Firnkern – Merkblatt für Ihre IT

Firnkern GmbH i. Gr. · Stand 3. November 2026 · ohne Gewähr · firnkern.com/it/

Firnkern ist eine Software für Ihr Firmennetz, kein Cloud-Dienst: ein Server mit Browser-Oberfläche auf einem Windows-Rechner. Auf den Arbeitsplätzen wird nichts installiert.

Systemvoraussetzungen

	Mindestens	Empfohlen
Betriebssystem	Windows 10 oder 11, 64 Bit	Windows Server 2022 (laut IT-Anleitung auch Server 2019 oder neuer)
Rechner	2 Kerne, 4 GB frei	4 Kerne, 8 GB frei; keine Grafikkarte nötig
Platte	1 GB	30 GB mit Sprachmodellen und Aufnahmen
Arbeitsplätze	Chrome oder Edge, nichts zu installieren	

Der Installer (rund 781 MB) bringt seine Python-Laufzeit mit. Der Rechner läuft während der Arbeitszeit.

Netzwerk und Ports

- Eingehend TCP 8780 (änderbar mit `FIRNKERN_PORT`) von den Arbeitsplätzen; Firewall-Regel «Firnkern Server» optional im Installer.
- Ausgehend braucht der Server im Betrieb nichts. Aus dem Internet nicht erreichbar, solange kein Port freigegeben wird.
- Optional TCP 8790 für den Briefkasten (Handys von unterwegs), davor Reverse-Proxy mit HTTPS.

Betrieb als Dienst

- Start beim Hochfahren ohne Anmeldung: Aufgabe «Firnkern Server (Dienst)», Konto LOCAL SERVICE, Neustart bei Absturz (3 Mal). Daten in `%ProgramData%\Firnkern-Server\daten`. Alternative: Start bei Anmeldung (`Autostart-einrichten.bat`).

HTTPS im Firmennetz

- Mikrofon, Kamera, Offline-Modus und die Web-App am Computer brauchen https (oder localhost).
- Weg A (empfohlen): Zertifikat der Firmen-CA als `cert.pem` / `key.pem` in den Datenordner. Weg B: `firnkern-ca.crt` (aus `Zertifikat-erstellen.bat`) auf den Arbeitsplätzen eintragen. Weg C: Warnseite hinnehmen, nur für Tests.
- Ablauf des Zertifikats meldet Firnkern nicht.

Datensicherung und Wiederherstellung

- Tägliche automatische Sicherung, Tagessicherung alle 6 Stunden erneuert, 14 Stück. Admin: «Mitarbeitende» › «Sicherung» (Jetzt sichern, Download, Wiederherstellen mit Bestätigungswort).
- Aufgabe der IT: Datenordner täglich in die Firmensicherung; bei laufendem Server Dateien aus `sicherungen\` nehmen. Die Download-Sicherung enthält Schlüsseldateien (`ki_schluessel.txt` im Klartext, `geheimnis.key`): geschützt aufbewahren.

Updates

- Der Admin installiert selbst; nichts wird automatisch eingespielt. Vorher sichern (Server stoppen, Datenordner kopieren). Der Datenordner liegt ausserhalb des Programmordners.
- Update-Prüfung: optional, aus bis zum Einschalten durch den Admin.

Was die Software ins Internet sendet

- **Nichts ohne Zutun des Admins** (AGB 10.1, F4); Dossier-Inhalte nie. Optional: Meldedienst, Fehlerberichte, Update-Prüfung (Firnkern erhält IP-Adresse und Fassung).
- Einmalig, wenn ein Modell fehlt: huggingface.co (erhält die IP-Adresse, keine Inhalte). KI-Stufe 2 (Infomaniak, Genf, Modell Mistral) und Stufe 3 (Anthropic, USA) nur auf Wunsch mit eigenem Konto; mit `FIRNKERN_CLOUD_KI_AUS=1` dauerhaft verboten. Keine Telemetrie.

Installer: unsigniert

> Der Installer ist noch nicht signiert: Chrome kann «wird selten heruntergeladen» melden, Windows SmartScreen «Der Computer wurde durch Windows geschützt» (Weitere Informationen › Trotzdem ausführen). Prüfsumme vorher vergleichen (SHA-256 auf firnkern.com/testen/ bzw. `SHA256SUMS.txt`):
> `Get-FileHash -Algorithm SHA256 .\Firnkern-Setup-<Fassung>.exe`

Supportzeitraum und Kontakt

- Sicherheitsupdates je Hauptfassung mindestens 5 Jahre ab Markteinführung, kostenlos, auch im Lesemodus (AGB B4); Enddatum folgt mit dem Verkaufsstart. Unterstützt werden die aktuelle und die vorhergehende Hauptfassung.
- Support: Mo–Fr 9–17 Uhr (Schweizer Zeit), Antwort in der Regel innert 2 Arbeitstagen (Zielwert). info@firnkern.ch · Sicherheitslücken: security@firnkern.com