importante bene aziendale da tutelare.
In particolare, le informazioni rappresentano un asset aziendale e, in quanto tali, devono essere adeguatamente protette.
Per questo motivo Da Lio S.p.A. ha implementato un Sistema di Gestione della Sicurezza delle Informazioni, identificando anche gli strumenti organizzativi, gestionali e di controllo rilevanti. L'obiettivo generale è proteggere i dati dalle minacce, al fine di:

a. Assicurare la continuità di gestione;
b. Minimizzare i danni operativi;
c. Massimizzare la redditività degli investimenti e le opportunità di mercato.

La sicurezza delle informazioni è intesa come il mantenimento di:

a. riservatezza, ossia garantire l'accesso alle informazioni solo ai soggetti autorizzati;
b. integrità, ossia salvaguardare l'accuratezza e la completezza delle informazioni e delle modalità di trattamento;
c. disponibilità, ossia garantire l'accesso alle informazioni e agli asset associati ai soggetti autorizzati che lo richiedono.

La riservatezza, l'integrità e la disponibilità delle informazioni sono obiettivi fondamentali per garantire trasparenza e obiettività, per raggiungere e mantenere un margine di competitività, cash-flow, redditività, conformità legale e un'immagine aziendale affidabile.
La sicurezza delle informazioni è ottenuta implementando una serie di controlli adeguati quali il Manuale di Gestione della Sicurezza delle

Da Lio S.p.A. approved this information security policy.

Da Lio S.p.A. is aware that, for the development of its market, the ISMS plays a role of absolute strategic importance and represents an important corporate asset to be protected.
In particular, information represents a company asset and as such must be adequately protected.

Da Lio S.p.A. has therefore implemented a Management System for Information Security, also identifying the related organisational, management and control tools. The general objective is to protect data from threats in order to:

a. Ensuring continuity of management;
b. Minimise operational damages
c. Maximising return on investment and market opportunities;

Information security is understood as the maintenance of:

a. confidentiality, i.e. ensuring that only authorised persons have access to information;
b. integrity, i.e. safeguarding the accuracy and completeness of the information and processing methods;
c. availability, i.e. ensuring access to information and related information assets for authorised users who request it;

Confidentiality, integrity and availability of information are fundamental objectives to ensure transparency and objectivity, to achieve and maintain a competitive edge, cash flow, profitability, legal compliance and a reliable business image.

Information security is obtained by implementing a series of suitable controls such as the Information Security Management Procedures, organisational

Informazioni, disposizioni organizzative, istruzioni gestionali ed operative, strutture organizzative e funzioni software. Questi controlli sono stati implementati al fine di garantire il rispetto degli obiettivi specifici che mirano a proteggere il patrimonio di Da Lio S.p.A.

provisions, management and operational instructions, organisational structures and software functions. These controls have been established to ensure compliance with the specific objectives aimed at protecting the assets of Da Lio S.p.A.

La sicurezza raggiungibile solamente attraverso le misure tecniche è limitata e deve essere supportata da procedure di gestione della sicurezza delle informazioni adeguate.

Security that can only be achieved by technical means is limited and must be supported by appropriate

La sicurezza e i relativi controlli richiedono una pianificazione attenta e sistematica, oltre ad un'attenzione meticolosa verso i dettagli.

Information security management procedures. Security and its controls require careful and systematic planning, together with meticulous attention to detail.

La gestione della Sicurezza delle informazioni è il risultato tangibile della partecipazione responsabile e competente anche di fornitori e clienti.

Information Security Management is the tangible result of competent and responsible participation by suppliers and customers.

I requisiti di sicurezza sono stati identificati utilizzando tre fonti principali.

Prima fonte: valutazione del rischio. Questa fonte ha consentito di identificare le minacce, valutare la vulnerabilità e la probabilità di accadimento delle minacce oltre a stimare l'eventuale impatto.

Seconda fonte: requisti legali, prescritti da leggi, norme regolamentari e contrattuali che Da Lio S.p.A. deve soddisfare.

Terza fonte: specifica serie di principi, obiettivi e requisiti per il trattamento e l'elaborazione dei dati che Da Lio S.p.A. ha sviluppato per supportare le proprie attività e a valle della valutazione del rischio.

Security requirements have been identified through the use of three main sources.

First source: risk assessment. This source made it possible to identify threats, evaluate the vulnerability and probability of occurrence of threats and estimate their possible impact.

Second source: the legal requirements, prescribed by laws, regulations and contractual standards that Da Lio S.p.A. must fulfil.

Third source: a specific set of principles, objectives and requirements for data processing and processing that Da Lio S.p.A. has developed to support its activities overall the risk assessment.

Il Responsabile della sicurezza delle informazioni esegue revisioni periodiche della valutazione dei rischi di protezione e dei controlli implementati per:

a. prendere in considerazione le modifiche ai requisiti gestionali e alle priorità;
b. prendere in considerazione nuove minacce e vulnerabilità;

The Information Security Manager carries out periodic reviews of the protection risk assessment and controls implemented for:

a. taking into account changes in management requirements and priorities;
b. considering new threats and vulnerabilities;

c. confermare che i controlli siano validi, idonei ed efficaci.

Vengono eseguite revisioni periodiche ogni qualvolta necessarie, in base ai risultati di valutazioni precedenti e per confronto ai livelli di rischio stabiliti. In particolare, sono implementate revisioni periodiche e/o estemporanee, quando necessario, dei seguenti fattori:

a. l'efficacia della politica per la sicurezza delle informazioni dimostrata dalla natura, dal numero e dall'incidenza degli accadimenti dannosi registrati;
b. il costo e l'incidenza dei controlli sull'efficacia gestionale;
c. gli effetti delle modifiche apportate alla tecnologia.

Da Lio S.p.A. considera rilevanti per un'implementazione positiva della sicurezza delle informazioni i seguenti fattori:

- la politica di sicurezza delle informazioni e le attività che riflettono gli obiettivi gestionali in essa contenuti;
- un approccio di implementazione della sicurezza delle informazioni coerente con la cultura di Da Lio S.p.A.;
- la buona comprensione dei requisiti di sicurezza, valutazione e gestione dei rischi;
- la distribuzione ai fornitori di direttive per l'attuazione delle norme e della politica di sicurezza delle informazioni;
- la garanzia di addestramento e formazione inerenti la sicurezza delle informazioni;
- un sistema di misurazione per valutare le prestazioni di gestione della sicurezza delle informazioni e suggerimenti per il miglioramento continuo.

c. confirming that the controls are valid, appropriate and effective.

Periodic reviews are carried out whenever necessary, based on the results of previous assessments and in comparison with the established risk levels. In particular, periodic and/or extemporary revisions are implemented, when necessary, of the following factors:

a. the effectiveness of the information security policy as demonstrated by the nature, number and incidence of recorded malicious occurrences;
b. the cost and impact of the controls on management effectiveness;
c. the effects of changes in technology;

Da Lio S.p.A. considers the following factors crucial for a positive implementation of information security:

- the information security policy and activities reflecting the management objectives contained therein;
- the approach to implementing information security in line with the culture of Da Lio S.p.A.;
- a good understanding of security requirements, risk assessment and management;
- the distribution to suppliers of guidelines for the implementation of rules and the information security policy;
- ensuring training and education related to information security;
- a measurement system to evaluate information security management performance and suggestions for continuous improvement.

Questi fattori rilevanti di successo per la gestione della sicurezza delle informazioni impegnano Da Lio S.p.A. dalla gestione di tale sistema ad un approccio organizzativo che include le seguenti direttive:

- la conformità ai requisiti legislativi e contrattuali;
- la prevenzione e rivelazione di software non autorizzati;
- la gestione della continuità operativa;
- le conseguenze della violazione della politica di sicurezza;
- una definizione delle responsabilità gestionali e specifiche per la gestione della sicurezza delle informazioni;
- la verbalizzazione di incidenti inerenti la sicurezza delle informazioni;
- la documentazione organizzativa, gestionale e operativa a supporto della politica della sicurezza delle informazioni;
- la divulgazione in forma adeguata, accessibile e comprensibile agli operatori e agli utenti, delle direttive e procedure di sicurezza;
- la sistematica e periodica valutazione dei rischi come attività preventiva;
- la eliminazione dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non è possibile, loro riduzione al minimo;
- la riduzione dei rischi alla fonte;
- la programmazione della prevenzione che integri in modo coerente le condizioni tecniche, produttive e organizzative nonché l'influenza dei fattori dell'ambiente di lavoro;
- la sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
- la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale.

These crucial success factors for information security management commit Da Lio S.p.A. from managing such a system to an organizational approach that includes the following directives:

- compliance with legislative and contractual requirements;
- prevention and revelation of unauthorised software;
- business continuity management;
- the consequences of the breach of security policy;
- a definition of the management and specific responsibilities for the management of information security;
- the reporting of information security incidents;
- the organisational, management and operational documentation supporting the information security policy;
- the provision in an appropriate form, accessible and comprehensible to operators and users, of security directives and procedures;
- systematic and periodic risk assessment as a preventive activity;
- the elimination of risks in relation to knowledge acquired as a result of technical progress and, where this is not possible, their reduction to a minimum;
- reduction of risks at their source;
- prevention planning that coherently integrates technical, production and organisational conditions as well as the influence of the factors of the working environment;
- the replacement of what is dangerous by what is not, or what is less dangerous;
- the priority of collective protection measures over individual protection measures.

Noale, 15/09/2023
La Direzione Generale
General Management

VALIDITA' / VALIDITY

Il presente documento aziendale è valido immediatamente dopo la pubblicazione.
This Company Document is valid immediately after publication.

La Politica della sicurezza delle Informazioni è verificata annualmente in sede di Riesame di Direzione.
The Information Security Policy is verified annually during the Management Review.