Misure di Sicurezza delle Informazioni nell'erogazione dei servizi

INDICE DELLE REVISIONI					
Versione	Data	Oggetto	Redatto	Verificato	Approvato
01	10/01/2025	Prima emissione	RSGI	RSGI	RSGI

Attenzione
Il presente documento è disponibile in copia originale nella rete aziendale.
Ogni copia cartacea si ritiene copia di lavoro **non controllata**.
È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

SOMMARIO

1 INTRODUZIONE 3
2 COMPLIANCE E CERTIFICAZIONI SULLA SICUREZZA DELLE INFORMAZIONI 3
3 COMPETENZE DEL PERSONALE 4
4 GESTIONE DEI RISCHI E OPPORTUNITÀ 4
5 GESTIONE DEI CAMBIAMENTI E DELLE CAPACITÀ 4
6 SICUREZZA LOGICA 4
6.1 ARCHIVIAZIONE SICURA DELLE INFORMAZIONI 4
6.2 TRASMISSIONE SICURA DELLE INFORMAZIONI 4
6.3 SICUREZZA DELLA RETE 5
7 SICUREZZA FISICA 5
8 SICUREZZA DEI SUBFORNITORI DI SERVIZI CLOUD DI LIKE 5
9 SICUREZZA DEGLI APPLICATIVI E SVILUPPO SICURO 5
10 GESTIONE DELLE VULNERABILITÀ 6
11 GESTIONE DEGLI INCIDENTI DI SICUREZZA 6
12 GESTIONE DEI LOG 6
13 GESTIONE DELLE EMERGENZE 6
14 PROTEZIONE DEI DATI PERSONALI 7
15 CONTATTI LIKE 8

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

1 INTRODUZIONE

Like Srl è stata fondata nel 2012 dall'entusiasmo e l'affiatamento di 5 professionisti che hanno maturato esperienza quasi ventennale nel settore informatico. La consulenza e le tecnologie che mettiamo a disposizione dei nostri clienti permettono di rimodellare e velocizzare i processi interni di scambio informazioni. Negli anni la nostra azienda è cresciuta grazie all'acquisizione di figure tecniche qualificate ed esperte e, insieme alle certificazioni conseguite, ci hanno consentito di proporre servizi e consulenza sempre più qualificativa creando un successo condiviso con clienti e partner.

MISSION
Ascoltare il cliente, interpretare le sue esigenze e offrire la giusta soluzione. Definire strategie e risultati finali, che siano misurabili. Adottare soluzioni innovative che siano veloci e semplici da utilizzare ma pensate in maniera critica e costruttiva.

VISION
Creiamo un rapporto di collaborazione e partnership reale con i clienti che migliora e supera il tradizionale modello di relazione tipico delle aziende che operano nel settore informatico, dove la condivisione dell'obiettivo diventa la chiave di volta.

VALUES
In Like, per vocazione e per passione, superiamo gli ostacoli e abbattiamo le barriere. Siamo certi che sia l'unica possibile strategia per creare valore, insieme a clienti e partner, tramite l'esperienza e l'innovazione.

Supportiamo i clienti attraverso prodotti e servizi in ambito:

TECNOLOGICO
Realizziamo soluzioni di System Integration per il business e progettiamo infrastrutture innovative per le ICT aziendali. La consulenza e le tecnologie che mettiamo a disposizione dei nostri clienti permettono di rimodellare e velocizzare i processi interni di scambio informazioni. Per maggiori info vedi qui.

DIGITALE
Progettiamo e sviluppiamo soluzioni complete di innovazione digitale. Attraverso la realizzazione di siti web, e-commerce e campagne di web marketing, Like elabora strategie in grado di migliorare con efficacia il business. Per maggiori info vedi qui.

SVILUPPO
Realizziamo tecnologie software e web application, digitalizziamo e semplifichiamo i processi e integriamo diversi business aziendali. Partiamo dall'analisi dei processi e li traduciamo in strumenti di lavoro efficienti e ottimizzati, mettendo il bisogno dell'utente al primo posto. Per maggiori info vedi qui.

Il documento presenta le misure per la sicurezza delle informazioni e la protezione dei dati personali messe in campo da Like e dai fornitori dei servizi cloud dove pertinente.

2 COMPLIANCE E CERTIFICAZIONI SULLA SICUREZZA DELLE INFORMAZIONI

Data la natura delle proprie attività, Like considera la qualità e la sicurezza delle informazioni, inclusi i dati personali, un fattore irrinunciabile per la protezione del proprio patrimonio informativo e di quello affidatole dai clienti. Per questo motivo l'azienda ha sviluppato un Sistema di Gestione Integrato per Qualità e la Sicurezza delle Informazioni (SGI) definito secondo regole e criteri previsti dalle best practice e dagli standard internazionali di riferimento in conformità alle indicazioni delle seguenti norme internazionali:

- ISO 9001 - "Quality Management System"
- ISO/IEC 27001 - "Information Security Management System"

Like è sottoposta a valutazione di conformità da parte di CSQA, un ente di controllo di terza parte indipendente accreditato da Accredia, l'ente unico nazionale di accreditamento designato dal Governo italiano. I certificati emessi da CSQA sono riconosciuti a livello internazionale.
A livello normativo Like è perfettamente allineata a tutte le leggi nazionali ed europee in merito alla sicurezza delle informazioni e protezione dei dati personali. Potrete trovare maggiori informazioni sulle compliance e sulle certificazioni di Like nella pagina dedicata del sito web aziendale.

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

3 COMPETENZE DEL PERSONALE

Like comunica regolarmente con il proprio personale circa gli obblighi esistenti relativi alla sicurezza delle informazioni, inclusi i dati dei clienti e sulla protezione dei dati personali. In dettaglio l'azienda si avvale dei seguenti canali di comunicazione:

- Attività di formazione annuali
- Attività di formazione all'atto dell'assunzione di nuovi dipendenti
- Attività di aggiornamento annuali per le figure di responsabilità
- Survey interne per misurare il livello di competenza/consapevolezza
- Email interne
- Cartellonistica

4 GESTIONE DEI RISCHI E OPPORTUNITÀ

La direzione di Like ha sviluppato un piano aziendale strategico che include l'identificazione dei rischi e opportunità sulla sicurezza delle informazioni e l'implementazione di specifici trattamenti per mitigarli o perseguirli. Per quanto riguarda l'identificazione dei rischi e delle opportunità ogni anno vengono effettuate sessioni interne di valutazione da parte dei responsabili di area, valutazioni esterne da parte di società terze indipendenti o direttamente dai clienti per le loro infrastrutture in hosting.
L'analisi del rischio e delle opportunità viene condotta prendendo in esame gli scenari di rischi e opportunità per le informazioni relativamente a integrità, disponibilità e riservatezza, nel seguente modo:

- Elencando gli scenari di rischio e opportunità;
- Valutando per ognuno di essi:
  - il potenziale impatto negativo o positivo;
  - la probabilità di accadimento;
- Calcolando in questo modo il valore del rischio o opportunità.

Il valore del rischio o opportunità viene confrontato con i criteri di accettazione stabiliti dalla direzione di Like e se necessario vengono identificate le contromisure da attuare per gestirlo.

5 GESTIONE DEI CAMBIAMENTI E DELLE CAPACITÀ

Le procedure di gestione dei cambiamenti di Like assicurano che cambiamenti concordati agli applicativi e all'infrastruttura minimizzino gli impatti e gli incidenti rispetto i prodotti e i servizi erogati. Le politiche per la gestione sicura del cambiamento coinvolgono tutti i sistemi in gestione, come ad esempio: hardware, apparati di comunicazione e software, sistemi software, la documentazione e le procedure legate alla gestione, supporto e manutenzione degli ambienti di produzione. Ogni proposta di cambiamento è sempre progettata e verificata tra le parti per mezzo di specifici documenti di analisi tecnica e commerciale.
Le procedure di gestione della capacità di Like assicurano la comprensione di tutti gli aspetti relativi alle prestazioni e capacità attuali dell'organizzazione e quelle future al fine di anticiparle e veicolarle secondo esigenze aziendali.

Il processo per la gestione delle capacità include i seguenti elementi:

- Comprensione della domanda di servizi attuale e previsione dei bisogni futuri;
- Capacità di influenzare la domanda di servizi e risorse;
- Comprensione degli obiettivi di Qualità e Sicurezza delle Informazioni;

Le risorse cloud di calcolo e di storage sono scalabili e possono essere ridimensionate in modo affidabile e flessibile a seconda della specifica esigenza.

6 SICUREZZA LOGICA

6.1 ARCHIVIAZIONE SICURA DELLE INFORMAZIONI

I dati gestiti da Like in archiviazione sono sempre criptati con chiavi di cifratura sicure.

6.2 TRASMISSIONE SICURA DELLE INFORMAZIONI

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

I dati trasmessi in entrata e in uscita dai sistemi gestiti da Like vengono criptati attraverso protocolli sicuri quali ad esempio HTTPS, FTPS, VPN secondo specifica esigenza. Eventuali eccezioni dovranno essere segnalate dal cliente fin dalle fasi iniziali del progetto e saranno soggette a proposte di riconversione sicura da parte di Like.

6.3 SICUREZZA DELLA RETE

Le infrastrutture su cui poggiano gli applicativi gestiti da Like sono progettate secondo elevati standard di sicurezza:

- Sistemi di configurazione iniziale automatici permettono di limitare rischi di errate implementazioni;
- Soluzioni di Firewall per la protezione del traffico in ingresso e in uscita;
- Sistemi di protezione per tentativi di attacco DDoS;
- Sistemi di monitoraggio, di log management e aggiornamento/applicazione di patch di sicurezza.

L'infrastruttura cloud, formata dai componenti hardware e software, le reti e le strutture che eseguono i servizi è tutelata dai fornitori cloud stessi per cui Like ha sottoscritto specifici accordi contrattuali vincolanti in termini di sicurezza delle informazioni e protezione dei dati personali.

7 SICUREZZA FISICA

I locali di Like, con attenzione alle aree sicure contenenti dati di tipo riservato anche di tipo personale sono difesi dalle seguenti misure di sicurezza fisiche: accessi chiusi a chiave, muri, videosorveglianza, personale di sicurezza e altri dispositivi elettronici. Apposite procedure regolano le visite occasionali o regolari del personale esterno all'azienda. Il sistema di monitoraggio è sotto il presidio di Like che controlla e garantisce gli accessi.

Like è attenta anche ai fenomeni naturali come terremoti, alluvioni, eventi metereologici o incendi che possono causare rischi per la salute dei lavoratori e l'indisponibilità delle strutture; per questo effettua regolarmente sessioni di formazione al personale, prove di evacuazione e interventi migliorativi e del controllo funzionamento degli impianti speciali di sicurezza.

8 SICUREZZA DEI SUBFORNITORI DI SERVIZI CLOUD DI LIKE

I fornitori cloud di Like che permettono la fornitura di servizi cloud controllano rigorosamente l'accesso ai data center, anche nel caso di dipendenti interni. Le terze parti hanno accesso ai data center solo se espressamente autorizzati secondo specifiche policies di accesso. Prima di creare un data center i fornitori dedicano molto tempo all'analisi delle minacce potenziali e alla progettazione, implementazione e test dei controlli per verificare che sistemi, tecnologia e persone siano in grado di reagire ai rischi. Prima di scegliere una sede, sono eseguiti valutazioni ambientali e geografiche. Le posizioni dei data center sono attentamente selezionate per mitigare i rischi ambientali, come alluvioni, condizioni meteorologiche estreme e attività sismica. Le zone di disponibilità sono costruite per essere indipendenti e fisicamente separate l'una dall'altra.

Like garantisce che i servizi IT e i sistemi operativi utilizzati vengono regolarmente aggiornati secondo i criteri e le tempistiche indicate dal produttore.

9 SICUREZZA DEGLI APPLICATIVI E SVILUPPO SICURO

Like propone applicativi proprietari e software di terze parti (es. CMS) integrandole ove necessario con funzionalità custom nel rispetto del copyright delle case produttrici.

Per tutti gli aspetti legati alla sicurezza degli applicativi di terze parti utilizzati si rimanda alla documentazione specifica di volta in volta pertinente rispetto a quanto presente all'interno degli accordi tra le parti e condiviso dal commerciale di riferimento.

Like, nello sviluppare le modifiche agli applicativi, ne salvaguarda le caratteristiche di sicurezza intrinseche nel rispetto degli standard di sicurezza richiesti dai requisiti cogenti e contrattuali e più in generale seguendo le linee guida di sviluppo indicate dai produttori.

Per le attività di programmazione Like si basa sull'approccio OWASP (Open Web Application Security Project), volto a diminuire il rischio di introdurre possibili vulnerabilità.

Gli ambienti di sviluppo sono sempre separati dagli ambienti di test e di produzione ove si potrebbero annidare dati riservati aziendali tra cui dati personali. Nel caso fosse necessario utilizzare fin dalle prime fasi di sviluppo dati similari ai dati reali sono predisposte in accordo con i clienti specifiche procedure di anonimizzazione.

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

Like ha implementato automatismi collegati alla propria pipeline di sviluppo e rilascio che permettono di ispezionare continuamente la qualità e la sicurezza del codice in tutte le fasi di sviluppo e rilascio attraverso code reviewing e tool di verifica del software.

Ogni funzionalità concordata prima di essere rilasciata in ambiente di produzione deve passare positivamente diverse verifiche interne ed esterne.

10 GESTIONE DELLE VULNERABILITÀ

In Like è operativo un processo continuo di identificazione, valutazione e rientro delle vulnerabilità dei sistemi informativi e delle applicazioni. Il processo di gestione delle vulnerabilità prevede le seguenti macro-attività principali:

- Stilare un inventario degli asset IT della società, classificati in base al livello di criticità, inclusi server, infrastrutture di rete, postazioni di lavoro, stampanti e applicazioni;
- Rilevare le vulnerabilità esistenti, segnalate dai fornitori o verificate internamente/esternamente dai clienti utilizzando scanner di rete, scanner delle vulnerabilità e software per i test di penetrazione automatizzati stabilendo di volta in volta livelli di rischio appropriati;
- Valutazione tecnica della vulnerabilità rilevata rispetto a criteri di gravità, numero di sistemi impattati, disponibilità di upgrade, fix di sicurezza;
- Comunicazione a tutte le parti interessate della vulnerabilità e di come Like intende andare a mettere in sicurezza i sistemi;
- Applicazione di patch di sicurezza e test successivi secondo logica di rilascio sicuro;
- Comunicazione di applicazione patch avvenuta con successo e registrazione misure correttive nella knowledge base.

11 GESTIONE DEGLI INCIDENTI DI SICUREZZA

Like ha istituito un processo per la pianificazione, preparazione e gestione dell'organizzazione nell'eventualità di un incidente relativo alla sicurezza delle informazioni. Il processo di gestione degli incidenti relativi alla sicurezza delle informazioni comprende un insieme dettagliato di attività volte a prevenire, scoprire e mitigare l'impatto di un evento che possa compromettere la disponibilità, l'integrità, la riservatezza delle informazioni.

Figure adeguatamente formate in Like si occupano di valutare quali eventi si possono concretamente definire come Incidenti sulla Sicurezza delle Informazioni e gestirli nella loro totalità fino alla piena risoluzione e verbalizzazione finale. In caso di Incidenti a elevato impatto, tramite logiche interne di escalation, si attivano misure di gestione delle emergenze descritte all'interno del paragrafo successivo. In caso di data breach si attivano le specifiche procedure di notifica tra le parti secondo le modalità pattuite.

La segnalazione di possibili incidenti relativi alla sicurezza delle informazioni può giungere da fonti differenti: dai partner, da un sistema di monitoraggio antintrusione, da un dipendente o dai clienti stessi. In caso di presunto o accertato incidente per cui non sia stata data ancora nessuna comunicazione, Like richiede a tutti i suoi clienti di darne una immediata notifica attraverso i canali concordati tra le parti.

12 GESTIONE DEI LOG

Like ritiene che sia cruciale per la salvaguardia delle informazioni trattate per conto dei suoi clienti porre il focus non solo sulle attività di prevenzione e gestione dei problemi di sicurezza ma anche sul sistema di log management posto in essere per comprendere gli eventi negativi dopo che questi si sono verificati. I log sono asset fondamentali per far fronte efficacemente alle necessità di data protection, alla continuità di servizio e per garantire la compliance aziendale rispetto le normative in vigore in ambito nazionale e internazionale.

I sistemi di log implementati da Like includono sempre le informazioni sul chi e quando ha fatto una determinata operazione e sono mantenuti inalterabili.

Nel rispetto del provvedimento del 27 novembre 2008 del Garante per la Privacy italiano, Like mantiene secondo gli stessi principi anche i log degli amministratori di sistema.

13 GESTIONE DELLE EMERGENZE

Se un Incidente sulla sicurezza delle informazioni ha impatti rilevanti in termini di riservatezza, disponibilità e integrità delle informazioni vengono attivati tramite escalation specifici processi di gestione delle emergenze. Il processo di gestione delle

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

emergenze è un processo basato su tecniche di continuità operativa, disaster recovery e di pubbliche relazioni nei confronti di clienti, fornitori, autorità, altre parti interessate e mezzi di informazione.

Like anche in fase di crisi introduce tutte le misure e le procedure volte a garantire la continuità delle operazioni relative alla sicurezza delle informazioni. In termini operativi Like si occupa:

- della disponibilità delle informazioni con opportune ridondanze;
- della continuità dei processi di sicurezza delle informazioni, tra cui: controllo degli accessi, controllo degli archivi fisici e dei sistemi informatici, monitoraggio, gestione degli incidenti;
- della gestione completa dei backup i quali sono ridondati, criptati e ne è verificato periodicamente il restore.
- Per eventuali ulteriori informazioni si rimanda ai canali di contatto con il commerciale di riferimento.

14 PROTEZIONE DEI DATI PERSONALI

Per Like è fondamentale definire fin da subito il perimetro dei dati personali trattati all'interno dei sistemi forniti. Attenzione verrà posta alle situazioni dove si potrebbero annidate dati personali particolari e giudiziari secondo la definizione degli Articoli 9 e 10 del Regolamento UE 2016/679. Tali elementi devono essere valutati attentamente in fase di prevendita.

I Clienti di Like risultano Titolari del Trattamento dei dati personali trattati e Like Responsabile del Trattamento. Tra i due soggetti, ai sensi dell'Art. 28 paragrafo 3 del GDPR, è necessaria la stipula di un atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Like ha predisposto un template di nomina responsabile del trattamento che sarà inoltrato dal commerciale di riferimento al momento della stipula del contratto. Eventuali modelli di accordo alternativi devono essere validati dalle parti.

Ai sensi dell'Art. 28 paragrafo 2 il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Like condivide la lista dei subfornitori pertinenti e concordati tra le parti. Con tali subfornitori, Like ha sottoscritto a sua volta specifici accordi di data processing agreement. Eventuali trattamenti Extra-UE trattamenti sono effettuati nel rispetto delle leggi dell'UE.

Like, in riferimento ai servizi di consulenza erogati, in seguito a periodiche valutazioni d'impatto sulla protezione dei dati e per mezzo del suo sistema di gestione per la sicurezza delle informazioni ISO/IEC 27001, mette in atto di volta in volta il set di misure di sicurezza adeguate per garantire ai propri clienti il mantenimento dei principi di riservatezza, integrità, disponibilità delle informazioni e la protezione dei dati personali. Eventuali misure di sicurezza aggiuntive devono essere valutate attentamente in fase di prevendita. Inoltre, Like dietro approfondita valutazione e specifici accordi contrattuali garantisce la conformità dei sistemi rispetto ai diritti dell'interessato di cui al capo III del regolamento UE 2016/679.

Like si impegna a non utilizzare, modificare o rivelare a nessuno, a meno che non indicato dal cliente, i dati relativi ai suoi clienti. Like si impegna a non accedere agli account dei propri clienti, inclusi i dati relativi al cliente, se non per motivi di manutenzione del servizio, per anticipare o rispondere a problematiche tecniche o relative all'assistenza, su richiesta del cliente in connessione a un problema di supporto o quando richiesto dalla legge. Ove quindi sorgesse la necessità, l'accesso da parte del personale di Like avverrà tramite credenziali che rispettano le policies minime di sicurezza e secondo specifico profilo di autorizzazione.

In caso di violazione dei dati personali (di seguito "Data Breach"), Like, ai sensi dell'Art. 28 paragrafo 3 lettera f) e ai sensi dell'Art. 33 paragrafo 2 del GDPR, al fine di assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 33, 34 notificherà la violazione al Titolare del Trattamento entro i termini di legge o viceversa i termini concordati all'interno dei contratti pattuiti o in un altro documento alternativo definito tra le parti rispetto il momento in cui si è venuti a conoscenza della violazione. In parallelo, Like opererà a adottare tempestivamente tutte le azioni correttive necessarie ad impedire ulteriori violazioni e a minimizzare gli effetti negativi.

LIKE SRL | VIA NICCOLÒ COPERNICO, 2/A INT. L | 35013 CITTADELLA (PD) | TEL. +39 049 9401339 | INFO@LIKESRL.COM | P.IVA IT046104102

15 CONTATTI LIKE

Per qualsiasi necessità in ambito Sicurezza delle Informazioni e Protezione dei dati personali in Like sono attivi e disponibili i seguenti punti di contatto:

Integrated Management System Manager, Daniele Pilla
daniele@likesrl.com

Nonché i punti di contatto già a disposizione del commerciale di Like di riferimento.