Politica per la sicurezza delle informazioni

Rif documento	ISMS-DOC-A05
Versione	2
Data	20 January 2026
Autore	Net Patrol Italia
Proprietario del documento	*Net Patrol Italia*

Titolo documento:

Politica per la sicurezza delle informazioni

Revisioni

VERSIONE	DATA	AUTORE REVISIONE	RIEPILOGO DELLE MODIFICHE
1	02/12/2024	Claudio Basso	Prima Emissione
2	20/01/2026	Irene Benedetti	Revisione e miglioramento

Distribuzione

NOME	TITOLO

Approvazione

NOME	RUOLO	FIRMA	DATA

Sommario

Politica per la sicurezza delle informazioni 1
Revisioni 2
Distribuzione 2
Approvazione 2
1. Introduzione 4
2. Gestione del rischio 4
2.1 Gestione del rischio per i soggetti interessati (privacy) 4
2.2 Gestione del rischio di cybersecurity 5
3. Ruoli e Responsabilità 5
3.1 Affidabilità delle risorse umane 5
4. Classificazione delle informazioni 6
5. Gestione del rischio della supply chain 6
6. Gestione degli asset 7
7. Sicurezza fisica 7
8. Sicurezza dell'infrastruttura IT 8
8.1 Misure tecniche 8
8.2 Misure organizzative 8
9. Gestione degli incidenti 9
9.1 Piano di Incident Response 9
10. Formazione e consapevolezza 10
11. Riesame e miglioramento 10

1. Introduzione

La presente politica è stata sviluppata in conformità con lo standard ISO/IEC 27001:2022, al Regolamento UE 2016/679 (GDPR) e nel rispetto degli obiettivi stabiliti dalla Direttiva 2022/2555 (NIS2) e rappresenta il quadro di riferimento dei principi, delle linee guida e delle regole adottate da *Net Patrol Italia Srl* per la sicurezza delle informazioni e dei sistemi informativi.

La politica fornisce una guida a tutto il personale di *Net Patrol* ed eventuali Terze Parti sulle proprie responsabilità riguardo al trattamento dei dati personali, alla gestione e all'utilizzo delle risorse informatiche e alle responsabilità sul loro utilizzo.

Le finalità specifiche della presente politica sono:

- Stabilire i principi generali, gli obiettivi e le linee guida che orientano l'approccio dell'organizzazione alla sicurezza informatica;
- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e degli asset aziendali;
- promuovere l'adozione di misure tecniche, organizzative e procedurali adeguate e proporzionate ai rischi;
- garantire il rispetto dei requisiti normativi e regolamentari applicabili;

2. Gestione del rischio

La gestione del rischio è un processo fondamentale per garantire il rispetto dei diritti e delle libertà dei soggetti interessati, la sicurezza delle informazioni e la resilienza delle infrastrutture critiche.

2.1 Gestione del rischio per i soggetti interessati (privacy)

Net Patrol si impegna a sottoporre ogni trattamento che possa presentare un rischio elevato per i diritti e libertà delle persone fisiche a valutazione d'impatto sulla protezione dei dati ("DPIA") ai sensi dell'art. 35 GDPR, specie se il trattamento viene svolto con l'uso di nuove tecnologie. La valutazione di impatto viene comunque svolta a tutti i casi previsti per legge e in tutti i casi specificatamente definiti con Provv. N. 467/2018 dell'Autorità Garante per la Protezione dei Dati personali, pubblicato in G.U. n. 269 del 19 novembre 2018.

Inoltre, in caso in cui il trasferimento di dati al di fuori dello Spazio Economico Europeo possa dare luogo a rischi elevati per i soggetti interessati, *Net Patrol* sottopone lo stesso a una preventiva valutazione d'impatto (Transfer Impact Assessment) al fine di valutare e mitigare tali rischi – applicando le necessarie misure di sicurezza, organizzative e legali. Per specifici dettagli in merito ai criteri, ruoli e responsabilità per lo svolgimento di valutazioni d'impatto sulla protezione dei dati si rimanda al documento "Politica DPIA".

2.2 Gestione del rischio di cybersecurity

In conformità allo standard internazionale ISO/IEC 27001:2022 e altri standard e linee guida internazionali, la gestione del rischio include una serie di attività strutturate e continuative volte a identificare, valutare, mitigare e monitorare i rischi associati alle operazioni e ai sistemi informativi:

- Identificazione dei rischi: raccolta e analisi delle informazioni per individuare potenziali minacce e vulnerabilità. Vengono considerati sia i rischi interni, che quelli esterni, inclusi attacchi informatici, guasti tecnici, errori umani e disastri naturali;
- Analisi e Valutazione: una volta identificati i rischi viene valutato l'impatto e la probabilità di occorrenza;
- Piano di Trattamento: la mitigazione dei rischi implica l'implementazione di misure di trattamento e controllo per ridurne la probabilità e l'impatto;
- Monitoraggio e revisione: la gestione del rischio è un processo dinamico che richiede un monitoraggio continuo e una revisione periodica. È importante valutare l'efficacia delle misure di mitigazione e apportare modifiche in base ai cambiamenti del panorama delle minacce e nelle esigenze organizzative;
- Comunicazione: tutti i livelli dell'organizzazione sono periodicamente coinvolti e aggiornati relativamente al sistema di gestione per la sicurezza delle informazioni e sul Piano di Trattamento.

3. Ruoli e Responsabilità

La gestione della sicurezza delle informazioni è supportata da una struttura organizzativa che definisce responsabilità e autorità specifiche, assicurando coordinamento tra funzioni aziendali, processi operativi e gestione del rischio.

3.1 Affidabilità delle risorse umane

I dipendenti di *Net Patrol* devono attenersi a specifiche norme di comportamento al fine di assicurare un livello omogeneo di sicurezza, riducendo i rischi connessi a errori umani, in ottemperanza delle procedure aziendali.

Per avere adeguate garanzie che il personale abbia chiare le proprie responsabilità, che sia stato selezionato ed incaricato in modo conforme al ruolo affidatogli e che abbia le competenze necessarie per lo svolgimento delle mansioni assegnategli, *Net Patrol* predispone appropriate misure di sicurezza organizzative durante tutto il ciclo di vita aziendale del personale. In particolare:

- All'atto di selezione vengono effettuati controlli sui candidati, in proporzione all'inquadramento e del ruolo aziendale, nel rispetto delle leggi e dei regolamenti pertinenti;
- Sono definiti e comunicati al dipendente gli obblighi di riservatezza;
- Si mantiene una gestione continua delle autenticazioni, delle identità digitali e degli accessi.

4. Classificazione delle informazioni

Le informazioni possono assumere varie forme, tra cui: dati cartacei conservati su carta, dati archiviati elettronicamente in sistemi informatici e comunicazioni inviate tramite posta. L'organizzazione ha la responsabilità di proteggere le informazioni che detiene ed elabora, utilizzando controlli proporzionati alla sensibilità e alla criticità delle informazioni coinvolte.

Al fine di proteggere tali informazioni, è stato definito un modello di classificazione delle informazioni, così strutturato:

LEVEL 0	***CLEAR*: pubblico o non soggetto a classificazione**
LEVEL 1	***GREEN***: riservato ai membri di una community
LEVEL 2	***AMBER***: : riservato all'organizzazione ed ai suoi clienti
LEVEL 3	***AMBER + STRICT***: riservato solo all'organizzazione
LEVEL 4	***RED***: Confidenziale, riservato ai singoli soggetti elencati

Al momento della creazione, tutte le risorse informative devono essere valutate e classificate dal proprietario in base al loro contenuto. La classificazione determinerà come il documento deve essere protetto e a chi deve essere consentito l'accesso. Qualsiasi sistema che consenta successivamente l'accesso a queste informazioni deve indicare chiaramente la classificazione.

5. Gestione del rischio della supply chain

Net Patrol riconosce che la sicurezza delle informazioni non dipende esclusivamente dalla misure tecniche e organizzative adottate internamente, ma anche dal livello di protezione garantito dai propri fornitori, partner commerciali e soggetti terzi coinvolti nei processi aziendali.

A tal fine, l'organizzazione definisce e implementa un processo di gestione del rischio legato alla supply chain che comprende, in primo luogo, la valutazione preliminare dei fornitori e dei partner strategici prima dell'avvio di qualsiasi collaborazione. Tale valutazione include l'analisi del loro livello di maturità in ambito cybersecurity, delle certificazioni possedute (ad esempio ISO/IEC 27001, ISO 22301, o equivalenti) e delle politiche di sicurezza applicate, nonché la verifica delle misure tecniche e organizzative adottate per la protezione delle informazioni e dei servizi critici.

L'organizzazione adotta inoltre un monitoraggio continuo dei fornitori durante l'intero ciclo di vita del rapporto commerciale, al fine di individuare tempestivamente variazioni nel livello di sicurezza o nuovi rischi emergenti. Questo processo di monitoraggio si basa su verifiche periodiche, aggiornamenti di documentazione e, se necessario, rivalutazioni del rischio.

6. Gestione degli asset

Per “asset” si intendono tutte le risorse tecnologiche, informative e infrastrutturali che contribuiscono al funzionamento dei processi aziendali e al raggiungimento degli obiettivi strategici dell’organizzazione.

Net Patrol adotta un approccio sistematico e centralizzato alla gestione degli asset, finalizzato a garantire una visibilità completa sul patrimonio tecnologico e informativo, a minimizzare i rischi legati a utilizzi non autorizzati o non controllati e a supportare le attività di monitoraggio, protezione e risposta agli incidenti.

A tal fine, l’organizzazione mantiene un inventario aggiornato e accurato di tutti gli asset rilevanti, costantemente revisionato e aggiornato in occasione di acquisizioni, modifiche infrastrutturali, dismissioni o cambiamenti significativi nel contesto operativo.

7. Sicurezza fisica

Net Patrol ha definito, mediante opportuna analisi del rischio e con il supporto delle strutture aziendali preposte, criteri e requisiti di sicurezza fisica e ambientale al fine di impedire e/o limitare perdite di dati e di risorse critiche dovute a vulnerabilità nell’ambito del dominio fisico.

L’accesso ai locali ove risiedono strumenti di elaborazione e agli archivi cartacei deve essere consentito solo al personale preposto e autorizzato.

L’accesso alle sedi aziendali deve essere consentito solo previa identificazione della persona che necessita di entrare.

Le aree che ospitano i sistemi di maggiore criticità devono essere localizzate in zone sicure e protette al fine di minimizzare il rischio di perdite o danneggiamenti e utilizzi impropri e non consentiti. I locali che ospitano elaboratori elettronici devono disporre di dispositivi che consentono di:

- Segregare e tracciare gli accessi effettuati dal personale autorizzato;
- Monitorare i tentativi di accesso non autorizzato e di effrazione nei locali.

8. Sicurezza dell'infrastruttura IT

L'infrastruttura IT e le sue principali componenti devono essere adeguatamente protette e ne deve essere mantenuta l'efficacia e l'efficienza nel tempo. Pertanto:

- Le procedure operative, le architetture definite, le configurazioni applicate, devono essere documentate e mantenute aggiornate per garantire l'uso corretto e sicuro delle risorse IT;
- Devono essere pianificate e messe in atto le misure necessarie a garantire un adeguato livello di efficienza e di prestazioni dei sistemi IT, la prevenzione del rischio di malfunzionamenti o di degrado delle funzionalità di sicurezza applicate;

8.1 Misure tecniche

Le misure tecniche comprendono tutte le soluzioni e le tecnologie per proteggere le informazioni e i sistemi da accessi non autorizzati, attacchi informatici e altre minacce. Tali misure includono:

- Controllo accessi: : implementazione di sistemi di autenticazione robusti, come MFA e la gestione dei privilegi degli utenti, per garantire che solo il personale autorizzato possa accedere alle informazioni sensibili;
- Sicurezza sei sistemi endpoint: protezione dei dispositivi endpoint (computer, server, dispositivi mobili) tramite software antivirus, anti-malware e patch management);
- Backup e ripristino: implementazione di procedure di backup regolari e strategie di ripristino per garantire che i dati possano essere recuperati in caso di perdita o danneggiamento.

8.2 Misure organizzative

Le misure organizzative si riferiscono alle politiche, alle procedure e alla cultura aziendale necessarie per garantire un ambiente sicuro e includono:

- Sviluppo e implementazione di politiche e procedure chiare e documentate che stabiliscano aspettative e responsabilità in materia di sicurezza delle informazioni;
- Formazione e sensibilizzazione: programmi di formazione regolari per il personale su tematiche di sicurezza informatica, buone pratiche e procedure da seguire in caso di incidente;
- Valutazione e mitigazione dei rischi: processi regolari di valutazione dei rischi per identificare, analizzare e mitigare i rischi per la sicurezza delle informazioni;
- Gestione fornitori: procedure per la valutazione e gestione della sicurezza dei fornitori e dei partner, assicurando che anche le terze parti che accedono ai sistemi e alle informazioni dell'organizzazione rispettino gli standard di sicurezza adeguati;

9. Gestione degli incidenti

Al fine di prevenire qualsiasi evento dannoso derivante da violazioni di dati e incidenti di sicurezza, Net Patrol adotta procedure e protocolli di gestione per tali eventi.

9.1 Piano di Incident Response

Il piano di gestione delle violazioni di dati personali e degli incidenti di *Net Patrol* prevede i seguenti elementi, ulteriormente dettagliati anche in specifiche politiche e procedure:

- Pianificazione: definizione di politiche e procedure, formazione del personale, creazione di un team di risposta agli incidenti e l'acquisizione degli strumenti necessari.
- Rilevamento e segnalazione: identificazione tempestiva degli incidenti di sicurezza. Utilizzando strumenti di monitoraggio e rilevamento delle minacce, l'organizzazione deve essere in grado di individuare attività sospette o anomale;
- Contenimento, eradicazione e ripristino: Dopo aver identificato un incidente, è necessario contenerlo per prevenire ulteriori danni. Questo può includere l'isolamento dei sistemi compromessi, la disconnessione delle reti infette e l'applicazione di patch di sicurezza.
- Comunicazione e notifica: La comunicazione efficace durante un incidente è cruciale. È necessario informare tempestivamente tutte le parti interessate, sia interne che esterne. In particolare, è obbligatorio notificare violazioni di dati personali e incidenti alle Autorità competenti, nonché eventualmente ai soggetti interessati, entro i termini di legge. La trasparenza e la chiarezza nella comunicazione aiutano a mantenere la fiducia e a coordinare le azioni di risposta.
- Post-incident e miglioramento continuo: Dopo la gestione di un incidente, è importante condurre una revisione post-incidente per valutare l'efficacia della risposta e identificare le aree di miglioramento. Questo include la registrazione della violazione di dati nell'apposito registro interno, l'aggiornamento delle politiche di sicurezza, la revisione dei piani di risposta agli incidenti e la formazione aggiuntiva del personale. L'obiettivo è imparare dagli incidenti per prevenire future occorrenze e migliorare continuamente la postura di sicurezza dell'organizzazione.

Per la specifica procedura di gestione e risposta agli incidenti informatici si rimanda al relativo documento: "Procedura di Incident Management", "Data Breach procedure". Le istruzioni stabilite in quel documento devono essere utilizzate solo come guida quando si risponde a un incidente. La natura esatta di un incidente e il suo impatto non possono essere previsti con un elevato grado di certezza, e quindi è importante che venga utilizzato un buon livello di buon senso quando si decidono le azioni da intraprendere.

10. Formazione e consapevolezza

Al fine di garantire un'ottima ed efficace gestione della protezione dei dati personali e della sicurezza informatica, il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity e del trattamento dei dati personali.

I programmi di formazione sono regolari e aggiornati, includendo simulazioni di attacchi informatici ed esercitazioni pratiche per migliorare le reattività e la preparazione del personale. Inoltre è importante promuovere una cultura della sicurezza attraverso campagne di sensibilizzazione che evidenziano l'importanza della protezione dei dati e della cybersecurity, incoraggiando comportamenti responsabili.

11. Riesame e miglioramento

Il riesame della presente politica verrà effettuato annualmente o ogni qualvolta intervenga una delle seguenti circostanze:

- Evoluzioni normative o regolatorie in materia di sicurezza informatica e protezione dei dati personali;
- Incidenti significativi di sicurezza o data breach che impattano sull'organizzazione;
- Variazioni organizzative rilevanti.