POLITICA PER LA CYBERSECURITY

Revisione e data	Rev. 1 del 04.06.2026
Classificazione	documento pubblico

Elenco delle revisioni

revisione	data	descrizione	approvazione
0	01.07.2025	Prima emissione	il Direttore Generale
1	04.06.2026	Revisione dei contenuti, aggiunta dei riferimenti al Framework NIS2	il Direttore Generale

Indice

VILLANI SPA
Via E. Zanasi, 24
41051 Castelnuovo Rangone (MO)
C.F./P.IVA 00772580361

Premessa

Per lo scopo di questa politica, il termine Cybersecurity utilizzato in questo documento ha il significato equivalente di sicurezza informatica.

Villani S.p.A. e le società del Gruppo (di seguito, anche "Gruppo Villani") riconoscono il ruolo cruciale che le informazioni svolgono nei processi aziendali e la loro importanza per il raggiungimento degli obiettivi di business. Allo stato attuale, i sistemi informatici aziendali utilizzati dal gruppo Villani devono essere altamente interconnessi e accessibili da qualsiasi luogo; sebbene questo rappresenta grandi opportunità, il rischio di attacchi ostili o perdita di dati è una minaccia reale e in costante aumento.

La società Villani S.p.A., che è tenuta agli adempimenti richiesti dal Decreto Legislativo n. 138 del 4 settembre 2024 ("Decreto NIS") in quanto "soggetto importante" come individuato nell'ambito di applicazione di cui all'art. 3 comma 1 del Decreto NIS, con questa politica intende adottare un proprio modello organizzativo per la Cybersecurity, in conformità ai requisiti del Decreto NIS che viene identificato e recepito quale framework normativo di riferimento.

1. Riferimenti normativi

- DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022, *relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*. (di seguito, "direttiva NIS2");
- DECRETO LEGISLATIVO 4 settembre 2024, n. 138 - *Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148* (di seguito "decreto NIS").

1.1. Riferimenti al Framework NIS2

Funzioni interessate	Categorie
GOVERNO - (GV) La strategia di gestione del rischio di Cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate.	**POLITICA (GV.PO):** La politica di Cybersecurity dell'organizzazione è stabilita, comunicata e applicata.

2. Scopo ed applicazione

Questa politica stabilisce l'impegno della società Villani S.p.A. verso l'adozione di un modello organizzativo di Cybersecurity, finalizzato a proteggere da minacce interne ed esterne i sistemi informativi e le reti aziendali e le informazioni che vengono trattate, attraverso la definizione di requisiti minimi per la Cybersecurity da applicare per tutelare la proprietà intellettuale, il vantaggio commerciale, il personale aziendale, dalle conseguenze di una scarsa sicurezza informatica e di eventuali attacchi informatici, con lo scopo di garantire il funzionamento delle attività e dei servizi dell'organizzazione.

Poiché tutte le società del Gruppo Villani utilizzano i sistemi informativi e di rete di Villani S.p.A. o vi accedono, si ritiene opportuno che questa politica per la Cybersecurity sia condivisa e applicata da tutte le società del Gruppo Villani.

3. Obiettivi

L'adozione di un'efficace modello organizzativo di Cybersecurity persegue i seguenti obiettivi:

- proteggere le informazioni aziendali da accessi non autorizzati, modifiche, divulgazioni o distruzioni e garantirne i requisiti di integrità, riservatezza e disponibilità;
- assicurare la continuità operativa, minimizzando i rischi legati alla Cybersecurity;
- conformarsi alle normative e agli standard di sicurezza applicabili;
- contribuire ad incrementare il livello aziendale, nazionale e comunitario di Cybersecurity, a tutela della società e di tutte le parti interessate.

4. Principi di Cybersecurity

Villani S.p.A., in quanto soggetto NIS importante ai sensi del D.Lgs. 138/2024, si impegna ad attuare misure tecniche, operative ed organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete utilizzati nelle proprie attività, allo scopo di prevenire o ridurre al minimo l'impatto degli incidenti sulla sicurezza delle informazioni e garantire la continuità dei processi aziendali. Le misure adottate sono basate su un approccio multirischio, mirato a proteggere i sistemi informativi e comprendono: politiche e procedure di analisi dei rischi e di sicurezza dei sistemi informatici; procedure di gestione degli incidenti e condivisione delle informazioni sulle minacce; piani di continuità operativa.

Le altre società del gruppo recepiscono e condividono i principi di Cybersecurity insieme con le misure tecniche, operative ed organizzative implementate dalla capogruppo Villani S.p.A. per garantire la sicurezza. Se del caso, a seguito di analisi e valutazione dei rischi, le altre società del gruppo potranno definire linee guida aggiuntive e richiedere l'adozione di ulteriori misure di sicurezza per garantire il livello di sicurezza atteso.

5. Responsabilità, formazione, consapevolezza

Nell'ambito del proprio modello organizzativo di Cybersecurity, la direzione di Villani S.p.A. esercita il potere decisionale per adempiere ai requisiti del Decreto NIS in materia di Cybersecurity, assegna ruoli e responsabilità, accetta i rischi e approva i piani per il loro trattamento e le misure di sicurezza, fornisce le risorse necessarie per la loro implementazione e sovraintende alla loro attuazione.

Il personale del dipartimento IT di Villani S.p.A. si occupa dell'implementazione, aggiornamento e monitoraggio delle misure di sicurezza tecnologiche per la sicurezza informatica.

I dipendenti e collaboratori del gruppo Villani che utilizzano i sistemi informativi e le reti di Villani S.p.A. sono responsabili dell'osservanza e dell'applicazione di questa politica, delle procedure e delle regole di sicurezza che gli sono comunicate; vengono informati sui rischi e le minacce informatiche che possono affrontare e su come reagire quando si imbattono in attività sospette; sono tenuti alla segnalazione di anomalie, incidenti o disservizi inerenti alla sicurezza delle informazioni, di cui dovessero venire a conoscenza.

Il gruppo Villani fornirà adeguata formazione ed aggiornamenti sulla sicurezza informatica al personale interessato, per assicurare la consapevolezza e la comprensione delle migliori pratiche di Cybersecurity.

Il personale esterno, i fornitori e le terze parti che hanno relazioni con i sistemi informativi e le reti di Villani S.p.A., ovvero che vi accedono, devono rispettare gli standard di sicurezza applicabili ai nostri dipendenti e collaboratori e devono garantire le adeguate misure di sicurezza e protezione; Villani S.p.A. e le società del gruppo selezioneranno fornitori con adeguati standard di sicurezza, monitorandone periodicamente il livello di affidabilità.

Ogni persona, responsabile di qualsiasi atto deliberato di mettere a rischio la sicurezza delle informazioni gestite con i sistemi informativi e le reti di Villani S.p.A. sarà soggetta alle opportune azioni disciplinari e/o legali.

6. Revisione e comunicazione della politica di Cybersecurity

Villani S.p.A. è impegnata per il miglioramento continuo del modello organizzativo di Cybersecurity, anche con il supporto ed il contributo delle società del Gruppo Villani, al fine di garantire la protezione delle proprie risorse informative, consolidare la fiducia delle parti interessate e contribuire allo sviluppo, alla sicurezza ed al progresso.

L'applicazione di questa politica sarà regolarmente monitorata ed eventualmente aggiornata o integrata, in caso di variazioni delle minacce informatiche, modifiche ai sistemi informativi aziendali, cambiamenti dei requisiti normativi.

Il contenuto di questa politica è pubblicamente condivisibile, la Direzione di Villani S.p.A. stabilisce che questo documento sia reso disponibile alle parti interessate:

- in copia digitale nel sistema documentale accessibile al personale aziendale;
- mediante pubblicazione nel sito web aziendale all'indirizzo www.villanisalumi.it