

1. SCOPO

La presente politica definisce il quadro di riferimento per proteggere riservatezza, integrità e disponibilità delle informazioni trattate da Dr. Feel S.r.l., incluse informazioni cliniche, dati personali e documentazione del Sistema di Gestione per la Qualità (SGQ), in coerenza con ISO 13485:2016 e principi ISO/IEC 27001.

2. PRINCIPI

- Minimizzazione dei dati e accesso basato su ruolo (need-to-know)
- Segregazione ambienti di sviluppo, test e produzione
- Cifratura in transito (HTTPS/TLS) per servizi esposti e integrazioni
- Gestione vulnerabilità (patch, npm audit, assessment e penetration test)
- Backup, ripristino e continuità operativa verificati periodicamente
- Tracciabilità delle modifiche software e degli accessi amministrativi

3. RESPONSABILITÀ

Direzione: approvazione politica e risorse.

Responsabile sicurezza / IT (Paolo De Angelis): implementazione controlli tecnici, monitoraggio, incidenti, evidenze audit.

Personale e fornitori: rispetto procedure, segnalazione incidenti e anomalie.

4. CONTROLLI TECNICI (SINTESI)

- Infrastruttura Microsoft Azure (VM EU), NSG, SSH non esposto, VPN Tailscale admin
- Applicazioni Dr.Feel: Firebase/GCP, header di sicurezza (CSP, HSTS, X-Content-Type-Options)
- Google Workspace drfeel.com: MFA, DLP, audit log, account nominativi
- Fornitori SaaS critici (Stripe, Whereby, Complai): assessment e checklist
- Registro incidenti sicurezza e piano risposta incidenti

5. SVILUPPO SICURO

Linee guida security-by-design e review del codice prima del deploy in produzione (documento dedicato nel SGQ).

6. FORMAZIONE E REVISIONE

Il personale coinvolto riceve indicazioni su privacy, sicurezza e uso strumenti aziendali.

La politica è riesaminata almeno annualmente o dopo incidenti gravi / cambi architetturali.

Documento pubblicato sul sito www.drfeel.com (footer).