1. DICHIARAZIONE DELLA DIREZIONE

Master Soft S.r.l. ritiene che la qualità dei prodotti e servizi offerti, la sicurezza e l'efficacia dei dispositivi medici, la sicurezza delle informazioni e la protezione dei dati personali siano elementi fondamentali della propria strategia aziendale e fattori distintivi nel mercato dei servizi IT e del software.

A tal fine, l'azienda ha implementato e si impegna a mantenere efficiente un Sistema di Gestione Integrato (SGI) conforme alle norme:

2. CONTESTO E CAMPO DI APPLICAZIONE

Master Soft S.r.l. è una società IT che offre servizi informatici a clienti pubblici e privati, specializzata nella progettazione, sviluppo e realizzazione di software, nell'erogazione di servizi cloud in modalità SaaS e nel servizio di conservazione a norma.

Il Sistema di Gestione Integrato si applica ai seguenti ambiti:

ISO 9001:2015:

- Servizio di progettazione, codifica, realizzazione e test di sistemi software destinati alle imprese e al settore sanitario e biomedicale, Web e Web APP
- Servizi di progettazione e gestione di sistemi server, web farm, IT&C

ISO 13485:2016:

- Servizio di progettazione, codifica, realizzazione e test di sistemi software destinati alle imprese e al settore sanitario e biomedicale

ISO/IEC 27001 con estensioni ISO/IEC 27017 e ISO/IEC 27018:

- Progettazione e sviluppo di software
- Servizi di consulenza e assistenza ITC
- Erogazione di servizi cloud relativi a software gestionali e conservazione a norma in modalità SaaS

3. IMPEGNI DELLA DIREZIONE

La Direzione di Master Soft S.r.l. è responsabile dell'istituzione, del mantenimento e del miglioramento continuo del Sistema di Gestione Integrato. Essa fornisce il quadro per la definizione degli obiettivi, stabilisce i principi di azione in materia di qualità e sicurezza e garantisce il massimo impegno per la protezione dei dati, nel rispetto della legislazione vigente applicabile.

Nel rispetto degli obiettivi strategici aziendali, la Direzione si impegna a:

- Leadership proattiva nella promozione del miglioramento continuo della qualità, della sicurezza dei dispositivi medici e della sicurezza delle informazioni;
- Responsabilizzazione di tutte le funzioni aziendali nell'applicazione del SGI e nella protezione degli asset informativi;
- Conformità normativa scrupolosa alle leggi, ai regolamenti applicabili, agli impegni contrattuali e ai requisiti correlati, con particolare attenzione a: GDPR, Regolamento (UE) 2017/745 (MDR), IEC 62304, ISO 14971 e normativa sulla Conservazione a Norma;
- Valutazione preventiva e continua dei rischi per la qualità, la sicurezza dei dispositivi medici e la sicurezza delle informazioni in ogni processo decisionale, assicurando il bilanciamento tra: rischio di impresa, sostenibilità economica, risultati delle analisi e valutazione del rischio, politiche aziendali e strategie di fornitori e clienti;
- Formazione e sensibilizzazione del personale sui requisiti del SGI e consapevolezza del contributo individuale al conseguimento dei risultati;
- Selezione accurata di fornitori e partner che garantiscano comportamenti corretti e livelli di qualità e sicurezza adeguati;
- Protezione delle informazioni garantendo riservatezza, integrità e disponibilità attraverso controlli appropriati e proporzionati ai rischi identificati;

- Monitoraggio costante dell'applicazione della politica, del conseguimento degli obiettivi e dell'efficacia del Sistema di Gestione;
- Miglioramento continuo dell'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), conformemente ai requisiti della norma ISO/IEC 27001:2022.

4. ISO 9001 – QUALITÀ

Master Soft S.r.l. ha aderito volontariamente allo schema di certificazione ISO 9001 per garantire un continuo monitoraggio delle prestazioni e un aggiornamento costante delle procedure operative.

Obiettivi principali:

- Sviluppo ed erogazione di soluzioni software conformi ai requisiti dei clienti e alle normative vigenti;
- Rispetto delle tempistiche di progetto e degli SLA concordati;
- Formazione continua del personale tecnico sulle tecnologie emergenti e sulle best practice di sviluppo;
- Utilizzo di metodologie, strumenti e infrastrutture tecnologiche di eccellenza;
- Selezione di fornitori qualificati secondo standard elevati;
- Mantenimento di elevati livelli di soddisfazione del cliente attraverso supporto tecnico efficace e tempestivo;
- Riduzione delle non conformità e miglioramento continuo dei processi.

5. ISO 13485 – DISPOSITIVI MEDICI

Master Soft S.r.l. riconosce la responsabilità derivante dallo sviluppo di software classificati come dispositivi medici e si impegna a garantire la sicurezza e l'efficacia dei propri prodotti.

Obiettivi principali:

- Progettazione e sviluppo di software medicali conformi al Regolamento (UE) 2017/745 (MDR) e alla norma IEC 62304;
- Applicazione sistematica della gestione del rischio secondo ISO 14971 lungo tutto il ciclo di vita del prodotto;
- Garanzia della tracciabilità completa dei prodotti e dei componenti software;
- Prevenzione degli incidenti di sicurezza che possano compromettere la salute dei pazienti e gestione tempestiva in caso di occorrenza;
- Sorveglianza post-market efficace e gestione tempestiva di reclami e segnalazioni;
- Mantenimento della documentazione tecnica conforme ai requisiti regolamentari;
- Validazione rigorosa dei processi software e verifica della conformità ai requisiti specificati.

6. ISO/IEC 27001 – SICUREZZA DELLE INFORMAZIONI

Master Soft S.r.l. tratta dati pubblici e riservati, dati anonimi, personali comuni e/o particolari ai sensi dell'art. 9 GDPR. È fondamentale garantire la massima sicurezza delle informazioni in qualunque formato, assicurandone riservatezza, integrità e disponibilità.

L'approccio alla sicurezza delle informazioni è basato sul rischio, conformemente alla norma ISO 27001 e alle migliori pratiche. Nella valutazione dei rischi, l'azienda considera i fattori esterni ed interni pertinenti alle proprie finalità e gli obblighi commerciali, giuridici, regolamentari e contrattuali. Devono essere sempre garantiti livelli di sicurezza che assicurino il bilanciamento tra rischio di impresa, sostenibilità economica, risultati delle analisi e valutazione del rischio, politiche e strategie aziendali, politiche e strategie dei fornitori e dei clienti, e necessità di costante adeguamento al contesto.

Principi cardine:

- Le informazioni devono essere accessibili solo a chi ne ha necessità (principio need to know), nei tempi e nelle modalità stabiliti;
- Il personale deve essere opportunamente formato in materia di sicurezza delle informazioni e seguire i principi etici e comportamentali prescritti;

- I fornitori devono essere tenuti sotto controllo attraverso misure adeguate al contesto;
- I partner devono essere selezionati anche per la capacità di conformarsi alle regole di sicurezza aziendali;
- I requisiti di sicurezza devono essere considerati sin dalla fase di progettazione dei servizi.

Obiettivi principali:

- Protezione della riservatezza delle informazioni dei clienti, dei dati di progetto e del know-how tecnologico;
- Garanzia dell'integrità dei sistemi, del codice sorgente e delle configurazioni;
- Assicurazione della disponibilità dei servizi secondo gli SLA definiti;
- Identificazione, valutazione e trattamento sistematico dei rischi per la sicurezza;
- Gestione tempestiva ed efficace degli incidenti di sicurezza;
- Garanzia della continuità operativa attraverso piani di disaster recovery e business continuity;
- Promozione di una cultura della sicurezza attraverso programmi di awareness e formazione continua;
- Adozione di pratiche di sviluppo sicuro (secure coding);
- Verifica periodica dell'efficacia dei controlli attraverso audit e vulnerability assessment.

7. ISO 27017 E ISO 27018 – SICUREZZA E PRIVACY NEI SERVIZI CLOUD

Master Soft S.r.l., in qualità di fornitore di servizi cloud (SaaS), si impegna a implementare controlli specifici per la sicurezza delle informazioni e la protezione dei dati personali trattati nelle proprie piattaforme cloud.

Impegni specifici:

- Definizione chiara delle responsabilità tra fornitore e cliente del servizio cloud;
- Implementazione di controlli di sicurezza specifici per l'ambiente cloud;
- Protezione dei dati personali (PII) conformemente al GDPR e alle best practice internazionali;
- Trasparenza verso i clienti sulle misure di sicurezza adottate;
- Garanzia della localizzazione e del trattamento dei dati secondo i requisiti normativi e contrattuali;
- Gestione sicura della cessazione del servizio e della restituzione/cancellazione dei dati;
- Limitazione delle finalità: i dati personali (PII) del cliente vengono trattati esclusivamente per gli scopi contrattuali concordati e non per finalità proprie del fornitore cloud;
- Garanzia dei diritti degli interessati: accesso, rettifica e cancellazione dei propri dati personali su richiesta del cliente cloud;
- Notifica tempestiva al cliente cloud in caso di violazione dei dati personali (data breach) che coinvolga PII, conformemente ai requisiti normativi applicabili.

8. COMUNICAZIONE E RIESAME

La presente Politica è:

- Comunicata a tutto il personale attraverso affissione in bacheca, pubblicazione nella intranet aziendale e momenti formativi;
- Resa disponibile alle parti interessate su richiesta e pubblicata sul sito web aziendale;
- Riesaminata almeno annualmente in occasione del Riesame della Direzione, o in seguito a cambiamenti significativi del contesto interno o esterno, al fine di garantirne la continua idoneità e adeguatezza.

La Direzione si impegna ad attuare, sostenere e verificare periodicamente la Politica sopra esposta e a fornire le risorse necessarie per il conseguimento degli obiettivi stabiliti.

9. GESTIONE DOCUMENTALE

Il presente documento viene riesaminato periodicamente, almeno una volta all'anno, e viene conservato per un periodo di 10 anni.