

Politica della sicurezza delle informazioni

MATRICE DI REVISIONE		
Rev. 3 del 10/03/2021		FIRMA
<i>Redatto da RSGSI: (S. Minucci)</i>		
<i>Verificato da DPO: (C. Mancino)</i>		
<i>Approvato da AU: (G. Tarallo)</i>		
data	Rev.	Descrizione e motivazioni della revisione
22/10/2017	0	Prima emissione
16/01/2018	1	Inseriti par. 3.1 -3.2 -3.3
15/06/2020	2	Revisioni minori
10/03/2021	3	Revisione generale

COPIA N.	ASSEGNATA A			
DISTRIBUZIONE CONTROLLATA	<input checked="" type="checkbox"/> SI		<input type="checkbox"/> NO	
LIVELLO	<input type="checkbox"/> AA (riservato)	<input type="checkbox"/> A (sensibile)	<input checked="" type="checkbox"/> M (confidenziale)	<input type="checkbox"/> B (pubblico)

INDICE

1	SCOPO	3
2	DESCRIZIONE	3
3	AMBITO DI APPLICAZIONE.....	4
3.1	SICUREZZA DELLE INFORMAZIONI NELLE RELAZIONI CON I FORNITORI.....	4
3.2	SICUREZZA DELLE INFORMAZIONI SVILUPPO DEL SOFTWARE.....	5
3.3	SISTEMI E PROCEDURE DI BACKUP E RESTORE DEI DATI	5
4	POLITICA PER LA SICUREZZA DELLE INFORMAZIONI.....	5
5	RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI.....	7

1 Scopo

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da ASMENET al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

2 Descrizione

Per ASMENET la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'ISMS, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architettonici associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione.
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

Nell'ambito della gestione dei servizi offerti da ASMENET, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione dell'ISMS, assicura:

- la garanzia di aver incaricato un partner affidabile al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale;
- la completa osservanza delle Service Level Agreement stabilite, ove previsto, con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza.

Per questo motivo ASMENET ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001-e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

3 Ambito di Applicazione

La politica per la sicurezza delle informazioni di ASMENET si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

3.1 Sicurezza delle Informazioni nelle Relazioni con i fornitori

ASMENET assicura attraverso la sua politica di sicurezza delle informazioni la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.

I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori sono concordati con i fornitori stessi e documentati nei documenti contrattuali.

Tutti i requisiti relativi alla sicurezza delle informazioni sono stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire informazioni e/o componenti dell'infrastruttura IT dell'organizzazione.

Gli accordi con i fornitori includono i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni e delle comunicazioni dei servizi e prodotti inclusi nella filiera di fornitura dei servizi Asmenet.

ASMENET ricorre unicamente a fornitori che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, nominando questi ultimi, ove previsto, responsabili del trattamento dei dati personali, come prescritto dall'art. 28 del Regolamento (UE) 2016/679.

ASMENET verifica l'attuazione degli accordi con i fornitori per mantenere un livello concordato di sicurezza delle informazioni ed erogazione dei servizi; monitorizza, riesamina e sottopone ad audit l'erogazione dei servizi da parte dei fornitori, relativamente al rispetto dei requisiti di sicurezza delle informazioni nella fornitura, ove applicabili.

I cambiamenti alla fornitura dei servizi da parte dei fornitori vengono gestiti tenendo conto della criticità delle informazioni, dei sistemi e dei processi coinvolti, basandosi su di una costante rivalutazione dei rischi.

La presente Politica per la sicurezza delle Informazioni viene condivisa con i fornitori esterni che si impegnano a rispettarla ed attuarla così come riportato nei documenti contrattuali.

3.2 Sicurezza delle Informazioni Sviluppo del Software

Al fine di assicurare la sicurezza delle Informazioni e definire le responsabilità e le modalità operative del processo di sviluppo dei sistemi informativi, ASMENET ha emesso un documento specifico di Politica di Sviluppo Software con l'obiettivo di rappresentare, descrivere e schematizzare il flusso procedurale e le fasi che costituiscono il ciclo di vita degli elementi dei sistemi informativi, gestiti attraverso la gestione delle "Change Request", ovvero di una Richiesta di Sviluppo Software per soddisfare un Requisito di Business o Normativo.

Tale Politica di Sviluppo Software si applica a tutto il personale interno di ASMENET e alle terze parti (inclusi i fornitori esterni) che accedono ai sistemi informativi gestiti dalla Funzione ICT di ASMENET, per quanto compatibile ed in relazione alle peculiarità e alle dimensioni delle Società ed in coerenza con i vincoli normativi e regolatori dello specifico business (***rif. documento Politica per lo sviluppo dei Software***)

3.3 Sistemi e procedure di backup e restore dei dati

ASMENET ha definito la propria Politica per l'attuazione delle procedure di backup e restore dei dati, nel rispetto del Regolamento sulla protezione dei dati personali e la libera circolazione dei dati personali (Reg. UE 679/2016 GDPR) ed alle Linee Guida Agid.

Tra le misure minime da adottare vi è certamente la realizzazione di un sistema di backup dei dati in formato elettronico, efficace e funzionale, in grado di offrire reali garanzie nella gestione di situazioni critiche che potrebbero sorgere in corrispondenza di crash di sistemi con conseguenti perdite di dati.

La ASMENET ha investito risorse e mezzi nell'adozione di standard operativi e tecnici con l'obiettivo di ottenere risultati concreti ed efficaci in termini di sicurezza dei dati.

A tal fine è stato emesso ed approvato il documento ***Sistemi e procedure di Backup e Restore dei dati allegato alla presente Politica e considerato parte integrante della stessa.***

4 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di ASMENET rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di ASMENET si ispira ai seguenti principi:

- a) Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- b) Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- c) Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.

- d) Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- e) Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- f) Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- g) Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- h) Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- i) Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

La politica della sicurezza delle informazioni e viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.


L'impegno della direzione si attua tramite la definizione di una struttura organizzativa adeguata a:

- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che le procedure e i controlli siano sviluppati efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza delle informazioni.

La Direzione è impegnata per:

- attuare, sostenere e verificare periodicamente la presente Politica, a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa;
- garantire le risorse necessarie per l'efficace protezione delle informazioni;
- definire gli obiettivi in materia di sicurezza delle informazioni;
- riesaminare periodicamente gli obiettivi e la Politica per la sicurezza delle informazioni per accertarne la continua idoneità.

Tutto il personale interno ed esterno deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni. L'applicazione del sistema di gestione richiede pertanto piena partecipazione, impegno ed efficace interazione di tutte le risorse umane e tecnologiche. La continua crescita del livello di servizio verrà perseguita mediante il regolare riesame dello stesso,

	Politica della sicurezza delle informazioni	
	Cod. ALL. 01 MSGI REV. 3 del 10/03/2021	Pag. 7 di 7

volto al monitoraggio degli obiettivi prestabiliti e al riconoscimento di eventuali aree di miglioramento.

5 RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
 - nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
 - significativi incidenti di sicurezza;
 - evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;
-