
NOLOOP

POLITICA DELLA SICUREZZA INFORMATICA

BREVE INTRODUZIONE

NOLOOP S.r.l. – Società Benefit considera la sicurezza delle informazioni, la continuità operativa e la protezione dei dati personali elementi essenziali per garantire affidabilità, tutela degli stakeholder e qualità dei servizi.
Le informazioni commerciali, organizzative, progettuali, economiche, tecniche e personali costituiscono un patrimonio fondamentale per NOLOOP e per i suoi clienti. La loro protezione richiede il coinvolgimento responsabile di tutte le persone che operano nell'Organizzazione e dei soggetti esterni che accedono a dati, sistemi o informazioni aziendali.
NOLOOP è certificata secondo la norma ISO/IEC 27001:2022 e mantiene un Sistema di Gestione per la Sicurezza delle Informazioni integrato con gli altri sistemi di gestione adottati dall'Organizzazione.
La presente Politica aggiorna e sviluppa gli impegni già assunti da NOLOOP in materia di sicurezza delle informazioni, continuità operativa e protezione dei dati personali, adeguandoli all'attuale assetto certificativo e organizzativo della Società.

1. SCOPO

La presente Politica definisce i principi, gli impegni e gli obiettivi attraverso i quali NOLOOP intende:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni;
- prevenire accessi, utilizzi, divulgazioni, modifiche, perdite o distruzioni non autorizzate;
- tutelare i dati personali durante l'intero ciclo di vita del trattamento;
- assicurare la continuità dei processi e dei servizi aziendali critici;
- prevenire e gestire gli incidenti di sicurezza;
- garantire la conformità agli obblighi normativi, contrattuali e volontariamente assunti;
- gestire i rischi e le opportunità connessi alla sicurezza delle informazioni;
- sviluppare consapevolezza, competenze e comportamenti responsabili;
- monitorare e migliorare continuamente l'efficacia delle misure adottate.

La Politica costituisce il quadro di riferimento per la definizione degli obiettivi annuali e per il monitoraggio delle prestazioni del Sistema di Gestione per la Sicurezza delle Informazioni.

2. CAMPO DI APPLICAZIONE

La presente Politica si applica alle informazioni, ai dati personali, ai documenti, ai sistemi informativi, alle piattaforme, ai dispositivi, alle infrastrutture e agli altri asset utilizzati da NOLOOP nello svolgimento delle proprie attività.
La Politica riguarda tutte le informazioni trattate dall'Organizzazione, indipendentemente:

- dal formato, cartaceo o digitale;
- dal luogo in cui sono conservate o utilizzate;
- dal soggetto che le ha generate;
- dal mezzo attraverso il quale vengono comunicate;
- dalla proprietà dell'informazione;

- dal fatto che si tratti di informazioni di NOLOOP, dei clienti, del personale, dei fornitori, dei partecipanti agli eventi o di altri stakeholder.

La Politica si applica a tutte le sedi, funzioni, attività e processi di NOLOOP e deve essere rispettata dal personale, dagli amministratori, dai collaboratori, dai consulenti e, per quanto pertinente, dai fornitori e dai partner che operano per conto dell'Organizzazione.

3. RIFERIMENTI

La presente Politica è definita in coerenza con:

- la norma ISO/IEC 27001:2022 relativa ai sistemi di gestione per la sicurezza delle informazioni;
- il Regolamento UE 2016/679 in materia di protezione dei dati personali;
- il D.Lgs. 196/2003 e successive modifiche e integrazioni;
- la normativa applicabile in materia di sicurezza informatica, protezione dei dati e continuità operativa;
- gli obblighi contrattuali assunti nei confronti di clienti, fornitori, partner e altre parti interessate;
- le norme ISO 9001, ISO 14001, ISO 45001 e ISO 20121, per gli aspetti pertinenti all'integrazione dei sistemi di gestione;
- i Dieci Principi del Global Compact delle Nazioni Unite;
- gli Obiettivi di Sviluppo Sostenibile dell'Agenda 2030;
- lo Statuto e le finalità di beneficio comune di NOLOOP;
- il Codice Etico, il Codice di Condotta dei Fornitori e le altre politiche istituzionali adottate dall'Organizzazione.

La Politica contribuisce in particolare ai seguenti Obiettivi di Sviluppo Sostenibile:

- SDG 9 – Imprese, innovazione e infrastrutture, attraverso lo sviluppo di infrastrutture digitali affidabili, resilienti e sicure;
- SDG 16 – Pace, giustizia e istituzioni solide, attraverso trasparenza, responsabilizzazione, protezione delle informazioni e tutela dei diritti delle persone;
- SDG 17 – Partnership per gli obiettivi, attraverso la collaborazione responsabile con clienti, fornitori e partner nella protezione delle informazioni condivise.

4. TERMINI E DEFINIZIONI

Informazione: qualsiasi dato, documento, comunicazione o contenuto avente valore per NOLOOP o per una parte interessata, indipendentemente dal relativo formato.

Riservatezza: proprietà per cui le informazioni sono accessibili esclusivamente ai soggetti autorizzati.

Integrità: proprietà per cui le informazioni sono complete, accurate e protette da modifiche o alterazioni non autorizzate.

Disponibilità: proprietà per cui le informazioni e i sistemi sono accessibili ai soggetti autorizzati quando necessario.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Asset informativo: informazione, sistema, dispositivo, servizio, infrastruttura o altra risorsa avente valore per l'Organizzazione.

Incidente di sicurezza: evento che compromette o può compromettere la riservatezza, l'integrità o la disponibilità delle informazioni e dei sistemi.

Continuità operativa: capacità dell'Organizzazione di proseguire o ripristinare le attività prioritarie in seguito a eventi avversi.

Disaster recovery: insieme delle misure finalizzate al ripristino di sistemi, infrastrutture, applicazioni e dati a seguito di un'interruzione significativa.

5. RESPONSABILITÀ

La Direzione approva la presente Politica, ne assicura la coerenza con gli indirizzi strategici di NOLOOP e mette a disposizione risorse adeguate alla protezione delle informazioni e la continuità operativa.
Il Responsabile del Sistema di Gestione Integrato coordina il mantenimento, il monitoraggio e il miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni.
Le funzioni competenti in materia di sistemi informativi e amministrazione dei sistemi assicurano l'attuazione e il mantenimento delle misure tecniche e organizzative assegnate.
Il Data Protection Officer svolge i compiti previsti dalla normativa in materia di protezione dei dati personali, mantenendo autonomia e indipendenza nell'esercizio delle proprie funzioni.
I responsabili delle funzioni aziendali garantiscono l'applicazione della Politica nei processi di propria competenza e assicurano che gli accessi alle informazioni siano coerenti con le effettive necessità operative.
Tutto il personale e i collaboratori sono responsabili del corretto utilizzo delle informazioni, dei dispositivi e dei sistemi messi a disposizione e devono segnalare tempestivamente incidenti, anomalie, smarrimenti, accessi sospetti o possibili violazioni.

6. PRINCIPI E IMPEGNI

6.1 Gestione dei rischi

NOLOOP identifica e valuta periodicamente i rischi relativi alle informazioni, ai dati personali, ai sistemi e alla continuità operativa.
Le misure di sicurezza sono definite in modo proporzionato:

- alla criticità delle informazioni;
- alle minacce e alle vulnerabilità individuate;
- alle possibili conseguenze per l'Organizzazione e per le parti interessate;
- agli obblighi normativi e contrattuali;
- all'evoluzione tecnologica e organizzativa;
- alle esigenze di continuità dei servizi.

La valutazione dei rischi viene aggiornata in occasione di cambiamenti significativi nei processi, nei sistemi, nelle tecnologie, nei servizi o nel contesto operativo.

6.2 Protezione delle informazioni

NOLOOP classifica e protegge le informazioni in funzione della loro natura, criticità e riservatezza.
L'Organizzazione adotta misure finalizzate a:

- limitare l'accesso alle sole persone autorizzate;

- applicare il principio della necessità di conoscere;
- garantire autenticazione e gestione controllata delle credenziali;
- proteggere dati e documenti durante la conservazione, l'utilizzo e la trasmissione;
- prevenire perdita, alterazione, divulgazione o utilizzo improprio;
- garantire la tracciabilità delle attività rilevanti;
- assicurare la corretta conservazione e cancellazione delle informazioni;
- proteggere dispositivi, reti, sistemi e ambienti fisici.

6.3 Protezione dei dati personali

NOLOOP tratta i dati personali nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.
L'Organizzazione applica, ove pertinente, i principi di protezione dei dati e sicurezza delle informazioni fin dalla progettazione e per impostazione predefinita.
NOLOOP tutela i diritti e le libertà delle persone fisiche e assicura il rispetto degli obblighi applicabili sia quando opera come Titolare del trattamento sia quando agisce come Responsabile del trattamento per conto dei propri clienti.

6.4 Gestione degli accessi

Gli accessi a informazioni, sistemi e piattaforme sono attribuiti sulla base delle responsabilità e delle effettive necessità operative.
NOLOOP si impegna a:

- autorizzare formalmente gli accessi;
- limitare i privilegi al minimo necessario;
- riesaminare periodicamente le autorizzazioni;
- modificare o revocare tempestivamente gli accessi in caso di variazione o cessazione del rapporto;
- adottare adeguate misure di autenticazione;
- monitorare e gestire i tentativi di accesso non autorizzato.

6.5 Gestione degli incidenti

NOLOOP mantiene modalità organizzative per la segnalazione, la valutazione e la gestione degli incidenti di sicurezza.
Ogni incidente o sospetto evento deve essere tempestivamente comunicato, registrato e analizzato al fine di:

- contenerne gli effetti;
- proteggere le persone e le informazioni coinvolte;
- ripristinare le condizioni di sicurezza;
- individuare le cause;
- prevenire il ripetersi dell'evento;
- adempiere agli eventuali obblighi di comunicazione o notifica;
- migliorare le misure tecniche e organizzative.

La segnalazione tempestiva degli eventi è considerata un comportamento responsabile e non deve essere ostacolata dall'obiettivo aziendale di prevenire gli incidenti.

6.6 Continuità operativa e resilienza

NOLOOP adotta misure di continuità operativa, backup e ripristino finalizzate a limitare gli effetti di guasti, indisponibilità, errori, incidenti informatici o altri eventi avversi.
I processi e i servizi critici sono individuati e sottoposti a misure proporzionate alla loro rilevanza.
I piani di continuità e ripristino sono sottoposti a verifiche periodiche per valutarne l'efficacia, rilevare i tempi di recupero e individuare eventuali azioni di miglioramento.

6.7 Fornitori e partner

NOLOOP valuta i rischi derivanti dall'affidamento a terzi di attività che comportano l'accesso a informazioni, dati personali, sistemi o servizi digitali.
I fornitori e i partner rilevanti devono:

- offrire adeguate garanzie tecniche e organizzative;
- rispettare gli obblighi di riservatezza;
- utilizzare le informazioni esclusivamente per le finalità autorizzate;
- limitare l'accesso al personale effettivamente incaricato;
- segnalare tempestivamente incidenti o violazioni;
- rispettare gli obblighi normativi e contrattuali applicabili;
- collaborare alle attività di verifica e gestione delle criticità.

I requisiti di sicurezza sono definiti in modo proporzionato alla natura della fornitura e al rischio associato.

6.8 Formazione e consapevolezza

NOLOOP promuove una cultura della sicurezza basata sulla consapevolezza e sulla responsabilità individuale.
Il personale riceve formazione e aggiornamento sui rischi connessi all'utilizzo delle informazioni, dei dispositivi, delle credenziali, della posta elettronica e degli strumenti digitali.
L'Organizzazione realizza inoltre attività periodiche di sensibilizzazione per favorire il riconoscimento delle minacce, la prevenzione degli errori e la tempestiva segnalazione degli eventi sospetti.

7. OBIETTIVI

7.1 Obiettivi qualitativi

NOLOOP persegue i seguenti obiettivi qualitativi:

- proteggere le informazioni aziendali e quelle affidate da clienti e altre parti interessate;
- mantenere un livello di sicurezza adeguato all'evoluzione delle minacce;
- prevenire incidenti, perdite di dati e accessi non autorizzati;
- garantire continuità e resilienza dei servizi critici;
- integrare la sicurezza nella progettazione dei processi e delle soluzioni tecnologiche;
- rafforzare la consapevolezza e la responsabilità del personale;
- migliorare la capacità di rilevare, gestire e risolvere gli incidenti;

- assicurare una gestione controllata degli accessi;
- valutare i rischi connessi a fornitori e servizi esterni;
- tutelare i dati personali e i diritti delle persone;
- migliorare continuamente l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni.

7.2 Obiettivi quantitativi

In coerenza con gli obiettivi definiti nel Riesame della Direzione, NOLOOP assume i seguenti riferimenti quantitativi:

- formare in materia di sicurezza delle informazioni almeno il 90% del personale interessato;
- realizzare almeno 3 campagne di sensibilizzazione all'anno;
- mantenere pari a zero il numero degli incidenti di sicurezza registrati, assicurando comunque la registrazione e l'analisi di ogni anomalia, evento o tentativo rilevato;
- mantenere un tempo medio di rilevamento degli incidenti non superiore a 24 ore e un tempo medio di risposta e risoluzione non superiore a 48 ore;
- disattivare entro 24 ore dalla cessazione del rapporto almeno il 90% degli account interessati;
- assicurare il blocco del 100% dei tentativi di accesso non autorizzato rilevati dai sistemi di controllo.
- sottoporre il 100% dei sistemi compresi nel perimetro a verifica e gestione degli aggiornamenti e delle patch di sicurezza;
- chiudere entro i termini stabiliti almeno il 90% delle azioni correttive;
- mantenere entro il valore massimo annuale di una non conformità il numero delle non conformità rilevate negli audit interni ed esterni;
- effettuare almeno 2 test di continuità operativa all'anno;
- registrare e valutare i tempi di ripristino nel 100% delle prove di continuità operativa.

Gli obiettivi quantitativi sono quelli definiti dalla Direzione per il periodo di riferimento e sono monitorati attraverso i KPI del Sistema di Gestione Integrato.
La Direzione può aggiornare annualmente i target sulla base dei risultati raggiunti, dei cambiamenti del contesto, dell'evoluzione delle minacce e delle priorità dell'Organizzazione.

8. MONITORAGGIO E MIGLIORAMENTO

L'attuazione della presente Politica è verificata attraverso:

- monitoraggio degli incidenti e degli eventi di sicurezza;
- controllo degli accessi e delle autorizzazioni;
- verifiche sugli aggiornamenti dei sistemi;
- risultati delle attività formative e di sensibilizzazione;
- test di continuità operativa e ripristino;
- audit interni ed esterni;
- gestione delle non conformità e delle azioni correttive;
- valutazione dei fornitori rilevanti;
- analisi dei rischi e delle vulnerabilità;
- verifica del rispetto degli obblighi normativi e contrattuali.

Gli eventuali scostamenti rispetto agli obiettivi sono analizzati per individuarne le cause e definire azioni correttive o di miglioramento.
La Politica viene riesaminata almeno annualmente e ogni volta che intervengano cambiamenti significativi nell'Organizzazione, nelle tecnologie, nei processi, nei requisiti applicabili o nel panorama delle minacce.

9. COMUNICAZIONE E DIFFUSIONE

NOLOOP assicura che la presente Politica sia comunicata e resa comprensibile al personale, ai collaboratori e ai soggetti che operano per conto dell'Organizzazione.
La Politica è resa disponibile ai clienti, ai fornitori, ai partner e alle altre parti interessate attraverso il sito aziendale e gli ulteriori canali istituzionali ritenuti appropriati.
Tutte le persone che operano per NOLOOP sono chiamate a contribuire alla protezione delle informazioni, adottando comportamenti responsabili e segnalando tempestivamente incidenti, anomalie e situazioni potenzialmente rischiose.

DONZELLI
PAOLO
30.07.2026
12:21:40
GMT+02:00