Politica di sicurezza dello shop

Principi tecnici e organizzativi per l'ambiente Futura+Farmacia

DOCUMENTO PRELIMINARE — da verificare e approvare con il consulente privacy/legale prima della pubblicazione in produzione.

Titolare / organizzazione	Futura+Farmacia Società Cooperativa
Sede	Via Guido Reni, 2/2 – Palazzo Godoli, 40125 Bologna (BO)
Contatti	info@futurapiufarmacia.it – PEC futurapiufarmacia@legalmail.it – Tel. +39 051 2960264
Revisione	18 agosto 2026 – versione preliminare 0.1

1. Obiettivo

Questa policy riassume l'impostazione di sicurezza dello shop Futura+Farmacia. È un documento informativo e operativo preliminare: controlli, ruoli e fornitori devono essere approvati prima della produzione.

2. Accesso e identità

Account amministrativi nominativi, privilegi minimi, password robuste, autenticazione multifattore ove disponibile e revisione periodica delle autorizzazioni. Gli account demo e le relative credenziali sono ammessi esclusivamente in locale e non fanno parte del pacchetto di produzione.

3. Protezione applicativa

Runtime e plugin provengono da release compilate e versionate; gli aggiornamenti seguono verifica di integrità e collaudo. Il traffico pubblico usa TLS. Token API e segreti sono gestiti in archivi dedicati o Kubernetes Secret e non sono salvati nel repository, nei template o nelle pagine pubbliche.

4. API e integrazioni

Ogni integrazione usa un token dedicato, ambiti minimi e rotazione in caso di sospetto. L'URL e la documentazione possono essere pubblici agli amministratori; token e webhook secret restano riservati. Le operazioni in scrittura devono essere abilitate solo se necessarie e monitorate.

5. Dati, backup e ripristino

Backup cifrati o protetti, separati dall'ambiente primario e verificati con prove periodiche di ripristino. Tempi di conservazione, RPO e RTO devono essere formalizzati con il gestore dell'infrastruttura. I backup non sostituiscono le misure preventive.

6. Logging e monitoraggio

Registrazione degli eventi amministrativi, degli errori e dei segnali di sicurezza con accesso limitato e conservazione proporzionata. I log non devono contenere password, token, dati di pagamento completi o informazioni eccedenti.

7. Vulnerabilità e aggiornamenti

Dipendenze, immagini e componenti vengono inventariati e aggiornati secondo la criticità. Le modifiche sono provate in ambiente non produttivo e promosse con procedura tracciata. Le segnalazioni di sicurezza possono essere inviate ai recapiti aziendali.

8. Incidenti

Gli eventi sospetti sono classificati, contenuti, analizzati e documentati. Il titolare valuta con i referenti competenti eventuali obblighi di notifica e comunicazione nei termini applicabili, preservando le evidenze e correggendo le cause.

9. Continuità e Kubernetes

Configurazione, immagini e manifest sono versionati; i segreti restano esterni. Readiness/liveness probe, limiti di risorse, replica e procedure di rollback sono verificati nell'E2E prima del rilascio. Il bootstrap applica soltanto seed idempotenti approvati.

10. Responsabilità condivisa

Futura+Farmacia governa finalità, account, ruoli e fornitori; NetForges cura le attività tecniche previste dall'incarico; hosting, pagamenti e logistica mantengono le rispettive misure. I ruoli contrattuali e privacy devono essere formalizzati separatamente.

Fonti normative essenziali: Regolamento (UE) 2016/679; Codice in materia di protezione dei dati personali, come modificato; indicazioni del Garante per la protezione dei dati personali. Il testo deve essere allineato ai trattamenti effettivamente attivati prima del go-live.