

Security model

Engineering note for a responsible team leader. Not a legal document. If this and the build disagree, the build wins.

This is an engineering note. It describes how this Nexus Label Studio build actually behaves: from the first login to the end of a contract, every route, every lock, every place data lives or dies. It is not a contract, a privacy notice, or a lawyer's letter. If a line here and a line in the code disagree, the code wins.

Product: Nexus Label Studio. Operator: Tmi Varlamitis (VAT 3356674-8). DPO: Stefanos Varlamitis. The customer is the controller of their people's data; we process only what this build actually moves.

1. Two worlds that do not mix

There are two realms. They share a browser, not a store, not a session, and not a wipe.

Customer workstation (studio)

- Labels, org folders, SQL connections, the local vault, workstation backups, session nexus-portal-session-v1.
- A panic lockdown wipes this world. It does not touch housekeeping stores.

Housekeeping (Tmi Varlamitis)

- Customers, teams, members, invoices, cyber alerts, payroll, vault-snapshot policy.
- Store nexus-hk-v1 / nexus-hk-idb-v1 is the operator working copy on this machine. A workstation panic wipe cannot delete it. The desk is sealed AES-256-GCM (desk seal). Sandbox keeps the seal in a file; the production pin (nexuslabelstudio.com) keeps the ciphertext row in Neon. DEK in session, recovery wrap aside.

Sessions exclude each other: operator sign-in clears the portal session, and the reverse. One person is not both seats in one browser at once.

2. Routes (every door)

The browser only shows these doors. Each door is a gate, not just a page.

/	Portal gate. Email + secret. Also recognises an operator key. Login yard, cookie note, Turvalomake, privacy offer.
/studio	Workstation. Needs a portal session. Otherwise back to the gate.
/housekeeping	The desk. Needs an operator session and TOTP enrolment. Otherwise root.
/housekeeping/login	Operator password + TOTP (six boxes, auto-submit).
/housekeeping/claim/{token}	One-time claim or reset key. Burned by SHA-256. There is no second time.
/Turvalomake	Public PDF. Written consent to hand over a vault snapshot. No session.
/Turvallisuuismalli	This note in Finnish. Public, no session.
/Security-model	This note in English.
/Tuotemaarittely	Product specification in Finnish. Public, no session.
/Varautumissuunnitelma	Not public on the gate. Privileged seat: Options ? Security. /Contingency-plan in English.

Server APIs: /api/desk-seal (desk seal: sandbox file or Neon on the production pin), /api/cyber (alerts and lockdown notice). Auth middleware rejects scripted sibling-site requests (Sec-Fetch-Site). __Host- cookies and trustedOrigins sit beside that. Login-help and operator keys do not travel as studio URL query. Raw claim keys are not put in the client bundle.

3. Identities and seats

Floor operator

A member housekeeping listed. Work email, not public webmail (gmail, outlook, yahoo and the rest). The team must have a leader. First secret is a one-time OTP (alphabet without confusing glyphs). Then a local vault: password at least 12 characters, AES-256-GCM, PBKDF2-SHA-256, 600,000 iterations. The vault is never sent to housekeeping.

Responsible team leader

The team's leaderEmail. Privileged. Two-step verification is mandatory: RFC 6238 TOTP, 6 digits, 30 s, window ± 1 , ten one-time recovery codes. Without MFA the studio does not open. The same duty applies to sales-related roles (role name contains sales). Basis: GDPR Article 32, NIS2 (EU 2022/2555), Implementing Regulation 2024/2690, Finnish Cybersecurity Act 124/2025, Data Protection Act, Trade Secrets Act, Traficom risk guidance. MFA is not decoration.

Housekeeping operator

Tmi Varlamitis desk. Claim key nls-hk1- + 64 hex, or reset key. Hashed SHA-256 and compared timing-safe. A spent key does not open a new password set. The operator password must not be the key itself. TOTP is required before the desk. 15 minutes idle signs out.

Sales and other floor roles

Role is chosen on the workstation. Sales is privileged (other people's data, quotes). Other floor roles do not get MFA duty or the 15-minute idle, but vault and OTP still apply.

4. Sign-in, step by step

4.1 Customer gate (I)

- Email field. If the string looks like an operator key, the field becomes a key check. Partial, valid, spent, wrong: shown honestly.
- Public webmail is refused as webmail. Unknown corporate address the desk does not know: refused. It does not leak membership except for a listed member.
- Five failures in 24 hours lock the address for 24 hours (FAIL_LIMIT 5, FAIL_WINDOW 24 h). Success clears the counter.
- If the organisation is on the lockdown list (customer id or email), the gate refuses. That sticks until housekeeping lifts it.
- Team has no leader: no-leader. Member marked locked: locked.
- credential otp-pending: the secret is the OTP. Correct: phase set-password, local vault is born.
- Local vault exists: unlockVault. Wrong password: refused, no vault leak.
- Vault gone but OTP remains: set-password again. Else no-vault.
- Privileged seat without MFA: TOTP enrolment in six boxes, then ten recovery codes. Copy them now. They are not shown again.
- Already enrolled: six boxes; pasting six digits submits. A recovery code is accepted in place of TOTP and is spent.

4.2 Operator gate

- Claim route burns the genesis key. Reset route burns the reset key. Both are one-shot.
- Password + TOTP. The desk does not open without both. Password change on the desk needs current, next (? 12), and refuses the claim key as a password.

4.3 Login help

The gate has a help chat. No model, no store. At least 12 characters, 18 s cooldown, at most 4 messages in 10 minutes, 12 per session. Lexical filter: prompt injection, jailbreak, nls-hk key shape, URLs, zalgo. A key shape in the email field or the chat raises a cyber alert. An actor labelled malicious is denied; a pack goes to Kyberturvakeskus.

5. Session and idle

- Portal session lives only in sessionStorage key nexus-portal-session-v1: email, name, customerId, teamId, mfaOk, lastActive.
- Operator session: nexus-hk-session-v1. No email, only kind=operator.
- TOTP secret is open only for the session (totp-open). Sign-out clears it.
- Privileged seats (housekeeping, team leader, sales): 15 minutes idle signs out. Touch is mouse, key, pointer, scroll. A floor operator without privilege is not idled out.
- Closing the tab ends the sessionStorage session. The localStorage vault remains until panic or the user clears it.

6. What the workstation keeps

nexus-label-studio-v2	Studio: labels, layouts, SQL, org tree. localStorage / IDB.
nexus-vault-v1	Wrapped vaults per email. AES-256-GCM. Not sent to housekeeping.
nexus-client-backup-v1	Rotating workstation copies, about every 10 minutes, keep 12, DEK on the station. Panic destroys these.
Org folders	Locks, shares, lockout on a wrong folder code. Alias codes for sales.
Confidential fields	Password, token, host, email, company: blurred until the operator reveals them.

SQL and IndexedDB connections are the customer's. Panic drops them and deletes non-protected IDB databases.

7. Housekeeping desk seal

The desk does not rest in plaintext. Desk seal v1: AES-256-GCM. DEK wrapped with the operator password (PBKDF2-SHA-256). Recovery wrap is separate. The seal holds customers, teams, members, TOTP wraps, lockdowns, vault-snapshot policy, books. lastOtp does not go into the seal. Route /api/desk-seal. Local IndexedDB hydrates before the seal, and Kirjaudu enables only after that, so MFA state is not lost on refresh.

7.1 The workstation is the working copy

Store nexus-hk-idb-v1 is the operator working copy. Persist refuses to write an empty desk over a full one: if teams, members, customers or an operator are present, an empty state must not wipe them. A remote seal is not adopted if it is poorer than the local desk, or if it drops the operator.

7.2 Two tracks that do not mix

Sandbox and the production pin do not share a seal. Sandbox writes the file data/desk-seal.json. On the production pin (host nexuslabelstudio.com or www) the seal lives in Neon, table desk_seal, one row, encrypted JSON only. Vercel disk is ephemeral — do not leave the desk there. The sandbox file must not be served on .com, even if the build was marked sandbox. The host name decides.

- GET on production: the Neon row or empty. Never the sandbox file.
- PUT: an empty blob is not written over a live one (409). The operator hash does not change without a burned reset (409).
- If Neon will not take the write, the pin answers 503. The workstation keeps the local desk.
- A wrong password or a missing DEK wrap does not mint a blank desk over an existing seal.
- The production recovery key is a separate Neon row. GET does not return it.
- Auth is off. The row is unowned. That is why PUT is guarded, and the body is ciphertext, not a team list.

7.3 What the seal does not restore

The first hydrated workstation that still has a real desk seeds the Neon row. The sandbox does not restore production teams or operators. If the workstation and Neon are both empty, the only copy is an off-site vault snapshot (chapter 8).

8. Backups and vault snapshots

8.1 Workstation copy (dies in a panic)

Encrypted snapshots in IndexedDB on this machine. Restore from the File menu. Panic destroys them on purpose: an attacker does not get the floor copy if the machine is left open.

8.2 Off-site vault snapshot (survives a panic)

A responsible leader points the organisation at its own database: kind (PostgreSQL, MySQL, SQL Server, SQLite, MongoDB, HTTPS), host, port, database, table, account. The browser cannot open raw SQL, so an HTTPS gateway is required. Proxy and VPN (WireGuard, OpenVPN,

IKEv2, SOCKS5) travel as X-Nexus-Proxy and X-Nexus-Tunnel so your gateway can tunnel.

- Schedule: manual, hourly, 4 h, daily, weekly. Local hour and weekday.
- Max copies per person, default 7, range 1–50, override per email.
- Pack on a background thread: USTAR tar, then LZ77, then DEFLATE. File .tar.xz.
- On top of the already encrypted vault: AES-256-GCM wrap with the organisation wrap key. SHA-256 digest.
- Panic does not send a delete to the gateway. Copies stay on your network.

8.3 Recovery through Tmi Varlamitis

We do not fetch a snapshot from your network. If you want help, you choose a copy, fill Turvalomake, sign it, and hand the copy by secure mail or in person. In Kyberturvakeskus: the file + wrap key + a tick that the signed Turvalomake arrived. Without the tick, restore does not run. If the production desk is empty (the pin died on the old disk, the workstation was wiped), Neon does not invent teams. The off-site .tar.xz is the only restore.

9. Panic lockdown

The control sits in the title bar, between Search commands and feedback. Not on its own ribbon. Only an MFA-complete responsible member.

- One-time recovery code + authenticator 6 digits. Both. Wrong: nothing happens.
- Confirm by dragging left to right (pointer capture). Enter is not enough. A click is not enough.
- Effect: the organisation's teams and operators are destroyed from the customer's point of view, internal workstation data is wiped, database connections are dropped, local vaults and workstation backups go.
- Not wiped: the housekeeping desk, operator TOTP, cyber alerts, off-site snapshots, Turvalomake.
- A critical pack to Kyberturvakeskus: organisation, work email, time. So we can ask if everything is OK.
- Lockdown is sticky. A new sign-in to that organisation is refused until housekeeping restores the customer.

10. Checks and balances

No webmail

Same organisation

Seat cap

Timing-safe compare

OTP alphabet

Six boxes

Masked fields

Sibling isolation

No key in the URL

Personal gmail does not reach the floor. Organisation domain.

A team only accepts addresses in the same mail organisation.

Billing follows filled seats. Overflow is not silent.

Secrets and keys: timingSafeEqual, not ===.

No I, L, O, U — they collide with 1 and 0.

Paste fills all and submits. It does not wait for Enter.

Secrets, hosts, emails stay blurred until revealed.

Scripted same-site request from another grok.me app = 403.

Claim is a dedicated path. The key is not left on the studio history bar.

Desk seal

Desk encrypted: workstation IDB, Neon on production (desk_seal). Empty is not written over full. .com does not get the sandbox file. Refresh must not drop MFA.

Two wraps

Vault + snapshot wrap. One leak is not enough.

Two copy classes

Workstation dies in a panic. Off-site does not.

Written consent

Restore only with Turvalomake. No quiet fetch.

Idle

15 min for privileged seats. Unprivileged floor work may continue.

Lockout

5 wrong / 24 h. Folder codes have their own lockout.

Cyber alert

Key in the wrong field, malicious login-help, panic. JSON pack.

11. Contract life: start to end

11.1 Start

- Housekeeping creates the customer: company, VAT id, country, seats, cadence (month,

two months, quarter, half year, year). A 14-day trial exists as state, but the gate does not open without a listed member and a leader.

- KYC: none / pending / verified / rejected. ISO audit and 24/7 support are add-ons, not gate keys.
- Team + leaderEmail. The first OTP is shown once on the desk and queued as legal mail. SMTP honesty: the desk says when mail is a local queue.
- The member sets a vault. The leader sets TOTP. Only then the studio.

11.2 Use

- Seats billed on fill, reference 55 seats / EUR 949.99 / month (0% VAT in this product). 24/7 support floor EUR 3,200 / month for the reference team.
- Invoice states: draft, sent, paid, overdue. Overdue does not automatically kill the vault in this build — it is a books state, not a kill switch. To cut a contract, housekeeping marks the member locked, or issues a lockdown.
- The leader runs the team, pyramid, tasks, vault snapshots, panic control.

11.3 End (contract ends, company ends, panic, departure)

- Ordinary leave: housekeeping removes the member or marks locked. The vault stays on the machine until the user or a wipe removes it. Off-site snapshots stay on the customer's network — they are the customer's property.
- Ending the contract on Tmi Varlamitis's side: customer, teams, members leave the desk. That does not fetch .tar.xz copies from your network.
- Panic: see chapter 9. Workstation dies. Off-site lives. Restore only with Turvalomake.
- Destroying the PC: sessionStorage dies, localStorage does not, unless the disk dies. That is why 15-minute idle and the vault password exist.
- Right to be forgotten: ask housekeeping. Off-site copies on your network are yours to delete. We cannot see them.

12. What this system does not do

- It does not open a WireGuard tunnel from the browser. It sends tunnel metadata to your gateway.
- It does not keep label contents in a Tmi Varlamitis cloud. Studio is on the workstation.
- It does not keep teams in plaintext in Neon. desk_seal is ciphertext, one row, not a customer directory.
- It does not copy the production desk into the sandbox, or the sandbox desk-seal.json onto .com.
- It does not use Vercel disk as the home of the desk. The disk dies with the instance.
- It does not sell data. There is one cookie, afloat, to help the gate stay up.
- It is not an ISO 27001 certificate just because this PDF exists. ISO is a commercial add-on.
- It does not replace your own network and backup policy. The off-site snapshot is a tool, not a miracle.
- It is not legal advice.

13. Responsible leader checklist

- ☐ TOTP on. Recovery codes on paper, not in mail, not on a label.
- ☐ Vault password ? 12, not shared, not the OTP.
- ☐ Off-site gateway, wrap key and per-person limits set before the floor fills. The production seal is in Neon; if both the workstation and the seal are empty, only off-site restores.
- ☐ You know who may press panic. The slider is deliberate.
- ☐ Turvalomake printed and filed where you can find it without this workstation.
- ☐ Team only takes your domain. Webmail out.
- ☐ 15-minute rule: do not leave a privileged screen in the coffee room.

☐ If something feels wrong: Kyberturvakeskus sees the packs. Call.

14. Glossary

Vault	Local AES-256-GCM wrap, key derived from the password.
OTP	Housekeeping one-time floor secret that births the vault.
TOTP	Authenticator six digits, 30 s.
Desk seal	AES wrap of the housekeeping desk. IDB on the workstation; Neon (desk_seal) on the production pin.
Neon	Postgres of the production pin. One encrypted desk_seal row. Not a customer directory.
Lockdown	Sticky organisation panic.
Turvalomake	Written consent to hand over a snapshot.

© 2026 Tmi Varlamitis. Nexus Label Studio. This PDF is a working paper for a team leader.

Law names: GDPR (EU) 2016/679, NIS2 (EU) 2022/2555, Finnish Cybersecurity Act 124/2025.