

TLP: CLEAR



morolabs

POLITICA DI SICUREZZA DELLE INFORMAZIONI

morolabs srl

www.morolabs.it

Revisione 1.0 del 23/01/2025



1. Introduzione

La presente Politica di Sicurezza delle Informazioni (di seguito "Politica") definisce gli obiettivi, le responsabilità e le misure per proteggere le informazioni sensibili e i sistemi dell'organizzazione in conformità ai requisiti della norma ISO/IEC 27001. L'obiettivo principale della presente politica è garantire la riservatezza, l'integrità e la disponibilità delle informazioni dell'organizzazione, riducendo al minimo i rischi derivanti da minacce interne ed esterne, rendere i sistemi sufficientemente resilienti in modo da rispondere adeguatamente e superare un evento traumatico o un momento di difficoltà.

La Politica descrive le misure tecniche e organizzative, le procedure e i controlli interni di sicurezza delle informazioni ("Misure di sicurezza") che l'organizzazione mantiene al fine di salvaguardare il patrimonio informativo proprio e dei clienti da accessi, divulgazione, alterazione, perdita o distruzione accidentali, non autorizzati o illegali.

Nel caso di trattamento di dati personali le misure di sicurezza sono progettate in logica security by-design e garantiscono un livello di sicurezza adeguato e conforme alla vigente disciplina.

L'organizzazione può modificare le misure di sicurezza in ogni momento, senza alcun preavviso o quando sia ritenuto necessario, a condizione di non ridurre o degradare il livello di protezione fornita.



*Ogni clic consapevole,
un firewall invisibile.*

— FRANCESCO MORONCINI

2. Obiettivi della Politica



La Politica di Sicurezza delle Informazioni si prefigge i seguenti obiettivi:

OBIETTIVI



proteggere le informazioni dell'organizzazione e dei clienti da accessi non autorizzati, divulgazione, alterazione, distruzione o perdita in conformità ai requisiti previsti dallo standard ISO/IEC 27001.



garantire che tutte le risorse informative siano gestite in modo sicuro durante l'intero ciclo di vita; mantenere un Sistema di Gestione della Sicurezza dell'Informazione allineato alle buone pratiche e agli standard internazionali, fornendo evidenza alle parti interessate



assicurare la conformità alle normative e agli standard di sicurezza applicabili; fornire una base per la gestione dei rischi legati alla sicurezza delle informazioni al fine di ridurre a un valore accettabile la probabilità che siano violati i parametri di sicurezza informatica nonché individuare tempestivamente quando ed in quale parte del sistema questo accade.



limitare i danni e ripristinare i requisiti violati nel minor tempo possibile; considerare il miglioramento continuo quale pratica per il mantenimento di un adeguato livello di sicurezza; promuovere la cultura della sicurezza tra i dipendenti e le altre parti interessate.

3. Ambito di applicazione

La presente politica si applica a tutte le informazioni, i sistemi e le risorse gestiti, elaborati, archiviati o trasmessi all'interno dell'organizzazione.

La politica fornisce la necessaria copertura sul personale dipendente, i collaboratori esterni, i fornitori e le altre parti che hanno accesso alle informazioni dell'organizzazione.



4. Principi base

I principi base che l'organizzazione applica nel perseguimento di elevati standard di sicurezza delle informazioni sono:

tutela dei diritti, delle libertà e della dignità delle persone

garanzia della necessaria continuità operativa per l'erogazione del miglior servizio possibile unito al minor dispendio di energie (umane, tecnologiche, temporali ed economiche);

conformità normativa e allineamento agli standard di mercato.

tutela del patrimonio informativo dell'organizzazione e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:

- accessi illegittimi ai sistemi o agli applicativi;
- modifiche indesiderate alle informazioni;
- perdita della disponibilità dei dati.

security e privacy by design ovvero considerare la sicurezza e la conformità alla protezione dati personali come parte integrante della progettazione complessiva del sistema;

approccio alla sicurezza di tipo multilivello (*Layered security*), adottando tecniche di segmentazione e segregazione quanto maggiormente possibile;

protezione del patrimonio informativo in ogni fase del trattamento e per tutto il ciclo di vita, ovvero quando i dati sono elaborati e comunicati (*"in transit"*) o quando sono conservati (*"in storage"*);

allineamento delle misure di sicurezza ai requisiti di business, in conformità alle normative vigenti e agli obblighi contrattuali;

corretto bilanciamento tra usabilità e sicurezza

riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia, partendo dal modello "tutto chiuso" e adottando principio del *"need-to-know"* correlato al business;

misure di sicurezza prescelte a seguito di valutazione del rischio, con criteri condivisi di accettazione delle soglie di rischio, al fine di garantire il corretto bilanciamento tra costi e benefici.

adozione della Regola del "minimo privilegio" rispetto alla finalità (*"separation of duties policy"*), in ottica di stratificazione dei profili e degli accessi;

consapevolezza di tutti gli utilizzatori rispetto ai rischi e alle corrette modalità di utilizzo dei sistemi e dei servizi IT;

misure di sicurezza semplici da comprendere e da attuare.

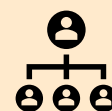
5. Ruoli e responsabilità

Sono assegnati i seguenti ruoli e responsabilità relativi alla sicurezza:



Responsabile della Sicurezza delle Informazioni (CISO)

figura incaricata di supervisionare la sicurezza delle informazioni e di garantire l'attuazione della presente Politica di Sicurezza delle Informazioni. Il CISO è responsabile della gestione delle risorse, della valutazione dei rischi e della conformità



Dirigenti e Responsabili di Area/UO

hanno la responsabilità di implementare la sicurezza delle informazioni nei rispettivi dipartimenti e di sensibilizzare il personale riguardo alle best practice di sicurezza.



DIPENDENTI

sono responsabili della protezione delle informazioni dell'organizzazione a cui hanno accesso, seguendo le pratiche di sicurezza definite nella presente politica e nella regolamentazione specifica.

— Name Surname

6. Gestione dei rischi

L'organizzazione adotta un approccio basato sulla gestione del rischio per identificare, valutare e mitigare i rischi associati alla sicurezza delle informazioni. Il processo include:

- *la valutazione periodica dei rischi per identificare minacce e vulnerabilità;*
- *l'attuazione di misure di controllo per ridurre i rischi a livelli accettabili;*
- *la revisione regolare della Politica e delle misure di sicurezza in base ai cambiamenti nei rischi o nelle condizioni operative.*

7. Misure di sicurezza

Le seguenti misure di sicurezza sono adottate per proteggere le informazioni dell'organizzazione:

Organizzazione della Sicurezza delle Informazioni

Definizione dei ruoli con specifici obblighi di riservatezza.

Regolamentazione e procedure dell'organizzazione.

Formazione specifica rispetto ai singoli ruoli.

Asset Management

È mantenuto aggiornato un inventario completo dell'infrastruttura, rete, applicazioni e ambienti cloud; l'accesso a tali informazioni è limitato al solo personale autorizzato.

Sicurezza fisica e ambientale

L'accesso alle strutture è limitato al solo personale autorizzato e secondo specifiche procedure.

Controlli di accesso

L'accesso alle informazioni dell'organizzazione è limitato e controllato sulla base di principi del minimo privilegio e necessità di conoscenza. Ogni utente è autenticato tramite password sicure e tramite 2FA/MFA.

Protezione dei Dati

I dati sensibili devono essere criptati durante la trasmissione e l'archiviazione.
I backup devono essere effettuati regolarmente e conservati in luoghi sicuri.

Antimalware

Sono presenti sistemi di controllo antimalware al fine di evitare che software dannosi ottengano l'accesso non autorizzato ai sistemi o alle informazioni.

Gestione delle vulnerabilità

L'organizzazione adotta politiche di patching e gestione delle vulnerabilità per garantire che i sistemi siano protetti dagli attacchi.

Gestione degli Incidenti di

È previsto un processo per la gestione degli incidenti di sicurezza delle informazioni, compresa la segnalazione tempestiva, l'investigazione e la risposta a qualsiasi violazione della sicurezza.

Registrazione degli eventi

Al fine di consentire il monitoraggio, il rilevamento e la risposta tempestiva a potenziali minacce o anomalie nel funzionamento dei sistemi informatici tutti gli eventi sono registrati in logica di sovrascrittura.

ALTRI ELEMENTI



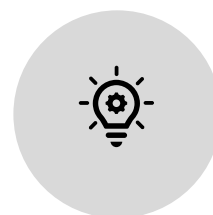
8. Formazione e sensibilizzazione

L'organizzazione si impegna a fornire formazione continua sulla sicurezza delle informazioni per tutti i dipendenti e i collaboratori, assicurando che siano a conoscenza delle minacce, dei rischi e delle misure di sicurezza pertinenti inclusa la regolamentazione interna. La sensibilizzazione riguardo alla sicurezza delle informazioni è parte integrante del processo di onboarding e delle valutazioni delle performance.



9. Conformità e monitoraggio

L'organizzazione monitora costantemente l'efficacia della Politica di sicurezza delle Informazioni e ne valuta la conformità attraverso audit interni, revisioni dei controlli e test di sicurezza. Ogni violazione della Politica è trattata secondo procedimento disciplinare.



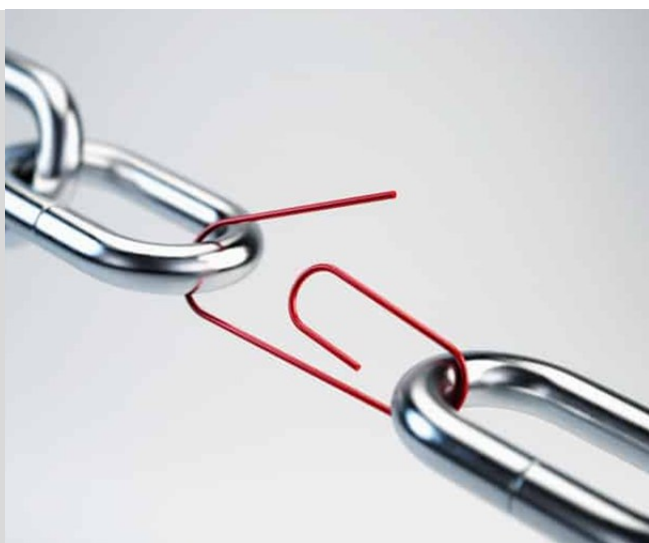
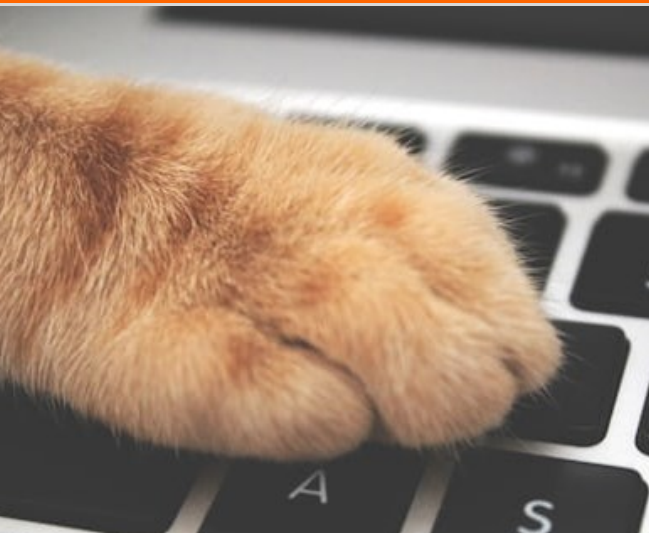
10. Business Continuity e Disaster Recovery

In caso di eventi imprevisti che possono compromettere la disponibilità delle informazioni, l'organizzazione ha messo in atto un Piano di continuità operativa e di Disaster recovery che assicura una rapida ripresa delle operazioni.

11. Revisione della Politica

La Politica di Sicurezza delle Informazioni è rivista annualmente al fine di garantire la necessaria adeguatezza ed efficacia. Eventuali modifiche saranno comunicate a tutto il personale.





12. Conclusioni

L'adozione della presente Politica di Sicurezza delle Informazioni è fondamentale per proteggere i beni informativi dell'organizzazione e mantenere la fiducia di clienti, partner e altre parti interessate. Ogni membro dell'organizzazione è tenuto a rispettare le disposizioni della politica per garantire una gestione sicura e responsabile delle informazioni dell'organizzazione.

La Direzione condivide i Principi e gli Obiettivi per la Sicurezza delle Informazioni sopra descritti e supporta pienamente un programma per la loro attuazione e mantenimento.

La Direzione approva ed emette il presente documento di Politica, quale documento programmatico per la Sicurezza delle Informazioni. L'attuazione di tale Politica sarà facilitata attraverso norme e procedure appropriate.

Saranno perseguite nelle opportune sedi le azioni che, disattendendo le indicazioni della presente Politica in modo intenzionale o riconducibile a negligenza, provocheranno un danno all'organizzazione.

La presente politica è riesaminata regolarmente per garantirne l'idoneità rispetto alle finalità dell'organizzazione ed alle aspettative delle parti interessate.

LA DIREZIONE





雲の上はいつも晴れ

*“sopra le nuvole
è sempre sereno”*

— proverbio giapponese

morolabs

MOROLABS SRL

Sede legale: P.zza Michelangelo, 11 60018 Montemarciano (AN)

Cod. Fisc./P.IVA 02763650427 Tel: +39 071.9030585

e-mail: info@morolabs.it PEC morolabs@legalmail.it

www.morolabs.it

Sedi Operative:

L.go Procaccini, 2 60037 Monte San Vito (AN)

Via della Resistenza, 10 61037 Marotta (PU)

