# POLITICA INTEGRATA DELLA QUALITA' E DELLA SICUREZZA DELLE INFORMAZIONI

## Motivazione

MADISOFT S.P.A., data la natura delle proprie attività, considera la qualità e la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

Per quanto riguarda la qualità, essa costituisce il riferimento generale per la gestione di tutte le attività aventi influenza sui processi dell'Organizzazione. Tutto il Personale è tenuto a basare le proprie attività sui principi contenuti nella presente politica in un'ottica di continuo miglioramento tecnico, economico e qualitativo.

Attraverso l'impostazione del Sistema Garanzia Integrato, in conformità alle norme UNI EN ISO 9001 e serie di norme ISO 27001, vogliamo migliorare la nostra immagine in materia di qualità e sicurezza delle informazioni, le performance aziendali e le relazioni con i nostri stakeholder. Con la Certificazione del Sistema di Gestione Integrato da parte di un Istituto accreditato a livello internazionale vogliamo inoltre dare garanzia a tutti i Clienti delle nostre capacità di erogare dei servizi di elevato standard sia in termini qualitativi che di sicurezza delle informazioni.

La direzione svolge direttamente il ruolo di Rappresentante della Direzione

## Obiettivi

L'obiettivo del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni di MADISOFT S.P.A. è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali, attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Inoltre, la Direzione ha fissato i seguenti obiettivi generali:

- disporre di un'organizzazione certificata;
- migliorare continuamente la soddisfazione dei Clienti e le aspettative degli Stakeholder;
- coinvolgere creativamente ed organizzativamente il Personale
- rispettare le norme applicabili sia di natura cogente che volontaria
- disporre di un parco fornitori affidabili ed efficienti;
- migliorare continuamente i processi di erogazione del servizio;
- disporre di indicatori di monitoraggio che permettano di misurare periodicamente il grado di soddisfacimento degli obiettivi suddetti, anche in ottica di miglioramento continuo.

Il Sistema di Gestione Integrato per la Sicurezza delle Informazioni definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi

- Integrità, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi
- Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi

Inoltre, con la presente Politica, MADISOFT S.P.A. intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- ✔ preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competitivo
- ✔ proteggere il proprio patrimonio informativo
- ✔ evitare al meglio ritardi nella delivery
- ✔ adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione
- ✔ rispondere pienamente alle indicazioni della normativa vigente e cogente
- ✔ aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza

## Contenuto della Politica

Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione, ai servizi e ai dati ad esse collegate: tutte le informazioni che vengono create o utilizzate da MADISOFT S.P.A. sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito della progettazione e sviluppo, tale sistema prevede – in conformità alla NORMA ISO/IEC 27001:2017 - che il Responsabile per la Sicurezza della Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente Politica, degli incidenti eventualmente occorsi e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate. La Direzione condivide con il Responsabile della Sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella relazione della metodologia, la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio. In seguito alla elaborazione dell'analisi dei rischi, la Direzione valuta i risultati ottenuti accettando la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere, classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il

budget a disposizione e la necessità di mantenere la conformità alle norme e alle leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

## Responsabilità

Tutto il Personale di che, a qualsiasi titolo, collabora con MADISOFT S.P.A. è responsabile dell'osservanza di questa policy e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

## Comitato della Sicurezza delle Informazioni

Viene istituito un comitato della sicurezza che si incontrerà con cadenza almeno semestrale. È composto, in forma stabile, dalla Direzione e dal responsabile della Sicurezza delle Informazioni. Ha il compito di fissare gli obiettivi, assicurare un indirizzo chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza coerentemente alle politiche e alle linee strategiche aziendali.

Responsabile della Sicurezza delle Informazioni: si occupa della progettazione del Sistema di Gestione per la Sicurezza delle informazioni e, in particolare di:

- ✔ emanare tutte le procedure necessarie, ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- ✔ adottare criteri e metodologie per l'analisi e la gestione del rischio;
- ✔ suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di MADISOFT S.P.A.;
- ✔ pianificare un percorso formativo, specifico e periodico in materia di sicurezza delle informazioni per il personale;
- ✔ 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 MADISOFT S.P.A. devono garantire il rispetto dei requisiti di sicurezza esplicitati nella presente Politica per la Sicurezza, anche attraverso la sottoscrizione di un "Patto per la Riservatezza" all'atto del conferimento del conferimento d'incarico (quando questo tipo di vincolo non sia espressamente citato negli accordi).

## Applicabilità

La presente Politica si applica indistintamente a tutti gli organi dell'azienda. La sua attuazione è obbligatoria per il personale e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsivoglia titolo, possa venire a conoscenza delle informazioni gestite in azienda.

MADISOFT S.P.A. 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.

## Riesame

MADISOFT S.P.A. verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo che controlli il variare delle condizioni o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

Pollenza, lì 02.01.2020

**Il Direttore Generale**