

Deviceflow Vendor Questionnaire

Published date: July 29, 2026

Last updated: July 29, 2026

Policy owner: Anatoly Geyfman

Document ID: DF-VQ-001

Version: 1.1

Classification: Confidential

Supplier assessment for GxP computerized systems per GAMP 5 (2nd Edition) guidelines.

1. Company information

#	Question	Response
1.1	Company legal name	Deviceflow, Inc.
1.2	Company address	3945 SE Grant Ct Portland, OR 97214
1.3	Year founded	2024
1.4	Total number of employees	5
1.5	Primary contact for quality/compliance inquiries	Anatoly Geyfman anatoly@deviceflow.com
1.6	Website	deviceflow.com

Product information

#	Question	Response
1.7	Product name and current version	Deviceflow
1.8	Brief product description	Deviceflow is a cloud-based SaaS platform for medical device field operations. The system manages order processing, inventory tracking, rep management, account management, logistics coordination, and compliance documentation workflows for medical device companies.
1.9	GAMP 5 software category	Category 4: Configured Software Product Deviceflow is a commercially available application configured (not custom-coded) for each customer's specific business rules, workflows, user roles, and product catalogs.
1.10	Deployment model	Multi-tenant SaaS hosted on AWS (us-west-2). Containerized services on ECS Fargate. No on-premise installation required.
1.11	Industries served	Medical device distribution, medical device manufacturing, healthcare supply chain

2. Quality management system

#	Question	Response
2.1	Does the company have a documented quality management system?	Deviceflow maintains documented software development and quality practices. Formal QMS certification is not yet in place. See our SDLC policy for details.
2.2	Is the QMS certified to any standard?	We are currently undergoing SOC 2 Type II audit, expected close December 2026
2.3	Is there a designated quality/compliance role?	Jason Katzer, Head of Engineering is our designated quality & FDA validation owner
2.4	Are quality records maintained and retrievable?	Yes. Quality records including test results, release artifacts, and change history are maintained in version control and our project management system.
2.5	Is there a process for handling customer complaints related to software quality?	Customer-reported issues are tracked in our project management system, triaged by severity, and resolved according to priority.
2.6	Are internal audits conducted?	Ad-hoc reviews are performed. A formalized audit schedule is planned.

Regulatory awareness

#	Question	Response
2.7	Awareness of 21 CFR Part 11?	Yes. Deviceflow is designed with Part 11 requirements in mind, specifically electronic record integrity and audit trail controls. Deviceflow follows FDA guidance for Part 11 signatures, see questionnaire.
2.8	Awareness of GAMP 5 guidelines?	Yes. Deviceflow is classified as GAMP Category 4. Our validation support package is structured per GAMP 5 Second Edition (2022) guidelines. See our validation approach.
2.9	Awareness of EU Annex 11?	Yes. Deviceflow's data integrity controls, access management, and audit trail capabilities support customers subject to both FDA and EU requirements.

3. Software development lifecycle

#	Question	Response
3.1	Is there a documented SDLC?	Yes. See our SDLC and Quality Practices document.

3.2	Development methodology?	Agile. Work tracked in Linear with defined workflows.
3.3	How are requirements captured?	User needs documented in our project management system (Linear). Each requirement traces to user stories and automated tests.
3.4	Are requirements traceable to design and testing?	Yes. A Requirements Traceability Matrix (RTM) is published with every release linking user needs to user stories to tests.
3.5	Version/source control system?	Yes. GitHub with branch protection rules. All changes require pull requests with at least one peer review before merge to the main branch.
3.6	Are code reviews performed?	Yes. All changes require at least one peer review via pull request before merge.

Testing

#	Question	Response
3.7	Types of testing performed?	Unit tests, integration tests, automated browser-based E2E tests (Playwright/Chromium), static analysis, and manual testing.

3.8	Automated test suite?	Yes. Unit/integration tests run on every push via GitHub Actions CI. E2E validation tests (35+ URS-mapped tests) produce screenshots, video recordings, database audit log verification, and structured result files. Published at validation.deviceflow.com .
3.9	Are test results documented and retained?	Yes. Test evidence (results, screenshots, videos, audit logs) is committed to version control and published with each release. All prior versions remain accessible on the validation site.
3.10	Regression testing before each release?	Yes. Unit tests, linting, Semgrep analysis, and build verification run in CI on every merge. E2E validation tests run on release branches.
3.11	Staging environment?	Yes. Changes are verified in staging before promotion to production.

Release and deployment

#	Question	Response
3.12	Documented release process?	Yes. See SDLC and Quality Practices .
3.13	Release frequency?	Approximately weekly.

3.14	Release notes provided?	Yes. Each release includes change history, updated RTM, and re-executed test evidence.
3.15	CI/CD pipeline?	Yes. GitHub Actions with separate workflows for CI (lint, test, build), staging deployment (auto on merge to main), and production deployment (on merge to production branch). Includes health check gates and Slack notifications.
3.16	Rollback capability?	Yes. Releases can be rolled back if issues are discovered.

4. Change management

#	Question	Response
4.1	Documented change control procedure?	Yes. All changes tracked in Git and Linear with author, timestamp, description, rationale, and reviewer.
4.2	How are changes classified?	By scope and risk: feature changes, bug fixes, and infrastructure changes.
4.3	Who authorizes changes?	Changes require peer review and approval before merge.
4.4	How are changes communicated to customers?	Release notes with change history, stored in Github. We plan on flagging Material changes in advance.

4.5	Emergency/hotfix process?	Hotfixes follow the same review process with expedited timelines. Emergency releases may bypass the review processes.
4.6	Are all changes recorded?	Yes. Git history captures author, timestamp, description, and linked issue for every change.

5. Security and access controls

#	Question	Response
5.1	Unique user identification?	Yes. Every user has a unique account. Shared accounts not permitted.
5.2	Role-based access control?	Yes. Configurable roles and permissions.
5.3	Audit trail?	Yes. Audit trail of all user actions: user identity, timestamp, action, affected record, before/after values.
5.4	Data encrypted in transit?	Yes. HTTPS required for all connections.
5.5	Data encrypted at rest?	Yes. RDS storage encryption enabled on all database instances (mandatory). Database credentials stored in AWS Secrets Manager.

5.6	Session timeout?	Yes. Sessions terminated after inactivity.
5.7	Penetration testing?	AWS infrastructure certifications (SOC 2, ISO 27001) in place. Semgrep static analysis for security patterns runs in CI. Third-party penetration testing planned during SOC 2 Type II audit.

6. Backup, recovery, and business continuity

#	Question	Response
6.1	Backup frequency?	Automated daily RDS backups (03:00–04:00 UTC) with 7-day retention. We're committed to implementing a longer-term backup strategy during our SOC2 audit period (before December 2026).
6.2	Backup storage?	AWS-managed backups with Multi-AZ replication across us-west-2a, 2b, and 2c availability zones.
6.3	Restoration tested?	Documented and periodically tested.
6.4	Recovery Point Objective (RPO)?	<i>[To be completed — determined by backup frequency, up to 24 hours with daily backups]</i>

6.5	Recovery Time Objective (RTO)?	<i>[To be completed]</i>
6.6	Disaster recovery plan?	Multi-AZ database with automatic failover. Read replica available for promotion if needed. Docker images retained for 30 days in ECR for rollback.
6.7	Historical uptime?	99.9% with dedicated downtime windows during releases of no longer than 15 minutes (Mondays, 5pm-7pm PST)

7. Data integrity and electronic records

#	Question	Response
7.1	How are record modifications tracked?	All modifications captured in the audit trail with original value, new value, user, and timestamp. Original records never overwritten.
7.2	Electronic signatures per 21 CFR Part 11?	Electronic signatures are not currently in scope. Where e-signatures are required, that workflow is handled in the downstream system of record.
7.3	Data export?	Yes. Data can be exported in CSV format.

7.4	Protection against data deletion?	Yes. Critical records cannot be permanently deleted. Soft-delete used where removal is supported.
7.5	Database-level controls?	Yes. Production databases are not publicly accessible (VPC-only). Direct access requires VPN (Twingate) and is restricted to authorized engineering personnel. All application data changes go through the application layer where audit trail controls are enforced. AWS CloudTrail and VPC Flow Logs provide infrastructure-level audit logging.

8. Support and maintenance

#	Question	Response
8.1	Support channels?	support@deviceflow.com Intercom Chat Widget in the application
8.2	Support hours?	8am - 5pm PST
8.3	SLA?	<24 hours Monday - Friday 48 hours Saturday - Sunday
8.4	Known issue communication?	Customers are notified of issues affecting their use of the platform.

8.5	Customer training?	Onboarding support and documentation provided.
-----	--------------------	--

9. Validation support

#	Question	Response
9.1	Documentation to support customer validation?	Yes. Deviceflow provides a validation support package including: RTM, test evidence, release notes with change history (TBD), system documentation, this vendor questionnaire, and the validation approach document.
9.2	Requirements traceability matrix available?	Yes. Published with every release at validation.deviceflow.com .
9.3	Test evidence available for review?	Yes. Automated test results, screenshots, and recordings available per release.
9.4	Notification of changes requiring revalidation?	Yes. Customers notified in advance of changes that may impact validated functionality.

10. Third-party components

#	Question	Response
---	----------	----------

10.1	Third-party developers?	Yes, Deviceflow has a dedicated contract developer working on the team.
10.2	Third-party libraries?	Yes. Dependencies managed via pnpm with lockfile verification in CI. Dependency health checked by Sherif. Key frameworks: SvelteKit, Drizzle ORM, Playwright, Vitest.
10.3	Third-party integrations for critical functions?	Azure Cloud - AI services Google Cloud - AI services

11. Data management and privacy

#	Question	Response
11.1	Data storage location?	AWS us-west-2 (Oregon, United States). AWS S3 (global)
11.2	Data retention policy?	Data Retention Policy . In general, Deviceflow will retain current customer data in perpetuity of customer contract.
11.3	Data export on termination?	Yes. All customer data can be exported in standard formats upon request.

Attestation

I attest that the responses provided in this questionnaire are accurate and complete to the best of my knowledge.

Field	Value
Name	Anatoly Geyfman
Title	CEO
Signature	
Date	07/29/2026

Document revision history

Version	Date	Author	Description
1.0	May 2026	Anatoly Geyfman	Initial version
1.1	July 2026	Anatoly Geyfman	- Added links to Data Retention Policy - Updated SOC 2 status - updated commitment to longer-term backup policy - added details about Part 11 Signatures