POLICY DI RESPONSIBLE DISCLOSURE

FiberCop

FIBER INFRASTRUCTURE PARTNER
OF MILANO CORTINA 2026

MILANO CORTINA 2026

MILANO CORTINA 2026

FIBERCOP – POLICY DI RESPONSIBLE DISCLOSURE

La sicurezza delle reti, dei sistemi e dei dati dei nostri clienti e utenti è una priorità per FiberCop. Siamo consapevoli che, nonostante le misure di sicurezza adottate, possano emergere vulnerabilità. Per questo incoraggiamo una segnalazione responsabile, collaborativa e in buona fede.

AMBITO

La presente Policy si applica esclusivamente alle vulnerabilità individuate nei servizi digitali, siti web e applicazioni ufficiali FiberCop, chiaramente identificabili come tali, inclusi sistemi e piattaforme digitali, applicazioni e servizi online, nonché componenti software e interfacce esposte verso l'esterno.

Non rientrano nell'ambito le segnalazioni relative a configurazioni standard o best practice di sicurezza prive di impatti concreti sfruttabili, tra cui, a titolo esemplificativo:

- assenza o configurazione non ottimale di security headers HTTP (es. CSP, HSTS, X-Frame-Options), se non associata a vulnerabilità sfruttabili;
- utilizzo di versioni o configurazioni TLS considerate deboli ma non sfruttabili nel contesto specifico;
- esposizione di banner o informazioni di versione senza impatto di sicurezza dimostrabile;
- segnalazioni di natura puramente informativa o di hardening.

Eventuali vulnerabilità relative a sistemi basati su Intelligenza Artificiale sono considerate in ambito esclusivamente ove comportino impatti concreti e dimostrabili sulla sicurezza delle informazioni (es. esposizione dati, accesso non autorizzato, bypass dei controlli).

COME SEGNALARE UNA VULNERABILITÀ

Invia la tua segnalazione a: cirt[@]fibercop[.]com

La segnalazione dovrebbe includere, ove possibile:

- descrizione della vulnerabilità;
- sistema o URL coinvolto;
- passaggi per la riproduzione;
- eventuali evidenze tecniche.

È possibile segnalare anche in forma anonima o sotto pseudonimo.

Per cifrare le segnalazioni inviate per email, è possibile utilizzare questa **PGP Public Key**.

COMPORTAMENTI RICHIESTI

Ti chiediamo di:

Non sfruttare la vulnerabilità o il problema che hai scoperto per trarne vantaggio;

- Non eseguire alcuna attività che possa danneggiare noi o i nostri utenti, interrompere il sistema o il servizio interessato o causare divulgazione non autorizzata di dati;
- Fare tutto quanto in tuo potere per evitare violazioni della privacy (perdita di confidenzialità, integrità, disponibilità dei dati) e/o deterioramento o sospensione dei servizi;
- Rispettare la privacy dei nostri utenti e / o clienti: è vietato accedere e/o utilizzare i dati personali trattati a seguito della rilevazione della vulnerabilità per scopi diversi dal rilevamento e gestione della stessa e/o per la protezione dei nostri utenti;
- Qualora la vulnerabilità rilevi una violazione di dati personali (perdita di confidenzialità, integrità, disponibilità dei dati personali) attuale o potenziale, inviare tempestivamente una notifica via email a dpo.fibercop[@]fibercop[.]com e a cirt[@]fibercop[.]com;
- Non apportare modifiche ai sistemi o alle applicazioni;
- Non utilizzare attacchi Denial of Service e brute force;
- Non effettuare scansioni automatiche aggressive;
- Non utilizzare tecniche di ingegneria sociale con nostri dipendenti o fornitori;
- Non effettuare attacchi alla sicurezza fisica;
- Non posizionare una backdoor nei sistemi. Inserendo una backdoor in un sistema, quel sistema diventa ancora più insicuro;
- Fornire informazioni sufficienti per riprodurre il problema, così saremo in grado di risolverlo il più rapidamente possibile. Di solito sono sufficienti l'indirizzo IP o l'URL del sistema interessato e una descrizione della vulnerabilità; tuttavia, per le vulnerabilità complesse potrebbero essere utili maggiori dettagli;
- Non divulgare a terzi dettagli relativi alla vulnerabilità fino alla sua risoluzione e coordinare preventivamente con noi qualsiasi comunicazione o pubblicazione riguardante la vulnerabilità stessa;
- Mantenere un atteggiamento responsabile anche dopo il rilascio della patch, valutando attentamente il tipo di informazioni rilasciate e sempre con lo scopo di preservare i nostri utenti e i loro dati.

IMPEGNI DI FIBERCOP

FiberCop si impegna a:

- prendere in carico la segnalazione;
- fornire un primo riscontro entro 7 giorni lavorativi con la nostra valutazione e una data di risoluzione prevista;
- mantenere riservate le informazioni ricevute;
- trattare i dati personali nel rispetto della normativa applicabile.

La Policy non autorizza attività illecite e non deroga alla normativa vigente. Ci riserviamo il diritto di gestire e agire contro segnalazioni e notifiche che non rispettano i criteri indicati nella nostra Responsible Disclosure Policy e nelle leggi applicabili.

RICONOSCIMENTI

Eventuali citazioni pubbliche o inserimenti in una "Hall of Fame" avverranno solo previo consenso espresso del segnalante.

Al momento non sono previsti compensi economici per le segnalazioni ricevute.

NOTE FINALI

La presente Policy:

- non costituisce un contratto né un'offerta al pubblico;
- non garantisce tempi o risultati specifici;
- può essere modificata o aggiornata da FiberCop in qualsiasi momento.