

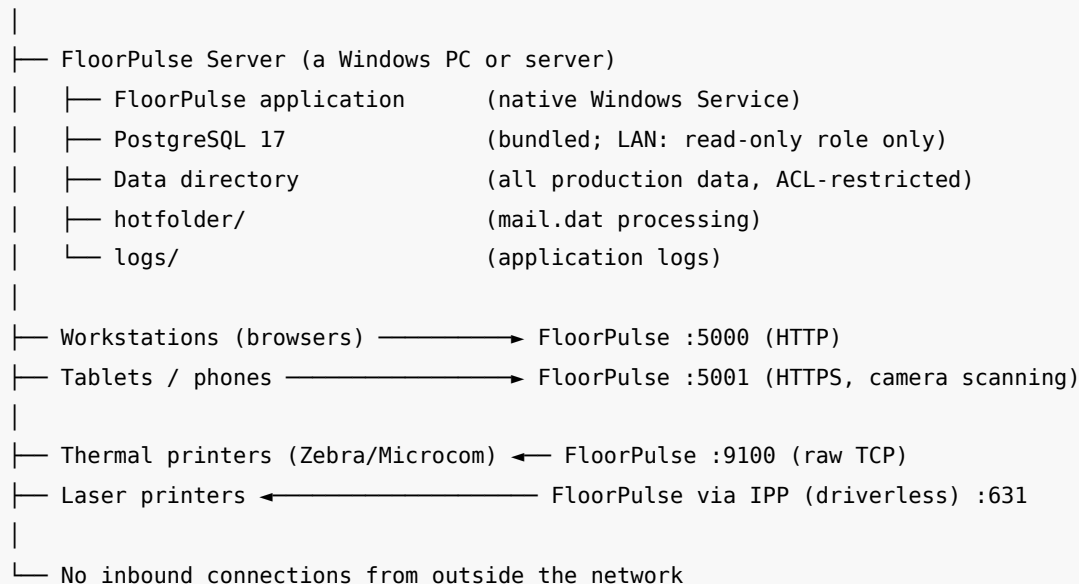
Everything your IT team needs before day one

FloorPulse is on-premises software. No data leaves your building. This page documents the network requirements, firewall rules, and security model so IT can review and approve before installation.

Architecture Overview

FloorPulse installs as a native Windows Service on a single machine inside your network, with PostgreSQL 17 bundled in. No cloud services, no external databases, no SaaS dependencies — and no outbound connections of any kind. The server has no HTTP client with which to make one.

Local Network (your facility)



What the native install means for IT

FloorPulse installs from a single signed Windows installer (EXE) that registers it as a Windows Service. It starts on boot and survives reboot and logoff with no user logged in, and requires no virtualization or special host configuration.

PostgreSQL 17 is bundled and installed alongside the application; its data lives at a known, ACL-restricted path on the host disk. Updating the application does not affect the data. **Schema changes ship inside the application code and apply automatically at startup — they are additive (new tables and columns are added in place), so older installations upgrade cleanly with no data loss and no manual DBA steps.** Major PostgreSQL version upgrades are handled by the installer with an

automatic pre-upgrade backup, validation, and rollback on failure, and have been tested successfully on production-scale data.

Why the database is embedded — and why that's good for IT

FloorPulse includes its own bundled PostgreSQL 17 instance, installed and managed by the FloorPulse installer. This is an **application database** — it functions as an internal component of the software, not a shared enterprise resource. It's comparable to the embedded database in a printer controller, a phone system, or a building access panel. It requires no DBA oversight, no backup coordination with other systems, and no shared infrastructure.

Why it must stay embedded:

- **Version-locked schema.** The database schema is tightly coupled to the application version. Every FloorPulse update includes automatic schema migrations that expect a specific database state. Pointing the application at an externally managed PostgreSQL instance introduces version drift — if the DBA applies a security patch or upgrade on a different schedule than the application, migrations can fail and production stops.
- **No shared data.** Nothing else reads from or writes to this database. There is no integration, no reporting system, and no ETL pipeline that depends on it. It stores only FloorPulse operational data (tray tags printed, barcodes scanned, job state). A pre-configured **read-only database user** is available if your team wants to query the data for custom reporting — without any risk of write conflicts. **Important:** direct SQL queries against the live database should be limited to simple, short-running reads. A malformed or expensive query (e.g., an unindexed join across millions of piece records) can saturate the host CPU and degrade production floor performance. For ad-hoc reporting, analysis, or query development, it is strongly recommended to work from a `pg_dump` backup restored on a separate machine — never experiment on the live production database.
- **Isolation is the security advantage.** Only the FloorPulse service, on the server itself, can write to the database. From the LAN, PostgreSQL admits exactly one role — the read-only reporting user `floorpulse_readonly`, password-authenticated (SCRAM-SHA-256) — on the port chosen at install (default 5433); every other role is refused before any password is checked. The installer adds one firewall rule for it, *FloorPulse PostgreSQL (read-only)*; if nobody will run reports from another machine, disable that rule and the database is reachable from the server alone. An externally hosted database would require network access rules, credentials management, and a larger attack surface. The embedded approach gives you a smaller security boundary, not a larger one.
- **Self-contained updates and recovery.** When FloorPulse is updated, the bundled database is updated alongside it — same installer, same moment, with automatic pre-upgrade backup and rollback. Backups are built in: Config → System schedules `pg_dump` backups, verifies each one by restoring it into a scratch database, and restores from the same panel. Scheduled backups are off until you turn them on. No coordination with a DBA team or shared maintenance window required.
- **No licensing cost.** PostgreSQL is open source (PostgreSQL License). The bundled instance adds no license fees, no per-core charges, and no CAL requirements. It runs as part of the application.

For IT's peace of mind: the database data directory lives at a known, ACL-restricted path on the host filesystem and can be included in your existing host-level backup routines (snapshots, rsync, or any agent you already run). Your monitoring tools can watch the FloorPulse Windows Service status just like any other service. FloorPulse's built-in health dashboard already tracks database connection pool utilization, disk usage, and memory — visible from any browser on the LAN.

Firewall Rules

FloorPulse requires **zero inbound connections from the internet**, and the server makes **zero outbound ones**. There is no firewall rule to add. You can verify this rather than take our word for it: `scripts/verify-zero-egress.sh` in the source tree checks it, and has a self-test that must FAIL against known-external addresses so you can confirm the checker is not rigged.

Outbound (FloorPulse server → internet)

Destination	Port	Protocol	Purpose	Required
<code>floorpulse.net</code>	443	HTTPS	Installer download — a person's browser , on whichever machine IT chooses, fetching the signed installer (EXE). The FloorPulse server never makes this request, and the machine that downloads need not be the server.	OPTIONAL

There are no required outbound rules, and the server originates none. Two optional ones used to be listed here — an opt-in update check and an opt-in license auto-renewal from GitHub. Both were **deleted** rather than defaulted off, because a capability that is switched off is still a capability, and a plant that has been through ransomware is right to care about the difference. FloorPulse operates fully offline: updates are applied by downloading the signed installer on any connected machine and transferring it to the server, and license keys are pasted into the configuration UI.

Inbound (LAN devices → FloorPulse server)

Source	Port	Protocol	Purpose	Required
LAN browsers (workstations, tablets, phones, supervisors)	5000	HTTP	Web UI access — all FloorPulse pages	REQUIRED
LAN browsers (devices using camera scanning)	5001	HTTPS	Camera barcode scanning requires HTTPS (browser security policy). Not needed if using Bluetooth/USB scanners only.	OPTIONAL
LAN browsers (device setup page)	5002	HTTPS	Trust check for the setup page: it answers one image so a device can confirm it trusts FloorPulse's certificate. Serves nothing else.	OPTIONAL
Other FloorPulse servers on the subnet	5099	UDP	Duplicate-server detection — a broadcast that stops two FloorPulse servers working the same hot folder. Local subnet only.	OPTIONAL

Source	Port	Protocol	Purpose	Required
Reporting tools (your BI, Excel, SQL clients)	5433 (default; set at install)	PostgreSQL	Read-only SQL access as <code>floorpulse_readonly</code> (SCRAM-SHA-256 password). No other database role is accepted from the network. The connection is not encrypted — disable the rule if you don't need it.	OPTIONAL

Outbound (FloorPulse server → LAN devices)

Destination	Port	Protocol	Purpose	Required
Thermal printers (Zebra, Microcom)	9100	Raw TCP	Tray tag and label printing — direct socket connection to printer	REQUIRED
Laser printers	631	IPP	Pallet placard printing via driverless IPP (FloorPulse is its own IPP client)	OPTIONAL

Optional: Conveyor Routing module

If the optional Conveyor Routing add-on is deployed, it runs as a second on-premises service that serves its browser UI on **5010 (HTTP)** and **5011 (HTTPS)**, plus a **controls socket API on TCP 10100** that palletizers, robots, and end-of-line controllers connect to for routing decisions. All three are **LAN-only** — no inbound internet, no additional outbound traffic, the same on-premises security boundary as the core platform.

Security Model

No data egress

All mail production data (barcodes, addresses, piece counts, job metadata) stays on the local machine. FloorPulse never sends production data to any external server — and makes no outbound requests at all, for any purpose.

No telemetry

No usage analytics, no crash reporting, no phone-home. The application does not track or report how it is used.

No cloud dependency

FloorPulse does not use AWS, Azure, GCP, or any cloud infrastructure. It runs entirely on hardware you control. If your internet goes down, production continues uninterrupted.

Authentication

Rank-based and deny-by-default. Operators (scan, print, view) need no login, so the floor is never interrupted. Configuration, job management and database operations are protected by access keys: named, individually revocable shared keys per access group, hashed with PBKDF2-SHA256. A fresh install is locked until its first Admin key is set.

License verification

Licenses are cryptographically signed (ECDSA P-256). The application verifies signatures using an embedded public key. License files contain only the customer name, expiration date, and feature flags — no sensitive data.

Data at rest

PostgreSQL data is stored in an ACL-restricted data directory on the host filesystem. Encryption at rest is the responsibility of the host OS (e.g., BitLocker on Windows, LUKS on Linux). FloorPulse does not implement its own disk encryption.

Data in transit

HTTPS (TLS) is supported for browser connections (port 5001) using FloorPulse's own certificate authority (trusted once on each device) or a certificate you supply. Printer communication uses raw TCP (industry standard for thermal printers — ZPL/LDS protocols have no TLS variant).

Update integrity

Update installers are code-signed (Authenticode) and downloaded over HTTPS from `floorpulse.net`. The signature can be verified before installing. Updates are never applied automatically — IT controls when updates are installed, and the installer takes an automatic pre-upgrade backup with rollback on failure.

Software Updates

FloorPulse **makes no outbound connections at all** — there is no setting to turn on. Earlier versions had an opt-in update check that fetched a static JSON file from `floorpulse.net`; it has been **removed outright**, along with the HTTP client, the URL setting and the flag that enabled it, because “it is configured not to” is a much weaker sentence than “it cannot” — and only the second is something your security team can confirm by reading the source. We notify you of new releases and deliver renewed license keys **by email**, and you apply them manually.

The server still tells an operator how old the running build is. That needs no network: the release date is embedded in the build, so the age is arithmetic against the clock and works on a machine that has never had a route to the internet.

Server on a routable network

1. We tell you a release is available, by email
2. IT reviews the release notes and downloads the signed installer (EXE) from `floorpulse.net`
3. IT runs the installer on the server at a convenient time
4. The installer takes a pre-upgrade backup, updates the service, and rolls back automatically if validation fails
5. Database migrations run automatically on startup

Air-gapped (no internet)

1. Download the signed installer (EXE) from the releases page on any internet-connected machine
2. Transfer the installer to the FloorPulse server via USB drive
3. Run the installer on the server
4. Same result — no internet required on the production server

Updates are never automatic. FloorPulse will never update itself, and it cannot learn that an update exists — it makes no outbound connections. We email you when a release is out; someone with administrator rights on the server runs the new installer when it suits you.

Security patches are announced the same way, by email, marked as security releases. FloorPulse shows how old the running build is, so an install that has fallen behind is visible on the server without any network access.

Server Requirements

Component	Recommendation	Notes
CPU	Intel Core i5 for fewer than 10 stations; Core i7 for 10 or more	Count every station, equipment stations and mobile units included. Server-class hardware is not required.
RAM	16 GB	FloorPulse and PostgreSQL typically use 1–2 GB; the rest serves the OS and database caching.
Disk	256 GB SSD for the OS, plus a 2 TB data drive (4 TB preferred)	Database size depends on mail volume and how long you keep history. Archiving a job deletes its piece records except those that were scanned.
OS	Windows 10/11 or Windows Server 2019+ (64-bit)	Installs as a Windows Service — starts on boot, no logged-in user required.
Software	None — the signed installer bundles everything	No separate .NET runtime, no separate PostgreSQL, no Java to install.
Network	Ethernet connection on the production floor LAN	One NIC is enough. Wi-Fi is acceptable for the server but wired is recommended.

Workstations, scanners and printers are covered in the [floor equipment guide](#).

Virtual machines & automation

We see no reason FloorPulse can't run on a properly configured VM (Hyper-V, VMware, Proxmox) — and a VM brings useful options, such as the replication-based disaster recovery described below.

One firm exception when you're driving automation. If you use the Routing module to control palletizers, robots, or end-of-line equipment, the fast socket protocol expects **sub-20 ms round trips**. That host — physical or virtual — should sit on a **network segment isolated from general office, file, and backup traffic**, with no contention on its NIC. Don't run the automation host on a busy shared VLAN, an oversubscribed hypervisor, or a Wi-Fi link. If you're supporting automation, spec the hardware and network for it — be smart, not cheap.

Compliance & Audit Notes

SOC 2 compatibility

FloorPulse does not process, store, or transmit data outside the customer's network. It is not a SaaS product and does not fall under most cloud-focused compliance frameworks. For SOC 2 audits: FloorPulse is an on-premises tool comparable to a local print server — it processes data within your security boundary.

PII handling

The mail.dat specification includes a file type (CDR — Certificate of Mailing Detail Record) that can contain recipient names and addresses. **FloorPulse does not import CDR records.** The application only imports the seven file types required for production floor operations (HDR, SEG, CSM, CQT, PQT, PBC, PDR) — none of which contain name or address data. Piece-level records contain Intelligent Mail barcodes with ZIP+4 routing codes only. This data is stored on the local machine and is subject to configurable retention policies.

Audit trail

Every tray tag print, pallet placard generation, and barcode scan is recorded with a timestamp and the station that did it. FloorPulse deliberately records stations, not individual people. This data is queryable via the built-in utility viewer or directly via SQL (a read-only database user is pre-configured).

Vendor access

FloorPulse does not include remote access, backdoors, or call-home functionality. The vendor has no ability to access your installation unless you explicitly provide remote access (e.g., TeamViewer, VPN) for support purposes.

Vendor Security Assessment — Pre-Answered

This section pre-answers the standard vendor security questionnaire (SIG/CAIQ/VSA). If your organization sends an annual security assessment, the answers below cover the typical questions. FloorPulse is on-premises software — many cloud/SaaS questions resolve to "customer-controlled."

Last updated: October 2026. Contact contact@floorpulse.net if your questionnaire includes questions not covered here.

1. Company & Product Information

Legal entity name	FloorPulseNet LLC
Product name	FloorPulse
Product description	On-premises production floor management software for Mail Service Providers. Barcode-driven tray tagging, pallet placard generation, and real-time job visibility.
Deployment model	On-premises only. Native Windows Service on customer-owned hardware. No cloud, no SaaS, no hosted option.

What data does the product process?	mail.dat files (USPS DTAC/IDEAlliance standard): job metadata, container/tray definitions, piece-level barcodes (Intelligent Mail barcodes). May include recipient ZIP codes and delivery route codes. All data stays on the customer's local server.
Does the vendor have access to customer data?	No. The vendor has no remote access, no API access, and no network path to customer installations. Support access requires the customer to explicitly grant it (e.g., TeamViewer, VPN).
Number of employees with access to customer data	Zero. See above.

2. Data Handling & Storage

Where is customer data stored?	On the customer's server, in a bundled PostgreSQL 17 database. Data is stored in an ACL-restricted data directory on the local filesystem. No data is stored off-premises.
Is data encrypted at rest?	The application does not implement its own disk encryption. Encryption at rest is the responsibility of the host operating system (BitLocker, LUKS, FileVault, etc.). The customer controls this.
Is data encrypted in transit?	HTTPS (TLS 1.2+) is supported for browser connections. The FloorPulse service talks to its database on the server itself (no network transit). Read-only reporting connections from the LAN are password-authenticated but not encrypted. Printer communication uses raw TCP (ZPL/LDS protocols — industry standard, no TLS variant exists).
Is data transmitted to third parties?	No. Production data never leaves the server. No third-party analytics, no subprocessors, no data sharing.
Is data transmitted to the vendor?	No, and not by policy — by construction. The server makes no outbound connections of any kind, so there is no request that could carry data whether or not it was meant to.
What PII is processed?	Piece-level records contain Intelligent Mail barcodes encoding delivery point ZIP+4 codes and routing information. No names, addresses, email addresses, phone numbers, SSNs, or financial data are imported. The mail.dat specification includes a CDR (Certificate of Mailing Detail Record) file type that can contain recipient names and addresses — FloorPulse explicitly does not import this file type. Only the seven file types required for production operations are consumed.
Data retention policy	Configurable by the customer. Archiving a job removes its piece-level barcode records, keeping only the pieces that production actually scanned or printed (the chain-of-custody evidence). Done jobs can be archived automatically after a set number of days (off by default). Whole jobs can be retained indefinitely or deleted on schedule. The customer controls retention through the Configuration UI.

Data deletion / right to erasure	The customer has full database access (admin and read-only users) and can delete any data at any time. A "Database Reset" function is available in the Configuration UI. The vendor has no data to delete because the vendor holds no customer data.
Data backup	Built in and customer-controlled. Config → System schedules <code>pg_dump</code> backups (off until enabled; default nightly at 02:00, newest 7 kept), verifies each by restoring it into a scratch database, and restores from the same panel. The installer also takes a backup before every upgrade. Backups stay on your hardware; the vendor does not perform or receive them.

3. Network Security

Does the product require inbound internet access?	No. No inbound connections from outside the customer's network are required or accepted.
Does the product require outbound internet access?	No, and it cannot use it. There is no setting that enables an outbound connection; the update check and license auto-renewal that once existed were deleted along with the HTTP client, so the answer does not depend on configuration. We deliver update notices and renewed license keys by email, and the installer is downloaded by a person on whichever machine suits them.
What ports does the product use?	Inbound: 5000 (HTTP), 5001 (HTTPS) — LAN only. Outbound LAN: 9100 (thermal printers, raw TCP), 631 (laser printers, IPP). Also inbound, optional: 5002 (HTTPS, device trust check), UDP 5099 (duplicate-server detection, local subnet), 5433 by default (PostgreSQL, read-only reporting role only). The optional Conveyor Routing module adds its browser UI on 5010 (HTTP) / 5011 (HTTPS) and a controls socket (TCP 10100) — all LAN-only. See Firewall Rules section for complete details.
Does the product open a listening port accessible from the internet?	No. The application listens on LAN interfaces only. Exposing it to the internet is not supported and not recommended.
Does the product use a VPN or tunnel?	No.
Does the product use WebSockets?	Yes. SignalR (WebSocket) is used for real-time updates between the server and browser clients on the LAN. This is internal traffic only.
TLS version	TLS 1.2 and 1.3, determined by the .NET runtime and host OS configuration.

4. Authentication & Access Control

Authentication method	Shared access keys with PBKDF2-SHA256 hashing (100,000 iterations, 128-bit salt), held in a cookie session. Each access group can have several named keys, each revocable on its own. Operators do not require authentication.
Does the product support SSO/SAML/OIDC?	Not currently. Access is by shared keys per access group. SSO integration is on the product roadmap for enterprise deployments.
Does the product support MFA?	Not currently. Physical LAN access is the primary security boundary. MFA is on the roadmap.
Does the product support RBAC?	Yes — rank-based and deny-by-default. Operator (scan, print, view — no authentication) is the floor; above it, access groups you name (e.g. Supervisor, Data Management) up to Admin, each with its own keys. Each protected action is assigned a minimum rank. Managing keys, installing the license and resetting the database are always Admin-only. There are no individual user accounts.
Session management	HTTP-only cookies, SameSite=Lax, 8-hour expiry. Elevated sessions are also tracked on the server, so an administrator can see them and revoke any one; revoking a key ends the sessions it opened.
Cookies and local storage	FloorPulse uses cookies and browser local storage for operational continuity on production floor devices. Workstation tablets store their workstation identity, assigned printer, sort direction, and active job — so an operator can power-cycle a tablet or refresh the browser and resume scanning immediately without reconfiguring. Supervisor stations store dashboard layout preferences. Blocking cookies or clearing local storage on these devices will force manual reconfiguration after every browser restart. These are first-party cookies from the FloorPulse server on the LAN — no third-party cookies, no tracking cookies, no advertising. Group Policy or MDM rules that clear browser data on close should exclude the FloorPulse server URL.
Password policy	No composition rules; a strength meter and blocklist guide the choice (NIST 800-63B approach), and sign-in is rate-limited to 5 attempts per minute per address. Keys are set by your administrator. Password is hashed with PBKDF2-SHA256 and never stored in plaintext.
Default credentials	None — and a fresh install is locked rather than open. Until the first Admin key is set, setting that key is the only protected action allowed; setting it also produces a one-time recovery code.

Emergency access / password recovery	Two recovery paths, matched to access level. Recovery code: a one-time code is generated when the admin password is first set; a supervisor can use it from any LAN browser to reset the password (rate-limited, single-use, rotated on use). Filesystem trigger: if the recovery code is also lost, an administrator with OS-level access drops a <code>reset-password.txt</code> file into a permission-protected admin directory (ACL-restricted to SYSTEM + Administrators on Windows); FloorPulse consumes it, resets the password, and writes back a freshly rotated recovery code. No vendor involvement, no cloud — works fully air-gapped.
---	--

5. Vulnerability Management

How are security vulnerabilities identified?	Automated CI/CD pipeline on every code push and weekly schedule: NuGet vulnerability scan (<code>dotnet list package --vulnerable</code>), filesystem/dependency scan (Trivy — fails on CRITICAL/HIGH), static analysis (GitHub CodeQL for C# and JavaScript — detects SQL injection, XSS, path traversal). Dependabot monitors NuGet packages and GitHub Actions for updates and creates PRs automatically. Manual code reviews supplement automated tooling. The frontend uses zero JavaScript frameworks (no React, Angular, Vue) — plain HTML/CSS/JS minimizes the attack surface.
Security development lifecycle	Monthly: automated dependency scans, GitHub Security tab review. Quarterly: manual endpoint-by-endpoint code review (auth, SQL, XSS, path traversal), vendored library version audit, credential scan, security header verification. Annually: threat model review and a security page accuracy check. Full audit process documented in project repository.
How are security patches delivered?	As signed installer (EXE) updates, and we notify you by email. The application never checks for them: it makes no outbound connections, and the opt-in update check earlier versions had was removed rather than defaulted off. Updates are never automatic — IT downloads the installer and runs it. See Software Updates.
How quickly are security fixes released?	FloorPulse runs on your own network with no internet access and makes no outbound connections, so it cannot be reached from outside your walls unless you expose it yourself. Security fixes go into the next release. A fix for a serious issue is released on its own, without waiting for the next scheduled release, and you are told by email.
Bug bounty program	Not currently. Security issues can be reported to contact@floorpulse.net.

OWASP Top 10 coverage	The application is developed with OWASP Top 10 awareness. Input validation at system boundaries, parameterized SQL (no string concatenation), HTML output escaping, CSRF protection via SameSite cookies, no deserialization of untrusted data. Login rate limiting (5 attempts/minute) prevents credential brute-force. Security headers (CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy) are set on all responses.
AI/LLM security posture	FloorPulse currently includes no AI or LLM features. A documented AI Integration Checklist is maintained in the project repository for review before any future LLM integration. The checklist addresses: prompt injection via user-controlled database fields (mail.dat free-text fields, configuration values, device names), structured output validation, and prohibition of executing LLM-generated commands or SQL.

6. Infrastructure & Operations

Cloud provider	None. FloorPulse is on-premises software. No cloud infrastructure is used for the product. (The vendor's website is hosted on Netlify — this is unrelated to the product.)
Data center / hosting location	The customer's facility. The customer chooses and controls the hardware.
Multi-tenancy	Not applicable. Each installation is a single-tenant deployment on customer-owned hardware.
Database architecture	PostgreSQL 17 runs as a bundled application database, version-locked to the application. It is not a shared enterprise database — it functions as an internal component (comparable to the embedded database in a phone system or access control panel). Only the FloorPulse service can write to it; from the LAN it accepts only the read-only reporting role. It requires no DBA management, and is updated alongside the application. See Architecture Overview for details.
Can the database be hosted externally?	Not supported. The application and database are version-locked — each application update includes schema migrations that expect a specific database state. Separating them introduces version drift risk and a larger attack surface. The embedded model is the intentional security and reliability architecture.
Service & process hardening	FloorPulse runs as a Windows Service (LocalSystem). Program files install under <code>C:\Program Files\FloorPulse\</code> ; the data directory and logs are ACL-restricted to SYSTEM + Administrators. The bundled PostgreSQL accepts only the read-only reporting role from the network.
Host OS hardening	Customer-managed. FloorPulse requires only a supported Windows version. Host OS patching and hardening are the customer's responsibility.

Logging and monitoring	Application logs are written to an ACL-restricted log directory on the host. The built-in health dashboard monitors CPU, memory, disk, database connections, and performance anomalies. Alerts are displayed in the web UI and pushed via WebSocket. Integration with external SIEM/log aggregators is possible by reading the log directory.
Uptime SLA	Not applicable. The software runs on customer hardware. Uptime depends on the customer's infrastructure. The application is designed to start automatically after power restoration (the Windows Service is set to start automatically on boot).

7. Business Continuity & Disaster Recovery

FloorPulse's database contains production state — which trays have been tagged, which pallets are complete, job progress. This data is useful but **not irreplaceable**. The source of truth is the mail.dat files from your presort software, which you already have. A fresh FloorPulse installation can reimport those files and be production-ready in minutes. This fundamentally changes the DR equation: you're not protecting a database, you're protecting uptime.

Three tiers of protection — choose the one that fits your operation:

Tier	Method	Recovery Time	Data Loss	Best For
1. Reinstall + Reimport	Run the FloorPulse installer on a spare Windows machine, paste the license key, reimport today's mail.dat files from presort output	~15 minutes	Production history (which trays were printed, timestamps). Current jobs are rebuilt from mail.dat files.	Single-shift shops, small operations, any shop that wants the simplest possible DR plan
2. VM Replication	Run FloorPulse in a VM (Hyper-V, VMware, Proxmox). Mirror or snapshot the VM to a standby host using your existing replication tools. If the primary fails, start the replica.	1–5 minutes	None (or minutes, depending on replication interval)	Shops that already manage VMs — uses tools and processes IT already has. No new concepts, no new software.
3. Database Backup	Scheduled <code>pg_dump</code> from the bundled database, or file-level snapshots of the data directory. Restore to any machine running FloorPulse.	5–15 minutes	Since last backup	Shops that want historical production data preserved (scan logs, tray event history, performance stats)

RPO (Recovery Point Objective)	Tier 1: current day's jobs (reimported from presort files). Tier 2: depends on VM replication interval (typically minutes). Tier 3: depends on backup schedule.
RTO (Recovery Time Objective)	Tier 1: ~15 minutes. Tier 2: 1–5 minutes (VM failover). Tier 3: 5–15 minutes (restore + restart).

Does the product have a single point of failure?	In the standard deployment (Tier 1), yes — one server. If it fails, Tier 1 recovery takes ~15 minutes on any available machine. Tier 2 (VM replication) eliminates the single point of failure entirely using your existing virtualization infrastructure.
What happens if the vendor goes out of business?	The software continues to operate indefinitely on existing installations. Perpetual license keys are available and will be issued to all active customers if the company ceases operations. They would be sent by email and pasted into Configuration, like any license key — installations make no outbound connections and do not fetch keys themselves. Source code escrow is available on request, arranged individually with a third-party escrow agent, for an additional annual fee that covers the escrow overhead.
Vendor lock-in / data portability	All data is stored in standard PostgreSQL tables with a documented schema. Customers have full SQL access via a pre-configured read-only database user. Data can be exported at any time using standard PostgreSQL tools. The application uses no proprietary data formats. Note: for reporting and analysis, restore a <code>pg_dump</code> backup on a separate machine rather than running ad-hoc queries against the live production database — an expensive query can consume host resources and impact production floor operations.

8. Third-Party Dependencies & Subprocessors

Subprocessors	None. No customer data is shared with or processed by any third party.
Third-party libraries	Server: .NET 10 runtime (Microsoft, MIT), Npgsql (PostgreSQL driver, PostgreSQL License), QuestPDF (PDF generation, MIT), SkiaSharp (graphics, MIT), ZXing.NET (barcode scanning, Apache 2.0), SharpIpp (driverless IPP printing client, MIT). Frontend: JsBarcode and bwip-js (barcode rendering, MIT), SignalR client (Microsoft, MIT). All dependencies ship inside the signed installer — no runtime downloads.
Open-source license compliance	All dependencies use permissive licenses (MIT, Apache 2.0, PostgreSQL License). No copyleft (GPL) dependencies. Full dependency list available on request.
Supply chain security	Dependencies are restored from NuGet.org during build and compiled into the application. The release installer is code-signed (Authenticode); its signature can be verified before installation.

9. Incident Response

Does the vendor have an incident response plan?	Yes. Security incidents affecting the product (e.g., a vulnerability in a dependency) are handled with: identification, patch development, patch release via a signed installer update, and notification by direct email to affected customers.
--	---

Breach notification timeline	Since the vendor holds no customer data, a data breach at the vendor does not expose customer data. If a vulnerability in the product is discovered that could allow unauthorized access, customers are notified by email as soon as it is confirmed, with what to do about it. Because FloorPulse runs on your own network with no internet access, such an issue is reachable only from inside your walls.
Security contact	contact@floorpulse.net

10. Physical Security

Data center physical security	Not applicable. The product runs on customer-owned hardware in the customer's facility. Physical security is the customer's responsibility.
Vendor office security	The vendor's development environment uses full-disk encryption and does not contain customer production data. Source code is stored in a private GitHub repository with 2FA-protected access.

11. Personnel Security

Security training	All developers follow secure coding practices (OWASP guidelines, parameterized queries, input validation). Code is reviewed before merge.
Access to customer environments	Zero employees have standing access to any customer environment. Support access is granted on a per-incident basis by the customer and revoked afterward.

12. Change Management

How are changes to the product managed?	Version-controlled source code (Git). All changes are committed with descriptions. Releases are tagged with semantic versioning (MAJOR.MINOR.PATCH).
How are changes deployed to customers?	As signed installer (EXE) updates. Customers control when updates are applied. No changes are pushed automatically. See Software Updates .
Can the customer decline or delay an update?	Yes, indefinitely. Updates are never forced. FloorPulse has no update check, so nothing in the product changes; the running build's age is shown so it is clear when an install has fallen behind.
Rollback capability	Yes. The installer takes an automatic pre-upgrade database backup and rolls back automatically if the update fails validation. A prior version can also be reinstalled from its signed EXE.

13. Compliance & Certifications

SOC 2 certification	Not applicable. FloorPulse is on-premises software — it does not operate a service that processes customer data. SOC 2 applies to service organizations. FloorPulse is comparable to a locally-installed print server or database application.
ISO 27001	Not currently certified. Planned for evaluation as the customer base grows.
HIPAA	FloorPulse does not process protected health information (PHI). Not applicable to mailing operations.
PCI DSS	FloorPulse does not process, store, or transmit payment card data. Not applicable.
GDPR	FloorPulse runs entirely on the customer's own server, and FloorPulseNet LLC never receives, stores or processes the data in it, so it is not a processor of that data. The customer is the controller of everything they import. If a customer grants us access to their server for support, we will sign a Data Processing Agreement (DPA) covering that access on request.
CCPA	Similar to GDPR: FloorPulse is a tool used by the customer. The customer determines what data is imported and how long it is retained. FloorPulse does not sell, share, or transmit personal information to any third party.
USPS compliance	FloorPulse generates tray tags and pallet placards in compliance with USPS Domestic Mail Manual (DMM) specifications: tray tags per USPS-L-3216A, pallet placards per DMM 204 Exhibit 3.4.3. Barcode formats: IMb (Intelligent Mail barcode) for tray tags, IMcb (Intelligent Mail Container Barcode) for pallet placards.

14. Frequently Asked Additional Questions

Does the product phone home?	No — and there is no “by default” attached to that. The product makes zero outbound connections, with no telemetry, no usage statistics and no version check. The opt-in update check earlier versions carried was deleted , together with the HTTP client and the setting that enabled it, so this is a property of the build rather than of its configuration. We notify you of updates by email.
Does the product install agents on other machines?	No. Workstations access FloorPulse through a standard web browser. Nothing is installed on operator devices.
Does the product modify the host OS?	It installs as a Windows Service and bundles PostgreSQL 17 under its own program and data directories. It does not alter unrelated system settings or write outside its own install and data locations.

Can the product be air-gapped?	Yes. FloorPulse operates fully without internet access. Updates can be applied via USB. Licenses can be pasted manually. No degradation in functionality.
What happens during a network outage?	It depends on where the FloorPulse server sits relative to the failure. If the server, workstations, and printers are all on the same switch or network segment, production continues uninterrupted — FloorPulse runs entirely on the local machine with no internet dependency. If the server is on the opposite side of a failed router, WAN link, or inter-building connection, workstations lose access. Recommendation: place the FloorPulse server as close to the production floor as possible — same room, same switch, same network segment as the workstation tablets and printers. For harsh production environments, consider an industrial fanless PC such as the OnLogic Karbon 803 or 804 (designed for dust, vibration, and temperature extremes common on mail production floors). This eliminates the dependency on upstream network infrastructure and IT closets.
Does the product support audit logging?	Yes. Every scan, print, reprint, job creation, job status change, and configuration change is logged with timestamps. Logs are queryable via the built-in UI and directly via SQL. Application logs are written to an ACL-restricted log directory on the host.
Can the product be uninstalled cleanly?	Yes. Uninstall via Windows Add/Remove Programs (or the installer's uninstall) removes the service, application, and bundled PostgreSQL. The data directory can be retained or deleted at your choice.
Insurance coverage	Errors & Omissions (E&O) and Cyber Liability insurance are being evaluated. Details will be available upon request once coverage is in place.
Does the product contain AI, machine learning, or LLM components?	No. FloorPulse contains no artificial intelligence features, no machine learning models, no large language model integrations, and no neural networks. All data processing uses deterministic algorithms — fixed-width record parsing, barcode lookup, SQL queries, and ZPL/PDF generation. No customer data is sent to any AI service, cloud inference endpoint, or training pipeline. The product does not use AI to make decisions, generate content, or analyze data. For organizations with policies restricting AI in production systems, FloorPulse is fully compliant — it is conventional software that does exactly what its code specifies, nothing more.

Quick Reference for IT Approval

Deployment model	On-premises, single machine, native Windows Service
Internet required	No — and not used, optionally or otherwise.

Data egress	None. Production data never leaves the server.
Outbound domains	None. The server contacts nothing — <code>floorpulse.net</code> is reached by a person's browser to fetch the installer, never by FloorPulse.
Inbound ports	5000 (HTTP), 5001 (HTTPS) — LAN only. Optional: 5002 (trust check), UDP 5099 (local subnet), 5433 (read-only reporting SQL). Optional Routing module: 5010 / 5011 (HTTP/HTTPS) + controls socket 10100, all LAN-only.
Outbound LAN ports	9100 (thermal printers), 631 (laser printers via IPP)
Software installed	None to pre-install — the signed installer bundles .NET, PostgreSQL 17, and all dependencies.
Auto-updates	Never. Updates require manual IT action.
Telemetry	None.
Remote access	None built in. Vendor has no access to your installation.

Questions? Contact contact@floorpulse.net

Generates a formatted PDF with today's date for your compliance records

FloorPulse — IT & Security Assessment

FloorPulseNet LLC — contact@floorpulse.net — floorpulse.net/security.html

FloorPulseNet LLC — contact@floorpulse.net — printed from floorpulse.net/security, where the current version always is.