



# **MA Provider S.r.l. a socio unico**

**Via Giosuè Carducci, 24 - Milano**

## **POLITICA PER LA SICUREZZA DELLE INFORMAZIONI**

Codice:	D.04.01
Versione:	1
Data della versione:	10/12/2016
Creato da:	Luca Oldrini
Approvato da:	Elena Lanati
Livello di confidenzialità:	Pubblico

## Cronologia delle modifiche

Data	Versione	Descrizione delle modifiche
10/12/2016	1	Prima versione

## Sommario

<b>1. SCOPO, AMBITO E DESTINATARI</b> .....	<b>3</b>
<b>2. RIFERIMENTI</b> .....	<b>3</b>
<b>3. TERMINOLOGIA DI BASE PER LA SICUREZZA DELLE INFORMAZIONI</b> .....	<b>3</b>
<b>4. GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI</b> .....	<b>3</b>
4.1. OBIETTIVI E VALUTAZIONE .....	3
4.2. REQUISITI DELLA SICUREZZA DELLE INFORMAZIONI .....	4
4.3. CONTROLLI DELLA SICUREZZA DELLE INFORMAZIONI .....	4
4.4. BUSINESS CONTINUITY .....	4
4.5. RESPONSABILITÀ .....	4
4.6. COMUNICAZIONE .....	5
<b>5. SUPPORTO PER L'IMPLEMENTAZIONE DEL SGSI</b> .....	<b>5</b>
<b>6. VALIDITÀ E GESTIONE DEL DOCUMENTO</b> .....	<b>5</b>

## 1. Scopo, ambito e destinatari

Lo scopo di questa politica di alto livello è quello di definire le finalità, la direzione, i principi e le regole di base per la gestione della sicurezza delle informazioni.

Questa politica si applica a tutto il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), come definito nel documento Campo di Applicazione del SGSI.

Gli utenti di questo documento sono tutti i dipendenti di MA Provider, come pure le parti esterne interessate nel campo di applicazione.

## 2. Riferimenti

- ISO/IEC 27001 standard, punto 5.2 and 5.3
- Campo di Applicazione del SGSI
- Valutazione del rischio e metodologia di trattamento
- Appendice A della ISO/IEC 27001:2013
- D.Lgs. 196/2003
- Politica per la business continuity
- Procedure per la gestione degli incidenti

## 3. Terminologia di base per la sicurezza delle informazioni

**Riservatezza** - caratteristica riferita a informazioni disponibili solo per le persone o i sistemi autorizzati.

**Integrità** - caratteristica riferita a informazioni che sono modificate solo da persone autorizzate o da sistemi in modo autorizzato.

**Disponibilità** - caratteristiche riferite a informazioni accessibili e rintracciabili da personale autorizzato solo quando è necessario.

**Sicurezza delle informazioni** – tutela della riservatezza, integrità e disponibilità delle informazioni.

**Informazioni sul sistema di gestione della sicurezza** - parte dei processi di gestione complessivi che si occupa di progettazione, realizzazione, manutenzione, revisione e miglioramento della sicurezza delle informazioni.

## 4. Gestione della sicurezza delle informazioni

### 4.1. Obiettivi e valutazione

L'obiettivo di MA Provider nello sviluppo del SGSI è fornire un livello di protezione adeguato alle informazioni gestite nell'ambito del processo di RWE, commisurato ai rischi identificati, valutati e considerati dal processo di analisi dei rischi che è parte integrante del SGSI.

Le attività di RWE svolte da MA Provider si distinguono in raccolta ed analisi di dati di tipo clinico, farmacologico ed economico. Tali dati possono essere raccolti in formato elettronico o cartaceo (trasformati poi in formato elettronico). Ai fini della raccolta e dell'analisi dei dati, la funzione

principale è un portale web con funzioni da data entry manuale o automatico mediante file di raccolta, disponibili per l'analisi.

Gli obiettivi della politica per la sicurezza delle informazioni sono:

- Consolidare l'immagine dell'azienda quale gestore di dati affidabile e competente;
- Proteggere il proprio patrimonio informativo collegato alle attività di RWE;
- Ottenere un vantaggio competitivo su altri soggetti di mercato che erogano servizi simili evidenziando il valore delle informazioni per MA Provider;
- Evitare, per quanto possibile, disservizi agli utenti del Portale RWE;
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza;
- Il miglioramento continuo dell'idoneità, adeguatezza ed efficacia del sistema di gestione per sicurezza delle informazioni.

#### **4.2. Requisiti della sicurezza delle informazioni**

I requisiti considerati nella sicurezza delle informazioni oggetto del SGSI sono quelli relativi a:

- Obblighi normativi di carattere generale quali Leggi sulla Protezione dei dati personali;
- Obblighi normativi specifici collegati al settore medicale o clinico;
- Obblighi eventualmente previsti nei contratti con i clienti.

#### **4.3. Controlli della sicurezza delle informazioni**

Il processo di selezione dei controlli (controlli di sicurezza) è definito nella valutazione del rischio e nella metodologia di trattamento del rischio.

I controlli selezionati e il loro stato di attuazione sono elencati nella Dichiarazione di Applicabilità.

#### **4.4. Business Continuity**

Dato che il Campo di Applicazione del SGSI riguarda un insieme di processi di raccolta dati, effettuata attraverso portale web esposto verso soggetti esterni, è data grande importanza alla continuità del servizio che gli utenti devono utilizzare per effettuare operazioni di caricamento dati. Per questo motivo è stato implementato un sistema che garantisce la continuità di servizio in caso di problematiche di vario livello.

#### **4.5. Responsabilità**

Le responsabilità per la gestione del SGSI sono le seguenti:

- La direzione approva la seguente Politica sulla sicurezza delle informazioni; mette a disposizione le risorse per l'implementazione della politica e del relativo sistema di gestione, rivede il SGSI almeno una volta l'anno o ogni volta che si verifica un cambiamento significativo, rendicontando attraverso specifico verbale tale attività. Esegue, inoltre, il riesame della direzione che ha come scopo l'idoneità, l'adeguatezza e l'efficacia del SGSI.

- Il responsabile del SGSI è responsabile di assicurare che il SGSI venga applicato e mantenuto in base a questa politica e di garantire che tutte le risorse necessarie siano disponibili.
- Il responsabile del SGSI è responsabile del coordinamento operativo del SGSI, nonché della valutazione circa le performance del SGSI.
- L'amministratore di sistema è responsabile per le attività tecniche operative inerenti la gestione del SGSI.
- Il responsabile del SGSI implementerà la formazione sulla sicurezza delle informazioni e programmi di sensibilizzazione per i dipendenti.
- Tutti gli incidenti di sicurezza devono essere segnalati al responsabile del SGSI.
- Il responsabile del SGSI è responsabile per l'adozione e l'attuazione del Piano di formazione e sensibilizzazione, che si applica a tutte le persone che hanno un ruolo nella gestione della sicurezza delle informazioni.

#### **4.6. Comunicazione**

La presente politica per la sicurezza delle informazioni deve essere comunicata a tutto il personale interno di MA Provider mediante invio annuale da parte del Responsabile del SGSI.

### **5. Supporto per l'implementazione del SGSI**

La Direzione di MA Provider fa propria la volontà di raggiungere gli obiettivi definiti dalla presente politica e si impegna a fornire le risorse necessarie. Tali risorse sono condivise e definite insieme al Responsabile del SGSI.

### **6. Validità e gestione del documento**

Questo documento è valido a partire dal 10/12/2016.

Il responsabile di questo documento è il Responsabile del SGSI, che deve controllare e, se necessario, aggiornare il documento, almeno una volta all'anno.

Quando si valuta l'efficacia e l'adeguatezza del presente documento, i seguenti criteri devono essere considerati:

- Numero di dipendenti e soggetti esterni che hanno un ruolo nel SGSI, ma che non hanno familiarità con questo documento.
- Il mancato rispetto nel SGSI di leggi e regolamenti, obblighi contrattuali e altri documenti interni dell'organizzazione.
- Inefficacia nell'implementazione e manutenzione del SGSI.
- Responsabilità poco chiare per l'attuazione del SGSI.

Managing Director  
Elena Lanati

Responsabile del SGSI  
Luigi Orlando

[firma]

[firma]