

CUSTOMER COPY · SAMPLE

SDS INSTANCE SECURITY & DATA SPECIFICATION

SECURITY & DATA SHEET



SUBJECT // INSTANCE OF

NORTHWIND ROBOTICS

Electromechanical, robotic and heavy equipment rebuild
Own instance · United States (San Francisco)

1 // HOSTING

OWN INSTANCE

2 // ENCRYPTION

AES-256 · HTTPS

3 // BACKUPS

NIGHTLY · LOCKED

4 // ON EXIT

FULL COPY

SAMPLE DOCUMENT. Northwind Robotics is a hypothetical shop and its profile is invented. The controls are Anvil's, true of every instance. Printed by the same pipeline that issues your inspection reports, quotes and inspection and test plans.

01 SHOP PROFILE HYPOTHETICAL

SHOP	Northwind Robotics (hypothetical)
WORK	Electromechanical repair, robotic cell refurbishment, heavy equipment component rebuild
FLOOR	Strip and inspect, machining, welding, motor and drive rewind, assembly and test
PEOPLE AND DEVICES	38 users in 5 roles · 14 tablets and 6 phones paired
QUALITY SYSTEM	The shop's own, working to ISO 9001. The shop holds the certificate; Anvil keeps the evidence for its audits.
INSTANCE	Its own, hosted in the United States (San Francisco)
ASSISTANTS	Workflow expert on · Ask your shop off

02 CONTROLS REVIEWED 2026-10-24

S.1 CONTROL	HOSTING YOUR OWN INSTANCE ▶ Each customer runs on its own instance: its own application service, database, photo storage and credentials. One shop's records are never in another shop's database. ▶ Inside an instance, every record also carries its organisation, and every read is filtered by it. ▶ Hosted on a cloud server in the United States (San Francisco).	STATUS IN PLACE ■■■■■
S.2 CONTROL	ENCRYPTION ENCRYPTED IN TRANSIT, ON THE DEVICE, IN BACKUP ▶ On the tablet: the app's database is encrypted (SQLCipher, AES-256), with its key held in the device's secure keystore. A copy of the file is unreadable off the device. ▶ Between tablet, browser and server: every connection is HTTPS, with HSTS, so browsers never fall back to plain HTTP. ▶ Backups are encrypted on our server before they are uploaded; the storage provider cannot read them.	STATUS IN PLACE ■■■■■
S.3 CONTROL	RECORDS THAT HOLD A SAVED RECORD IS NEVER REWRITTEN ▶ A change is a new version, with who and when. The earlier version stays, and the database itself refuses to alter or delete it. ▶ Every sign-in and every administrator action is logged, append-only. ▶ An issued PDF is kept with a fingerprint (SHA-256), so a copy can be checked against the original.	STATUS IN PLACE ■■■■■
S.4 CONTROL	BACKUPS AND RECOVERY BACKED UP NIGHTLY, OFF SITE, LOCKED ▶ Every night: the database, then the photos, to separate off-site storage. ▶ Each backup is locked against deletion or change for 30 days, by the storage itself. ▶ Restores are drilled: a backup is downloaded, restored and checked against live counts. A missed backup or drill raises an alert.	STATUS IN PLACE ■■■■■

S.5

CONTROL

ACCESS

YOU DECIDE WHO SEES WHAT

- ▶ Accounts and roles are set by your administrator; permissions are checked on every request.
- ▶ Passwords of 12+ characters, stored only as a one-way hash. Repeated failed sign-ins lock the account; a password change signs out every other session.
- ▶ A phone or tablet must be paired to your shop with a one-time code. A lost device is revoked in one click and its app locks.

STATUS

IN PLACE**S.6**

CONTROL

OFFLINE AND SYNC

NO SIGNAL, NO LOST WORK

- ▶ Inspections, readings and photos are saved on the device first. Work carries on with no signal.
- ▶ When the signal returns, the device sends what changed; nothing on the server is overwritten.
- ▶ Two devices change the same record at once: it is flagged on both, a person checks it, and both versions stay on record.

STATUS

IN PLACE**S.7**

CONTROL

YOUR DATA

YOURS TO TAKE

- ▶ Reports, photos and job data download at any time: PDF, spreadsheet and photo archives.
- ▶ If you leave, you get a complete copy of everything your shop recorded. Then it is deleted from the live service, and the last encrypted backups expire within 35 days.
- ▶ No advertising, no tracking cookies, no analytics. Your data is never sold.

STATUS

IN PLACE**S.8**

CONTROL

WATCHING THE SERVICE

MONITORED, AROUND THE CLOCK

- ▶ An outside monitor checks the service every few minutes and alerts on an outage.
- ▶ Crash reports carry the organisation and device, never a person's name or address.
- ▶ Server sign-ins and privileged commands are logged and copied off site.

STATUS

IN PLACE**S.9**

CONTROL

ASSISTANTS

ASSISTANT FEATURES: OFF UNTIL YOU SWITCH THEM ON

- ▶ The workflow expert and Ask your shop are switched on per organisation, and are off by default.
- ▶ Every change an assistant proposes waits for a person to approve it.

STATUS

PER SHOP**03****WHO ELSE HANDLES DATA**

A small number of service providers support the service: server hosting, encrypted backup storage, crash reporting (no names) and email. The current list, with what each does and where, is available on request. Contact hello@anvilmro.com.

04**REVIEW**

PREPARED BY

ANVIL • 2026-10-24

ACCEPTED BY • NORTHWIND ROBOTICS

NEXT REVIEW

2027-04-24