SECURITY POLICY

Security Policy

1. Unsere Sicherheits-Grundsätze

myHVAC PRO behandelt die Sicherheit Ihrer Daten als zentrale Anforderung. Wir setzen anerkannte Sicherheitsstandards um und entwickeln unsere Maßnahmen kontinuierlich weiter.

2. Technisch-organisatorische Maßnahmen (TOMs)

- **Transportverschlüsselung:** TLS 1.2/1.3 für sämtliche Verbindungen, HSTS aktiv.
- **Datenspeicherung:** Datenbank verschlüsselt „at rest“, Backups verschlüsselt.
- **Passwörter:** bcrypt-Hash mit ausreichend Runden; Klartext-Passwörter werden nie gespeichert.
- **Authentifizierung:** JWT mit kurzer Laufzeit, Single-Active-Session-Mechanismus, Token-Rotation bei Login/Logout.
- **Rate-Limiting:** Schutz gegen Brute-Force, Account-Farming und API-Missbrauch.
- **Zugriffskontrolle:** Rollenbasierte Berechtigungen (Technician / Team-Owner / Admin); Prinzip der minimalen Rechte.
- **Logging:** Sicherheitsrelevante Ereignisse werden im Audit-Log dokumentiert.
- **Monitoring:** Aktives Fehler-Monitoring (Sentry), Alerting bei Anomalien.
- **Software-Aktualisierung:** Regelmäßige Updates der eingesetzten Komponenten.
- **Personal:** Datenschutzschulungen, Vertraulichkeitsverpflichtung.

3. Schwachstellen verantwortungsvoll melden (Responsible Disclosure)

Wir freuen uns über sicherheitsrelevante Hinweise. Bitte melden Sie potenzielle Schwachstellen ausschließlich per E-Mail an support@myhvac-pro.de mit dem Betreff *„Security Disclosure“*. Wir bitten Sie:

- uns angemessene Zeit (mindestens 90 Tage) für die Behebung einzuräumen;
- keine Tests durchzuführen, die andere Nutzer beeinträchtigen könnten;
- keine Daten dritter Nutzer zu kopieren, zu verändern oder zu veröffentlichen;
- uns die Schwachstelle nachvollziehbar zu schildern (Steps to Reproduce).

Wir bestätigen den Eingang innerhalb von 5 Werktagen und informieren über den Fortgang.

4. Sicherheitsvorfälle & Benachrichtigung

Im Falle eines Sicherheitsvorfalls mit Risiko für personenbezogene Daten benachrichtigen wir die zuständige Aufsichtsbehörde innerhalb von 72 Stunden (Art. 33 DSGVO) und betroffene Nutzer unverzüglich, sofern ein hohes Risiko vorliegt (Art. 34 DSGVO).