AAMPS S.p.A. Information Security Policy

ISO27001 sec. 5.2

L' Organo Amministrativo e il management di AAMPS S.p.A., situata in Via dell' Artigianato, 39/B, 57121 Livorno LI, società in house che eroga tutti i servizi connessi alla gestione del ciclo integrato dei rifiuti e alla pulizia stradale nel Comune di Livorno, si impegnano a preservare la riservatezza, l'integrità e la disponibilità di tutte le risorse informative fisiche ed immateriali in tutta la loro organizzazione al fine di mantenere econsolidare il vantaggio competitivo, il fatturato, la redditività, la conformità legale, normativa e contrattuale e l'immagine commerciale. Le informazioni e i requisiti di sicurezza delle informazioni continueranno ad essere allineati agli obiettivi di AAMPS S.p.A. e l'ISMS (Information SecurityManagement System) costituisce la metodologia abilitante per la condivisione delle informazioni, in qualunque forma, digitale, analogica, cartacea, e per ridurre i rischi correlati alle operazioni connesse, a livelli accettabili.

L' attuale piano strategico aziendale e il quadro di gestione dei rischi di AAMPS S.p.A. forniscono il contesto per identificare, accertare, valutare e controllare i rischi legati alle informazioni attraverso l'istituzione e il mantenimento di proprio ISMS. Il Piano di valutazione del rischio, la dichiarazione di applicabilità e il piano di trattamento del rischio identificano il modo in cui i rischi correlati alle informazioni sono controllati. Il

Responsabile del Rischio è responsabile della gestione e della manutenzione del piano di trattamento del rischio. Ulteriori valutazioni del rischio possono, ove necessario, essere eseguite per determinare controlli adeguati per rischi specifici.

In particolare, i piani di Business Continuity e di Contingency, le procedure di backup dei dati, la prevenzione di Virus e Hacker Intrusion (Penetration), il controllo degli accessi ai sistemi e la segnalazione degli incidenti di sicurezza delle informazioni sono fondamentali per questa politica. Gli obiettivi di controllo per ciascuna di queste aree sono contenuti in nella sezione 6 della documentazione relativa e sono supportati da specifiche politiche e procedure documentate.

AAMPS S.p.A. mira a raggiungere obiettivi specifici e definiti di sicurezza delle informazioni, che sono sviluppati in conformità con gli obiettivi aziendali, il contesto dell'organizzazione, i risultati delle valutazioni del rischio e il piano di trattamento del rischio.

Tutti i Dipendenti di AAMPS S.p.A. e alcuni soggetti esterni identificati nell'ISMS sono tenuti a rispettare questa politica e l'ISMS che implementa questa politica. Tutti i Dipendenti, e alcune parti esterne riceveranno una formazione adeguata. Le conseguenze della violazione della politica di sicurezza delle informazioni sono stabilite nella politica disciplinare e nei contratti e accordi con terzi.

L'ISMS è soggetto a revisioni e miglioramenti continui e sistematici.

AAMPS S.p.A. ha definito il "Gruppo per la sicurezza delle informazioni", presieduto dal Responsabile dei sistemi Informativi (CISO) che include il Responsabile per la Sicurezza delle Informazioni e il Responsabile delle HR per supportare il framework ISMS e rivedere periodicamente la politica di sicurezza.

AAMPS S.p.A. si impegna a conseguire la certificazione del proprio ISMS secondo ISO27001: 2013.

Questa policy sarà riesaminata per rispondere a eventuali cambiamenti nella valutazione del rischio o piano di trattamento del rischio e almeno una volta all'anno.

In questa Policy, la 'sicurezza delle informazioni' è definita come:

Preservare

Ciò significa che il management tutto, i Dipendenti, permanenti e temporanei, i sub-contractor, i consulenti ed ogni altra entità esterna, sono e saranno informati delle loro responsabilità (definiti nei mansionari o nei contratti di lavoro) per preservare la sicurezza delle informazioni, segnalare violazioni della sicurezza e agire in conformità ai requisiti dell'ISMS. Tutti i Dipendenti riceveranno formazione sulla sicurezza delle informazioni mentre alcuni Dipendenti più specializzati riceveranno una formazione specifica sulla sicurezza delle informazioni.

La Disponibilità

Ciò significa che le informazioni e le risorse associate dovrebbero essere accessibili agli utenti autorizzati quando richiesto e quindi fisicamente sicuro. La rete di computer deve essere resiliente e AAMPS S.p.A. deve essere in grado di rilevare e rispondere rapidamente a incidenti (come virus e altri malware) che minacciano la continua disponibilità di risorse, sistemi e informazioni. Devono esserci piani di continuità operativa adeguati.

La Confidenzialità

Ciò implica garantire che le informazioni siano accessibili solo a coloro che sono autorizzati ad accedervi e quindi a impedire sia l'accesso non autorizzato deliberato e accidentale alle informazioni di AAMPS S.p.A. i suoi sistemi comprese le sue reti, siti web, extranet e sistemi di e-commerce.

L'Integrità

Ciò implica la salvaguardia dell'accuratezza e della completezza delle informazioni e dei metodi di elaborazione e, pertanto, richiede la prevenzione di modifiche intenzionali o accidentali, parziali o complete, distruzione o modifica non autorizzata, di beni materiali o di dati elettronici. Devono esserci contingenze appropriate *[comprese reti, sistemi di e-commerce, siti Web, extranet (s)]* e piani di backup dei dati e rapporti sugli incidenti di sicurezza.

degli asset fisici

Gli asset fisici di AAMPS S.p.A. inclusi, hardware, cablaggi, sistemi telefonici, sistemi di archiviazione e file di dati fisici.

e di tutto il patrimonio informativo

Le risorse informative includono informazioni stampate o scritte su carta, trasmesse per posta o contenute in filmati o parlate, nonché informazioni memorizzate elettronicamente su server, siti Web, extranet, intranet, PC, laptop, telefoni cellulari e PDA, nonché su CD-ROM, floppy disk, penne USB, nastri di backup e altri supporti digitali o magnetici e informazioni trasmesse elettronicamente con qualsiasi mezzo. In questo contesto, i "dati" includono anche la serie di istruzioni che indicano al sistema come manipolare le informazioni (cioè il software: sistemi operativi, applicazioni, utilità, ecc.).

di AAMPS S.p.A.

AAMPS S.p.A. e tutti i partner che fanno parte della nostra rete integrata e hanno aderito alla nostra politica di sicurezza e hanno accettato il nostro ISMS.

L' ISMS è il sistema di gestione della sicurezza delle informazioni, di cui questa politica e altra documentazione di supporto e relativa è parte e che è stato progettato in conformità con le specifiche contenute nella norma ISO 27001: 2013.

Una **VIOLAZIONE DELLA SICUREZZA** è qualsiasi incidente o attività che causa, o può causare, una interruzione nella disponibilità, riservatezza o integrità delle risorse informative fisiche o elettroniche di AAMPS S.p.A..

Titolare del documento e Approvazione

Il Responsabile per la Sicurezza delle Informazioni è il proprietario di questo documento ed è responsabile di garantire che questa procedura venga riesaminata in linea con i requisiti di revisione del ISMS.

Una versione corrente di questo documento è disponibile per tutti i membri dello staff sulla intranet aziendale

Questa procedura è stata approvata dall' the Amministratore Unico il *9/11/2021* ed è rilasciata in versione controllata sotto la sua firma.

Firma: Data:9/11/2021

Cronologia delle Modifiche

Versione	Descrizione delle Modifiche	Approvazione	Data di Emissione
1	Versione inziale	<Manager>	9/11/2021