Politica Generale di Gruppo del Sistema di Gestione per la Sicurezza delle Informazioni

Approvazione ed emissione	Marco Pescarmona, Alessandro Fracassi

Titolare del documento, Validità e Pubblicazione

Documento			
Classificazione[1]	Id o codice[2]	Data documento	Nome del file[3]
Pubblica	**PGSGSI**	16/03/2022	PGSGSI Politica Generale per il Sistema di Gestione per la Sicurezza delle Informazioni.docx
Versione corrente	**2022**	**Stato corrente[4]**	**Pubblicato**
Prossima revisione	Febbraio 2024		
Processo descritto	**Processo di responsabilità della direzione**		
Responsabilità processo	Marco Pescarmona, Alessandro Fracassi		

Ruoli del documento	
Ruolo	Descrizione
Titolare	**Giuseppe Spagoni (Responsabile Sistema di Gestione Gruppo MutuiOnline)**
Autore	Giuseppe Spagoni
Destinatario	**Tutta l'organizzazione**

Cronologia delle pubblicazioni			
Versione	Titolare	Data di revisione	Commento
2019	Giuseppe Spagoni	Gennaio 2019	Nuova emissione
2020	Giuseppe Spagoni	Gennaio 2020	Revisione contenuti
2021	Giuseppe Spagoni	Dicembre 2020	Revisione contenuti
2022	Giuseppe Spagoni	Marzo 2022	Aggiornamento obiettivi

Ciclo di vita		
Data di prima pubblicazione	Data di decadenza	Frequenza di revisione
Dicembre 2018	Su revoca espressa	24 mesi

[1]Pubblica, Pubblica aziendale, Riservata, Riservata sensibile, Confidenziale (PO01PP01 classificazione delle informazioni)
[2]Fare riferimento al processo di Gestione Documentale PP02 paragrafo 5.4.4
[3]Fare riferimento al processo di Gestione Documentale PP02 paragrafo 5.4.5
[4]In redazione, In approvazione, Pubblicato.

Politica Generale di Gruppo del Sistema di Gestione per la Sicurezza delle Informazioni

Le società del gruppo societario facente capo a Gruppo MutuiOnline S.p.A. (il "Gruppo MOL" o il "Gruppo") considerano i dati e le informazioni un bene fondamentale e prezioso, sia nel caso che siano di proprietà aziendale sia che appartengano a soggetti terzi, per cui viene posta la massima attenzione ed impegno nel garantire il paradigma di Riservatezza, Integrità e Disponibilità (RID) delle informazioni trattate.

Al fine di garantire la protezione del patrimonio informativo coerentemente con le scelte strategiche del Gruppo, risulta quindi fondamentale identificare in modo chiaro gli obiettivi e i principi di sicurezza in accordo con la propensione al rischio definita a livello aziendale.

Obiettivi del Sistema di Gestione

La presente Politica Generale di Gruppo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) descrive gli obiettivi e i principi generali che Gruppo MOL adotta e applica nel trattamento delle informazioni al fine di supportare i requisiti della propria offerta di servizi garantendo il rispetto di prescrizioni legali o regolamentari e l'allineamento alle strategie delineate in materia di gestione dei rischi.

Gli obiettivi definiti in questa Politica Generale sono qui delineati in termini generali e vengono tradotti in termini concreti in relazione a specifiche aree tematiche mediante obiettivi operativi nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni adottato.

Gli obiettivi di questa Politica Generale possono identificarsi nei seguenti punti, condivisi da tutte le società del Gruppo:

- Considerare la sicurezza delle informazioni elemento fondamentale nell'erogazione dei propri specifici servizi di comparazione/intermediazione (attività della Divisione Broking) o di business process outsourcing (attività della Divisione BPO).
- Salvaguardare il patrimonio del Gruppo nei suoi aspetti finanziari, fisici, di proprietà intellettuale e di reputazione e garantire la riservatezza e la correttezza delle informazioni trattate anche in relazione all'evoluzione delle minacce cyber.
- Garantire la continuità del servizio per rispettare i vincoli derivanti da normative vigenti e da obblighi contrattuali oltre che per assicurarne l'affidabilità nei confronti della clientela.
- Ottemperare alle leggi e alle disposizioni regolamentari in materia di sicurezza delle informazioni che disciplinano l'attività svolta e indicare a dipendenti e collaboratori esterni i principi da seguire.

Applicazione della politica

La presente politica si applica a tutti i processi e a tutte le risorse, umane e asset strumentali, anche esterne, coinvolte nella gestione delle informazioni trattate dalle società del Gruppo, per quanto di competenza di ciascuna di esse.

In particolare i destinatari del documento sono:

- Gli organi di amministrazione delle società del Gruppo, che approvano la Politica e assicurano un adeguato impegno e le risorse necessarie, manageriali ed economiche, per consentire l'effettiva attuazione dei principi definiti.
- I dipendenti delle società del Gruppo, che hanno il compito di attuare quanto definito nella presente Politica, ciascuno per gli ambiti di propria competenza.
- Tutte le terze parti che, nell'ambito di rapporti con le società del Gruppo, hanno la possibilità di accedere al patrimonio informativo aziendale.

Disponibilità della politica

Questa politica è disponibile a tutto il personale delle società del Gruppo tramite la "Intranet MOL" aziendale alla quale il personale può accedere con il solo requisito di avere un account Active Directory del dominio "**gruppomol**".

POLITICA GENERALE DEL SGSI

Di seguito è delineata in punti la Politica Generale del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) per la Sicurezza delle Informazioni e dei beni correlati alle quali tutte le politiche e le procedure conseguenti devono conformarsi, nell'ambito dell'attività delle società del Gruppo:

1	Riservatezza, integrità e disponibilità dell'informazione devono essere assicurate nell'operatività aziendale e nei servizi erogati
2	Tutti gli aspetti di sicurezza devono essere conformi agli obblighi di legge e a norme di sicurezza riconosciuti
3	Analisi dei rischi, non conformità o vulnerabilità rilevate devono essere gestite secondo un processo definito e su base periodica regolare
4	Un modello di classificazione delle informazioni sulla base dei requisiti normativi, contrattuali, di business e interni è definito e applicato
5	Tutto il personale deve essere informato della esistenza delle politiche di sicurezza stabilite in azienda, averne accesso e contribuire responsabilmente perché queste vengano rispettate integralmente
6	L'accesso all'informazione deve essere permesso quando necessario e per specifici trattamenti solo al personale autorizzato
7	La protezione degli asset critici viene garantita tenendo in considerazione, oltre agli aspetti di sicurezza logica, anche quelli di natura fisica
8	Piani di Gestione della Continuità Operativa e di Disaster Recovery devono essere definiti, documentati e collaudati su base periodica regolare
9	Piani di risposta agli incidenti di sicurezza, inclusi quelli che richiedono indagini legali, devono essere definiti, documentati e collaudati su base periodica regolare
10	Eventuali terzi e subappaltatori devono essere conformi alle politiche di sicurezza adottate