SEISMIX

Gestione e prevenzione dei rischi in materia di sicurezza informatica

Palermo, 26 Giugno 2023	Il Legale Rappresentante
	Stefano Limonta

Seismix s.r.l. P.I.: 06888470827
Via Briuccia 70, 90146 Palermo
091 5556231 info@seismix.it

Sommario

1 - premessa

Scopo di questo documento è stabilire le misure di sicurezza adottate da SEISMIX SRL al fine di rispettare gli obblighi previsti dal Reg. UE 2016/679 in materia di sicurezza del trattamento dei dati.

Il presente documento è stato redatto dal Sig. Stefano Limonta in qualità di Amministratore SEISMIX SRL, che provvede a firmarlo in calce.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

2 –Normativa di riferimento

Reg. UE 2016/679

3 -definizioni e responsabilità

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

AMMINISTRATORE DI RETE: il soggetto cui è conferito il compito di sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza l'amministratore di rete ha le responsabilità indicate nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI PARTICOLARI: i dati personali idonei a rivelare l'origine etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti,

sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è il signor Stefano Limonta. La titolarità è esercitata dal rappresentante legale, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

4 – titolare, responsabili e incaricati

Titolare del trattamento: Stefano Limonta

Responsabile del trattamento dei dati: Chiara Cocorullo

Amministratore di rete: Chiara Cocorullo

Incaricati del trattamento dei dati: Elenco dipendenti

5 – analisi dei rischi

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e quindi di definire l'insieme delle possibili contromisure di sicurezza da attuare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI: la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI, ulteriormente classificabili in:
  - DATI PERSONALI SEMPLICI: classe di dati a rischio intermedio;
  - DATI PERSONALI PARTICOLARI/GIUDIZIARI: classe di dati ad alto rischio;
  - DATI PERSONALI SANITARI: classe di dati a rischio altissimo.

6 – individuazione delle risorse da proteggere

Le risorse da proteggere sono:

- personale;
- dati/informazioni;

- documenti cartacei;
- hardware;
- software;

7 – individuazione delle minacce

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi	X	X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	

Intercettazione	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Ripudio	X		
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

8 – individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che potrebbero essere sfruttate qualora si realizzasse una delle minacce.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software

	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

9 – individuazione delle contromisure

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce. Esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico
- contromisure di carattere procedurale
- contromisure di carattere elettronico/informatico.

Contromisure di carattere fisico:

- Le apparecchiature informatiche critiche e gli archivi cartacei contenenti dati personali sono situati in locali protetti da porta blindata
- i responsabili dei trattamenti indicati nel paragrafo 4 – titolare, responsabili e incaricati sono anche responsabili dell'area in cui si trovano i trattamenti

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- l'ingresso nei locali da parte di estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati.

Contromisure di carattere elettronico/informatico

Interne

La rete aziendale è gestita mediante modem Fritz!Box.

Quotidianamente viene eseguito un backup di tipo incrementale su server online tramite connessione ssh e accesso con utenti e password.

Gli utenti ssh sono gestiti dall'amministratore di rete su indicazione del titolare del trattamento.

Ogni macchina dispone di antivirus aggiornato in continuo in relazione al rilascio di nuove versioni.

Esterne

L'accesso dall'esterno è protetto da un firewall che blocca tutte le porte. Eventuali accessi sono regolamentati mediante apertura di una porta dedicata e avvengono con protocollo ssh e utente con password.

Server online

I server online di elaborazione sono gestiti dall'amministratore di rete. Tutte le porte sono chiuse tramite firewall, tranne alcune dedicate. Su queste, il traffico è consentito solo a determinati IP pubblici statici.

10 – incident response

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id
- modifica e sparizione di dati
- cattive prestazioni del sistema (così come percepite dagli utenti)
- irregolarità nell'andamento del traffico
- irregolarità nei tempi di utilizzo del sistema
- quote particolarmente elevate di tentativi di connessione falliti. In caso di incidente sono considerate le seguenti priorità:
    1. evitare danni diretti alle persone
    2. proteggere l'informazione sensibile o proprietaria
    3. evitare danni economici
    4. limitare i danni all'immagine dell'organizzazione. Garantita l'incolumità fisica alle persone si procede a:
        a. isolare l'area contenente il sistema oggetto dell'incidente
        b. isolare il sistema compromesso dalla rete
        c. spegnere correttamente il sistema oggetto dell'incidente

d. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

- se l'incidente riguarda i dati, il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide

11 – piano di formazione

La formazione degli incaricati viene effettuata all'assunzione e all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete ed aggiornamento in continuo su eventuali nuove minacce di cybersecurity;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) e correlate a problemi di sicurezza.

12 – aggiornamento del piano

Il presente piano è soggetto a revisione ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della ditta ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo della ditta tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

Il presente Documento deve essere divulgato e illustrato a tutti gli incaricati.

Palermo, 26 Giugno 2023

Il Legale Rappresentante
Stefano Limonta