

Turvallisuusmalli

Insinöörimuistio vastuulliselle tiiminvetäjälle. Ei oikeudellinen asiakirja. Koodi voittaa, jos tämä ja toteutus eroavat.

Tämä on insinöörimuistio. Se kuvaa, miten tämä Nexus Label Studio -toteutus tosiasiasa käyttäytyy: kirjautumisesta sopimuskauden loppuun, jokainen reitti, jokainen lukko, jokainen paikka jossa data elää tai kuolee. Se ei ole sopimus, tietosuojaseloste eikä lakimiehen teksti. Jos rivi tässä ja rivi koodissa eroavat, koodi voittaa.

Tuote: Nexus Label Studio. Toteuttaja: Tmi Varlamitis (Y-tunnus 3356674-8).

Tietosuojavastaava: Stefanos Varlamitis. Rekisterinpitäjä asiakkaan henkilötiedoille on asiakas itse; me käsittelemme vain sen, minkä tämä toteutus oikeasti siirtää.

1. Kaksi maailmaa, jotka eivät sekoitu

Järjestelmässä on kaksi erillistä valtakuntaa. Ne jakavat saman selaimen, mutta eivät samaa säilöä, samaa istuntoa eivätkä samaa pyyhkäisyä.

Asiakkaan työasema (studio)

- Täällä ovat tarrat, organisaatiokansiot, SQL-yhteydet, paikallinen holvi, työaseman varmuuskopiot ja istunto nexus-portal-session-v1.
- Hätätilalukitus pyyhkii tämän maailman. Housekeeping-säilöihin se ei koske.

Housekeeping (Tmi Varlamitis)

- Täällä ovat asiakkaat, tiimit, jäsenet, laskut, kyberhälytykset, palkanlaskenta ja holvin tilannekuva-asetukset.
- Säilö nexus-hk-v1 / nexus-hk-idb-v1 on operatorin työkappale tällä koneella. Työaseman hätäpyyhintä ei saa sitä pois. Pöytä sinetöidään AES-256-GCM-kääreellä (desk seal). Sandbox pitää sinetin tiedostossa; tuotantopinni (nexuslabelstudio.com) pitää salatun rivin Neonissa. DEK istunnossa, palautuskääre erikseen.

Istunnot sulkevat toisensa: kun operator kirjautuu, portal-istunto poistetaan, ja päinvastoin. Sama ihminen ei ole kahdessa roolissa yhtä aikaa samassa selaimessa.

2. Reitit (kaikki ovet)

Selain näyttää vain nämä ovet. Jokainen ovi on portti, ei pelkkä sivu.

/	Portal-portti. Sähköposti + salaisuus. Tunnistaa myös operator-avaimen. Login-yard, evästeilmoitus, Turvalomake, tietosuojatarjous.
/studio	Työasema. Vaatii portal-istunnon. Ilman sitä takaisin portille.
/housekeeping	Pöytä. Vaatii operator-istunnon ja TOTP-enrolmentin. Muuten juuri.
/housekeeping/login	Operatorin salasana + TOTP (kuusi ruutua, automaattilähetys).
/housekeeping/claim/{token}	Kertakäyttöinen claim- tai reset-avain. Poltetaan SHA-256-tarkisteella. Toista kertaa ei ole.
/Turvalomake	Julkinen PDF. Kirjallinen suostumus holvin tilannekuvan luovuttamiseen. Ei istuntoa.
/Turvallisuusmalli	Tämä asiakirja suomeksi. Julkinen, ei istuntoa.
/Security-model	Sama insinöörimuistio englanniksi.
/Tuotemaarittely	Tuotemääritys suomeksi. Julkinen, ei istuntoa.
/Kayttoehdot	Yleiset sovellettavat käyttöehdot. B2B-lisenssi.
/Varautumissuunnitelma	Ei julkinen. Etuoikeutettu paikka: Asetukset ? Turvallisuus. /Contingency-plan englanniksi.

Palvelimen rajapinnat: /api/desk-seal (pöydän sinetti: sandbox-tiedosto tai tuotannossa Neon), /api/cyber (hälytykset ja lockdown-ilmoitus). Auth-middleware hylkää sisärsivuston skriptatut pyynnöt (Sec-Fetch-Site). __Host-evästeet ja trustedOrigins täydentävät tämän. Login-help ja operator-avain eivät kulje URL-parametrina työasemaan. Raakaa claim-avainta ei laiteta selainpakkaukseen.

3. Identiteetit ja paikat

Lattiaoperaattori

Jäsen, jonka housekeeping on listannut. Työsähköposti, ei julkista webmailia (gmail,

outlook, yahoo ja muut tunnetut). Tiimillä on oltava vetäjä. Ensimmäinen salaisuus on kertakäyttöinen OTP (aakkosto ilman sekoittavia merkkejä). Sen jälkeen paikallinen holvi: salasana vähintään 12 merkkiä, AES-256-GCM, PBKDF2-SHA-256, 600 000 kierrosta. Holvia ei lähetetä housekeepingille.

Vastuullinen tiiminvetäjä

Tiimin leaderEmail. Etuoikeutettu. Kaksivaiheinen tunnistus on pakko: RFC 6238 TOTP, 6 numeroa, 30 s, ikkuna ± 1 , kymmenen kertakäyttöistä palautuskoodia. Ilman MFA:ta studio ei aukea. Sama velvoite koskee myyntirooleja (role, jonka nimessä on sales). Peruste: GDPR 32 artikla, NIS2 (EU 2022/2555), täytäntöönpanoasetus 2024/2690, kyberturvallisuuslaki 124/2025, tietosuojalaki, liikesalaisuuslaki, Traficommin riskienhallintaohje. MFA ei ole koriste.

Housekeeping-operaattori

Tmi Varlamitoksen pöytä. Claim-avain nls-hk1- + 64 heksiä, tai reset-avain. Avain tiivistetään SHA-256:lla ja verrataan vakioihin ajallisesti vakiossa (timing-safe). Poltettu avain ei avaa uutta salasananasetusta. Operatorin salasana ei saa olla itse avain. TOTP pakollinen ennen pöytää. 15 minuutin joutenolo kirjaa ulos.

Myynti ja muut lattiaroolit

Rooli valitaan työasemalla. Myynti on etuoikeutettu (toisten henkilötiedot, tarjoukset). Muut lattiaroolit eivät saa MFA-pakkoa eivätkä 15 minuutin joutenoloa, mutta holvi ja OTP koskevat silti.

4. Kirjautuminen, vaihe vaiheelta

4.1 Asiakkaan portti (/)

- Sähköpostikenttä. Jos merkkijono näyttää operator-avaimelta, kenttä siirtyy avaintarkistukseen. Osittainen avain, kelvollinen, käytetty, väärä: näytetään rehellisesti.
- Julkinen webmail hylätään syynä webmail. Tuntematon korporatiiviosoite, jota pöytä ei tunne: refused. Ei vuoda, onko osoite olemassa, muuten kuin listatulle jäsenelle.
- Viisi väärää yritystä 24 tunnissa lukitsee osoitteen 24 tunniksi (FAIL_LIMIT 5, FAIL_WINDOW 24 h). Onnistuminen nollaa laskurin.
- Jos organisaatio on lockdown-listalla (asiakas-id tai sähköposti), portti kieltäytyy. Tämä jää voimaan kunnes housekeeping purkaa lukituksen.
- Tiimillä ei ole vetäjää: no-leader. Jäsen merkitty locked: locked.
- credential otp-pending: salaisuus on OTP. Oikein: vaihe set-password, paikallinen holvi syntyy.
- Paikallinen holvi olemassa: unlockVault. Väärä salasana: refused, ei holvin vuotoa.
- Holvi kadonnut mutta OTP tallella: set-password uudelleen. Muuten no-vault.
- Vastuullinen paikka ilman MFA:ta: TOTP-enrolment kuudella ruudulla, sitten kymmenen palautuskoodia. Kopioi koodit nyt. Niitä ei näytetä uudelleen.
- Jo enrolloidulle: kuusi ruutua, liitä-kuusi-numeroa-lähetää automaattisesti. Palautuskoodi kelpaa TOTP:n sijasta, ja se kulutetaan.

4.2 Operatorin portti

- Claim-reitti polttaa genesis-avaimen. Reset-reitti polttaa reset-avaimen. Molemmat ovat kertakäyttöisiä.
- Salasana + TOTP. Pöytä ei aukea ilman molempia. Salasanan vaihto housekeepingissa vaatii nykyisen, uuden (min. 12) ja kieltää avaimen käytön salasanana.

4.3 Login-apu

Portilla on apuchat. Ei mallia, ei säilöä. Vähintään 12 merkkiä, 18 s jäähdytys, enintään 4 viestiä 10 minuutissa, 12 viestiä istunnossa. Lexikaalinen suodatin: prompt-injektio, jailbreak, nls-hk-avaimen muoto, URL:t, zalgo. Avaimen muoto sähköpostikentässä tai chatissa synnyttää kyberhälytyksen. Haitalliseksi merkitty toimija evätään; paketti menee Kyberturvakeskukseen.

5. Istunto ja joutenolo

- Portal-istunto elää vain sessionStorage-avaimessa nexus-portal-session-v1: sähköposti,

nimi, customerId, teamId, mfaOk, lastActive.

- Operator-istunto: nexus-hk-session-v1. Ei sähköpostia, vain kind=operator.
- TOTP-salaisuus avoinna vain istunnon ajaksi (nexus totp-open). Sulkeminen pyyhkii sen.
- Etuoikeutetut paikat (housekeeping, tiiminvetäjä, myynti): 15 minuutin joutenolo kirjaa ulos. Kosketus hiirellä, näppäimellä, kosketuksella, vierityksellä. Lattiaoperaattoria ilman etuoikeutta tämä ei koske.
- Välilehden sulkeminen päättää sessionStorage-istunnon. localStorage-holvi jää, kunnes hätätila tai käyttäjä tyhjentää sen.

6. Mitä työasemalla säilytetään

nexus-label-studio-v2	Studio: tarrat, asettelut, SQL, organisaatiopuu. localStorage / IDB.
nexus-vault-v1	Kääreholvit sähköpostia kohti. AES-256-GCM. Ei housekeepingille.
nexus-client-backup-v1	Työaseman kiertävät kopiot, noin 10 min välein, 12 kappaletta, DEK asemalla. Hätätila tuhoaa nämä.
Organisaatiokansiot	Lukot, jaot, lockout väärästä kansioskoodista. Alias-koodit myynnille.
Luottamukselliset kentät	Salasana, token, host, sähköposti, yritys: peitetään kunnes operaattori paljastaa.

SQL- ja IndexedDB-yhteydet ovat asiakkaan omia. Hätätila katkaisee ne ja pudottaa muut kuin suojatut IDB-kannat.

7. Housekeeping-pöydän sinetti

Pöytä ei makaa selväkielisenä. Desk seal v1: AES-256-GCM. DEK kääritään operatorin salasanalla (PBKDF2-SHA-256). Palautuskääre on erillinen. Sinetti sisältää asiakkaat, tiimit, jäsenet, TOTP-kääreet, lockdownit, holvin tilannekuva-asetukset, kirjanpidon. lastOtp ei mene sinettiin. Reitti /api/desk-seal. Paikallinen IndexedDB hydratoidaan ennen sinettiä, ja Kirjautu elää vasta sen jälkeen, jotta MFA-tila ei katoa refreshissä.

7.1 Työasema on työkappale

Säilö nexus-hk-idb-v1 on operatorin työkappale. Persist kieltää tyhjän pöydän kirjoittamisen täyden päälle: jos paikalla on tiimejä, jäseniä, asiakkaita tai operator, tyhjä tila ei saa niitä pyyhkiä. Etäsinettiä ei oteta, jos se on köyhempi kuin paikallinen pöytä, tai jos se pudottaa operatorin.

7.2 Kaksi rataa, jotka eivät sekoitu

Sandbox ja tuotantopinni eivät jaa sinettiä. Sandbox kirjoittaa tiedostoon data/desk-seal.json. Tuotantopinnillä (isäntä nexuslabelstudio.com tai www) sinetti asuu Neonissa, taulu desk_seal, yksi rivi, vain salattu JSON. Vercelin levy on katoava — sinne ei saa jättää pöytää. Sandboxin tiedostoa ei saa tarjota .com-osoitteessa, vaikka build olisi merkitty sandboxiksi. Isäntänimi ratkaisee.

- GET tuotannossa: Neon-rivi tai tyhjä. Ei sandbox-tiedostoa.
- PUT: tyhjää blobia ei kirjoiteta elävän päälle (409). Operator-hash ei vaihdu ilman poltettua resettiä (409).
- Jos Neon ei ota kirjoitusta, pinni vastaa 503. Työasema pitää paikallisen pöydän.
- Väärä salasana tai puuttuva DEK-kääre ei minttaa tyhjää pöytää olemassa olevan sinetin päälle.
- Palautusavain tuotannossa on erillinen Neon-rivi. Sitä ei palauteta GET:llä.
- Auth on pois. Rivi on omistamaton. Siksi PUT on suojattu, ja body on salakirjoitusta, ei tiimilistaa.

7.3 Mitä sinetti ei palauta

Ensimmäinen hydratoitu työasema, jolla on oikea pöytä, täyttää Neon-rivin. Sandbox ei palauta tuotannon tiimejä eikä operaattoreita. Jos työasema ja Neon ovat tyhjiä, ainoa kopio on off-site holvin tilannekuva (luku 8).

8. Varmuuskopiot ja holvin tilannekuvat

8.1 Työaseman kopio (nukkuu hätätilassa)

Salatut snapshotit IndexedDB:ssä tällä koneella. Palautus File-valikosta. Hätätilalukitus tuhoaa nämä tahallaan: hyökkääjä ei saa lattian kopiota, jos kone jää auki.

8.2 Off-site vault snapshot (ei nukahda hätätilassa)

Vastuullinen vetäjä osoittaa organisaation oman tietokannan: laji (PostgreSQL, MySQL, SQL Server, SQLite, MongoDB, HTTPS), kone, portti, kanta, taulu, tunnus. Selain ei avaa raakaa SQL:ää, joten HTTPS-yhdyskäytävä on pakollinen. Välityspalvelin ja VPN (WireGuard, OpenVPN, IKEv2, SOCKS5) kulkevat otsikoissa X-Nexus-Proxy ja X-Nexus-Tunnel, jotta teidän yhdyskäytävänne voi tunneloida.

- Aikataulu: manuaalinen, tunti, 4 h, päivä, viikko. Paikallinen tunti ja viikonpäivä.
- Kopioiden enimmäismäärä henkilöä kohti, oletus 7, raja 1–50, ylikirjoitus sähköpostille.
- Pakkaus taustasäikeessä: USTAR-tar, sitten LZ77, sitten DEFLATE. Tiedosto .tar.xz.
- Päällä jo salatun holvin: AES-256-GCM-kääre organisaation wrap-avaimella. SHA-256 tarkiste.
- Hätätila ei lähetä poistoa yhdyskäytävälle. Kopiot jäävät teidän verkkoonne.

8.3 Palautus Tmi Varlamituksen kautta

Me emme hae tilannekuvaa verkostanne. Jos haluatte apua, valitsette kopion, täytätte Turvalomakkeen, allekirjoitatte, ja luovutatte kopion turvapostitse tai käteen. Kyberturvakeskuksessa: tiedosto + wrap-avain + rasti että allekirjoitettu Turvalomake on saapunut. Ilman rastia palautus ei käynnisty. Jos tuotantopöytä on tyhjä (pinni kuoli vanhalla levyllä, työasema pyyhittiin), Neon ei keksi tiimejä. Off-site .tar.xz on ainoa palautus.

9. Hätätilalukitus (panic)

Painike otsikkopalkissa, Hae komentoja ja palaute-napin välissä. Ei omassa nauhassa. Vain MFA-valmis vastuullinen jäsen.

- Kertakäyttöinen palautuskoodi + authenticatorin 6 numeroa. Molemmat. Väärä: ei tapahdu mitään.
- Vahvistus liu'uttamalla vasemmalta oikealle (pointer capture). Ei Enter, ei hiirenklikkaus riitä.
- Seuraus: organisaation tiimit ja operaattorit tuhotaan asiakkaan kannalta, työaseman sisäinen data pyyhitään, tietokantayhteydet katkaistaan, paikalliset holvit ja työasemakopiot pois.
- Ei pyyhitä: housekeeping-pöytää, operatorin TOTP:tä, kyberhälytyksiä, off-site tilannekuvia, Turvalomaketta.
- Kriittinen paketti Kyberturvakeskukseen: organisaatio, työ sähköposti, aika. Jotta voimme kysyä, onko kaikki kunnossa.
- Lockdown on tahmea. Uusi kirjautuminen samaan organisaatioon evätään, kunnes housekeeping palauttaa asiakkaan.

10. Tarkistukset ja vastapainot

Ei webmailia	Henkilökohtaiset gmailit eivät pääse lattialle. Organisaation domain.
Sama organisaatio	Tiimiin voi lisätä vain saman sähköpostiorganisaation osoitteita.
Paikkakatko	Laskutus paikkojen mukaan. Ylitys ei ole hiljaista.
Ajallisesti vakio vertailu	Salaisuudet ja avaimet: timingSafeEqual, ei ===.
OTP-aakkosto	Ilman I, L, O, U — sekoittuvat 1:een ja 0:aan.
Kuusi ruutua	Liittäminen täyttää kaikki ja lähettää. Ei jää odottamaan Enteriä.
Peitetty kentät	Salaisuudet, isännät, sähköpostit blur-kenttinä, kunnes paljastetaan.
Sisareristys	Skriptattu same-site-pyyntö toisesta grok.me-sovelluksesta = 403.

Ei avainta URL:ssa	Claim-polku on dedicated. Avainta ei jätetä historian hakuriville studion kautta.
Desk seal	Pöytä salattuna: työaseman IDB, tuotannossa Neon (desk_seal). Tyhjää ei kirjoiteta täyden päälle. .com ei saa sandbox-tiedostoa. Refresh ei saa pudottaa MFA:ta. Holvi + tilannekuvan wrap. Yksi vuoto ei riitä. Työasema tuhoutuu hätätilassa. Off-site ei. Palautus vain Turvalomakkeella. Ei hiljaista hakua. 15 min etuoikeutetulle. Lattia ilman etuoikeutta saa tehdä työtä.
Kaksi käärettä	5 vääriä / 24 h. Kansikoodit omalla logoutillaan.
Kaksi kopioluokkaa	Avain väärässä kentässä, haitallinen login-apu, panic.
Kirjallinen suostumus	JSON-paketti.
Joutenolo	
Lockout	
Kyberhälytys	

11. Sopimuskausi: alusta loppuun

11.1 Alku

- Housekeeping luo asiakkaan: yritys, Y-tunnus, maa, paikat, laskutusrytmi (kk, 2 kk, kvartaali, puoli vuotta, vuosi). 14 vuorokauden kokeilu on olemassa tilassa, mutta portti ei avaudu ilman listattua jäsentä ja vetäjää.
- KYC: none / pending / verified / rejected. ISO-audit ja 24/7-tuki ovat lisävalintoja, eivät portin avaimia.
- Tiimi + leaderEmail. Ensimmäinen OTP näytetään kerran pöydällä ja lähtee lailliseen sähköpostijonoon. SMTP-rehellisyys: pöytä kertoo, jos posti on paikallinen jono.
- Jäsen asettaa holvin. Vetäjä asettaa TOTP:n. Vasta sitten studio.

11.2 Käyttö

- Paikat laskutetaan täytön mukaan, viite 55 paikkaa / 949,99 € / kk (0 % ALV tässä tuotteessa). 24/7-tuki lattia 3 200 € / kk viitejoukkueelle.
- Laskun tilat: draft, sent, paid, overdue. Ylitykset eivät katkaise holvia automaattisesti tässä toteutuksessa — overdue on kirjanpidon tila, ei kill-switch. Jos sopimus pitää katkaista, se tehdään housekeepingissa: jäsen locked, tai lockdown.
- Vetäjä hallitsee tiimiä, pyramidia, tehtäviä, holvin tilannekuvia, hätäpainiketta.

11.3 Loppu (sopimus päättyy, yritys lakkaa, paniikki, lähtö)

- Normaali lähtö: housekeeping poistaa jäsenen tai merkitsee locked. Holvi jää koneelle kunnes käyttäjä tai pyyhintä poistaa sen. Off-site tilannekuvat jäävät asiakkaan verkkoon — ne ovat asiakkaan omaisuutta.
- Sopimuksen päättäminen Tmi Varlamituksen puolella: asiakas, tiimit, jäsenet pois pöydästä. Tämä ei käy noutamaan .tar.xz-kopioita teidän verkostanne.
- Hätätila: katso luku 9. Työasema kuolee. Off-site elää. Palautus vain Turvalomakkeella.
- Koneen hävitys: sessionStorage kuolee, localStorage ei, ellei levyä tuhota. Siksi 15 min joutenolo ja holvin salasana.
- Oikeus tulla unohdetuksi: pyytäkää housekeepingia. Off-site kopiot teidän verkossanne ovat teidän poistettavianne. Me emme näe niitä.

12. Mitä tämä järjestelmä ei tee

- Ei avaa WireGuard-tunnelia selaimesta. Se lähettää tunnelin metadatan yhdyskäytävällemme.
- Ei pidä tarrojen sisältöä Tmi Varlamituksen pilvessä. Studio on työasemalla.
- Ei pidä tiimejä selväkielisenä Neonissa. desk_seal on salakirjoitusta, yksi rivi, ei asiakashakemisto.
- Ei kopioi tuotantopöytää sandboxiin eikä sandboxin desk-seal.json-tiedostoa .com-osoitteeseen.
- Ei käytä Vercelin levyä pöydän kotina. Levy katoaa instanssin mukana.
- Ei myy dataa. Evästeitä on yksi, afloat, kirjautumisen tueksi.
- Ei ole sertifioitu ISO 27001 -auditointi pelkästään tämän PDF:n takia. ISO-valinta on

kaupallinen lisä.

- Ei korvaa teidän omaa verkko- ja varmuuskopiopolitiikkaanne. Off-site snapshot on työkalu, ei ihme.
- Ei ole oikeudellinen neuvonta.

13. Vastuullisen vetäjän tarkistuslista

- ☐ TOTP päällä. Palautuskoodit paperilla, ei sähköpostissa, ei tarrassa.
- ☐ Holvin salasana ? 12, ei jaettu, ei sama kuin OTP.
- ☐ Off-site yhdyskäytävä, wrap-avain ja kopiorajat asetettu ennen kuin lattia täyttyy. Tuotantosinetti on Neonissa; jos sekä työasema että sinetti ovat tyhjiä, vain off-site palauttaa.
- ☐ Tiedätte, kuka saa painaa hätää. Liu'utus on tahallinen.
- ☐ Turvalomake tulostettu ja kansion paikassa, jonka löytää ilman tätä työasemaa.
- ☐ Tiimiin vain oman domainin osoitteita. Webmail pois.
- ☐ 15 min sääntö: älä jätä etuoikeutettua näyttöä kahvihuoneeseen.
- ☐ Jos jokin tuntuu väärältä: Kyberturvakeskus näkee paketit. Soittakaa.

14. Sanasto

Holvi	Paikallinen AES-256-GCM-kääre, avain johdetaan salasanasta.
OTP	Housekeepingin kertakäyttöinen lattiasalasana holvin syntyyn.
TOTP	Authenticator-sovelluksen 6 numeroa, 30 s.
Desk seal	Pöydän AES-kääre. Työasemalla IDB; tuotantopinnillä Neon (desk_seal).
Neon	Tuotantopinnin Postgres. Yksi salattu desk_seal-rivi. Ei asiakashakemisto.
Lockdown	Organisaation tahmea hätätila.
Turvalomake	Kirjallinen suostumus tilannekuvan luovuttamiseen.

© 2026 Tmi Varlamitis. Nexus Label Studio. Tämä PDF on työpaperi tiiminvetäjälle.

Lakitekstit: GDPR (EU) 2016/679, NIS2 (EU) 2022/2555, kyberturvallisuuslaki 124/2025.