



LETTERA DI IMPEGNO DELLA DIREZIONE

IMPEGNO DELLA DIREZIONE PER LA SICUREZZA DELLE INFORMAZIONI, LA PROTEZIONE DEI DATI PERSONALI E IL MIGLIORAMENTO CONTINUO

RIFERIMENTI	ISO/IEC 27001:2022 – ISO/IEC 27017 – 27018 – NIS2	
CLASSIFICAZIONE	PUBBLICO	
REVISIONE	01	
DATA DI EMISSIONE	19 OTTOBRE 2026	

SICUREZZA DELLE INFORMAZIONI ALL'INTERNO DI CLOUDFIRE

CloudFire S.r.l., in qualità di fornitore di servizi cloud e soluzioni tecnologiche, riconosce la sicurezza delle informazioni, la cybersecurity, la protezione dei dati personali e la continuità operativa quali elementi fondamentali per garantire l'affidabilità dei propri servizi e tutelare gli interessi dei clienti, del personale, dei partner e delle altre parti interessate.

A tale scopo, CloudFire ha implementato e mantiene un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) conforme alla norma ISO/IEC 27001:2022, nell'ambito del quale sono definiti principi, responsabilità, processi e misure per la protezione delle informazioni.

Il Sistema di Gestione per la Sicurezza delle Informazioni di CloudFire è inoltre integrato con le linee guida e i controlli specifici previsti dalle norme ISO/IEC 27017 e ISO/IEC 27018, in coerenza con l'ambito delle certificazioni aziendali.

In particolare, la ISO/IEC 27017 riguarda la sicurezza delle informazioni nell'erogazione e nell'utilizzo dei servizi cloud, con particolare attenzione ai rischi specifici degli ambienti cloud e alla ripartizione delle responsabilità tra fornitore e cliente.

La ISO/IEC 27018 riguarda invece la protezione delle informazioni personali identificabili (PII) trattate nei servizi di cloud pubblico quando il fornitore opera per conto dei propri clienti, rafforzando le misure di tutela e riservatezza dei dati affidati a CloudFire.

Il funzionamento dell'ISMS contribuisce, in particolare, a:

- tutelare la riservatezza, l'integrità e la disponibilità delle informazioni;
- assicurare la continuità e l'affidabilità dei servizi erogati ai clienti;
- proteggere gli asset aziendali e le informazioni affidate a CloudFire;
- rispettare i requisiti legali, regolamentari e contrattuali applicabili;
- promuovere la gestione dei rischi e il miglioramento continuo della sicurezza.

IMPEGNO E RESPONSABILITÀ DELLA DIREZIONE

La Direzione assume un ruolo attivo nella definizione degli indirizzi strategici per la sicurezza delle informazioni e la cybersecurity, assicurando che tali obiettivi siano coerenti con le finalità aziendali e integrati nei processi organizzativi.

La Direzione assicura che i ruoli, le responsabilità e le autorità pertinenti alla sicurezza delle informazioni e alla cybersecurity siano definiti, attribuiti e comunicati all'interno dell'organizzazione, secondo le competenze e i livelli decisionali previsti.

L'impegno della Direzione si inserisce nel più ampio sistema di governance, controllo interno e conformità adottato da CloudFire, che comprende il Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001 e il Codice Etico aziendale. Tali strumenti concorrono a promuovere comportamenti responsabili, il rispetto della normativa applicabile e una cultura organizzativa orientata all'integrità, alla prevenzione dei rischi e alla tutela delle parti interessate.

Sono inoltre attribuite le responsabilità di assicurare che l'ISMS soddisfi i requisiti applicabili e di riferire alla Direzione sulle prestazioni del sistema, sui risultati delle verifiche e sulle eventuali esigenze di miglioramento.

La Direzione sostiene l'attuazione e lo sviluppo dell'ISMS mediante l'assegnazione di risorse adeguate, la promozione della consapevolezza del personale e il coinvolgimento delle funzioni aziendali competenti.

Assicura inoltre che le prestazioni dell'ISMS siano sottoposte a riesame periodico, tenendo conto degli obiettivi di sicurezza, dei risultati degli audit, degli incidenti, delle valutazioni del rischio e delle opportunità di miglioramento.

GESTIONE DEL RISCHIO E RESILIENZA

CloudFire adotta un approccio strutturato alla valutazione e al trattamento dei rischi per la sicurezza delle informazioni, coerente con i requisiti della norma ISO/IEC 27001:2022.

La gestione del rischio è integrata nei processi aziendali e considera, secondo quanto applicabile:

- i rischi che possono compromettere il raggiungimento degli obiettivi di sicurezza delle informazioni;

- i rischi associati ai sistemi, alle infrastrutture, ai servizi e ai processi aziendali;
- i rischi derivanti da modifiche organizzative, tecnologiche e operative;
- i rischi connessi a progetti e cambiamenti significativi;
- i rischi derivanti dalle dipendenze da fornitori, partner e altri soggetti della catena di approvvigionamento.

La Direzione promuove inoltre la resilienza dei servizi CloudFire attraverso la definizione di misure organizzative e tecniche per la prevenzione, l'individuazione e la gestione degli incidenti, nonché per la continuità operativa e il ripristino dei servizi.

IMPEGNO IN MATERIA DI CYBERSECURITY E NIS2

CloudFire S.r.l., in qualità di soggetto essenziale ai sensi del D.Lgs. 138/2024, riconosce la gestione del rischio di cybersicurezza come parte integrante della propria governance aziendale.

La Direzione si impegna a supervisionare l'attuazione delle misure di gestione del rischio e degli obblighi applicabili, promuovendo il coinvolgimento delle funzioni responsabili, l'assegnazione delle risorse necessarie e il monitoraggio dello stato di adeguamento.

Particolare attenzione è rivolta alla sicurezza dei sistemi informativi e di rete, alla gestione degli incidenti, alla continuità operativa e alla sicurezza della catena di approvvigionamento, in relazione alla natura dei servizi erogati e alle dipendenze da soggetti esterni.

Le responsabilità per la valutazione e il monitoraggio dei rischi associati ai fornitori sono attribuite alle funzioni aziendali competenti e integrate nei processi di gestione della sicurezza e del rischio.

PROTEZIONE DEI DATI PERSONALI E RESPONSABILITÀ DEL PERSONALE

CloudFire riconosce l'importanza della protezione dei dati personali e promuove il rispetto del Regolamento (UE) 2016/679 (GDPR), mediante l'adozione di misure tecniche e organizzative adeguate ai trattamenti effettuati e ai ruoli assunti nell'ambito dei servizi erogati.

Il personale e i collaboratori autorizzati al trattamento dei dati ricevono istruzioni pertinenti alle attività svolte e sono tenuti al rispetto delle politiche di sicurezza, delle regole di utilizzo dei sistemi informatici e degli obblighi di riservatezza applicabili.

CloudFire assicura che il personale sia informato dei propri ruoli e responsabilità prima dell'accesso alle risorse aziendali, promuovendo una cultura della sicurezza basata sulla consapevolezza, sulla responsabilità individuale e sulla formazione continua.

La Direzione sostiene la formazione e l'aggiornamento delle competenze in materia di sicurezza delle informazioni e cybersecurity, anche in relazione alle responsabilità degli organi di amministrazione e direzione e alle esigenze derivanti dalla normativa NIS2.

Sono inoltre previsti canali e modalità di segnalazione delle anomalie, degli incidenti e delle eventuali violazioni, secondo le procedure aziendali applicabili, nel rispetto degli obblighi di riservatezza e delle tutele previste dalla normativa.

COMUNICAZIONE E MIGLIORAMENTO CONTINUO

La Politica per la Sicurezza delle Informazioni è resa disponibile al personale e alle parti interessate pertinenti secondo le modalità definite da CloudFire.

La Direzione promuove il miglioramento continuo dell'ISMS, la verifica periodica dell'efficacia delle misure adottate e l'aggiornamento dei processi in relazione all'evoluzione delle minacce, dei servizi e dei requisiti applicabili.

Con la presente dichiarazione, la Direzione conferma il proprio impegno a sostenere e supervisionare la sicurezza delle informazioni, la cybersecurity, la resilienza operativa e la protezione dei dati quali responsabilità essenziali per l'affidabilità e lo sviluppo dei servizi CloudFire.

Cordiali saluti,

Roberto Bondavalli
Chief Executive Officer

Firmato digitalmente da: Roberto Bondavalli
Luogo: Reggio Emilia
Data: 19/10/2026 16:23:12