Firnkern – IT fact sheet

Firnkern GmbH i. Gr. · As of 3 November 2026 · without warranty · firnkern.com/en/it/

Firnkern is software for your company network, not a cloud service: a server with a browser interface on a Windows computer. Nothing is installed on the workstations.

System requirements

	Minimum	Recommended
Operating system	Windows 10 or 11, 64-bit	Windows Server 2022 (the IT guide also covers Server 2019 or newer)
Computer	2 cores, 4 GB free	4 cores, 8 GB free; no graphics card needed
Disk	1 GB	30 GB with language models and recordings
Workstations	Chrome or Edge, nothing to install	

The installer (about 781 MB) brings its own Python runtime. The computer runs during working hours.

Network and ports

- Inbound TCP 8780 (changeable with `FIRNKERN_PORT`) from the workstations; firewall rule «Firnkern Server» optional in the installer.
- In operation the server needs nothing outbound. Not reachable from the internet unless a port is opened.
- Optional TCP 8790 for the mailbox (Briefkasten, phones on the move), with a reverse proxy with HTTPS in front.

Running as a service

- Start at boot without sign-in: task «Firnkern Server (Dienst)», account LOCAL SERVICE, restart on crash (3 times). Data in `%ProgramData%\Firnkern-Server\daten`. Alternative: start at sign-in (`Autostart-einrichten.bat`).

HTTPS on the company network

- Microphone, camera, offline mode and the web app on the computer need https (or localhost).
- Option A (recommended): certificate from the company CA as `cert.pem`/`key.pem` in the data folder. Option B: register `firnkern-ca.crt` (from `Zertifikat-erstellen.bat`) on the workstations. Option C: accept the warning page, tests only.
- Firnkern does not warn when the certificate expires.

Backup and restore

- Automatic daily backup, daily backup renewed every 6 hours, 14 kept. Admin: «Employees» › «Backup» (start backup, download, restore with confirmation word).
- IT's task: include the data folder in the company backup every day; while the server runs, take the files from `sicherungen\`. The downloaded backup contains key files (`ki_schluessel.txt` in plain text, `geheimnis.key`): store them protected.

Updates

- The admin installs updates; nothing is installed automatically. Back up first (stop the server, copy the data folder). The data folder lies outside the program folder.
- Update check: optional, off until the admin switches it on.

What the software sends to the internet

- **Nothing without the admin's action** (Terms 10.1, F4); dossier content never. Optional: reporting, error reports, update check (Firnkern receives IP address and version).
- Once, if a model is missing: huggingface.co (receives the IP address, no content). AI level 2 (Infomaniak, Geneva, model Mistral) and level 3 (Anthropic, USA) only on request with your own account; permanently forbidden with `FIRNKERN_CLOUD_KI_AUS=1`. No telemetry.

Installer: unsigned

> The installer is not yet signed: Chrome may say «not commonly downloaded», Windows SmartScreen «Windows protected your PC» (More info › Run anyway). Compare the checksum first (SHA-256 on firnkern.com/en/try/ or `SHA256SUMS.txt`):
> `Get-FileHash -Algorithm SHA256 .\Firnkern-Setup-<version>.exe`

Support period and contact

- Security updates for each major version for at least 5 years from market launch, free of charge, also in read-only mode (Terms B4); end date follows with the start of sales. The current and the previous major version are supported.
- Support: Mon–Fri 9 am–5 pm (Swiss time), usually a reply within 2 working days (target). info@firnkern.ch · Vulnerabilities: security@firnkern.com