

Security deficiency and remediation log — Linear export

doc id	RECORD-LINEAR-SECURITY-LOG
version	export 2026-09-08
status	record
owner	Olaf Jacobson

Exported from Linear (workspace *soon*, team S) on 2026-09-08, query "SOC 2". Every finding from the ISO 27001 / SOC 2 readiness work is tracked as an issue with an owner, a priority and a status; the rows below are the live tracker, not a copy. Issue numbers link to the checklist row they remediate.

Issue	Title	Owner	Priority	Status	Opened	Closed
S-414	Approve the ready policy set (30 documents)	Olaf Jacobson	Urgent	Done	2026-08-22	2026-09-08
S-298	CI/CD & IaC hardening: OIDC vs static IAM keys, prod test gate, unpinned actions	Olaf Jacobson	High	Done	2026-07-02	2026-07-24
S-306	Security response headers + CSP on Cloudflare Pages	Olaf Jacobson	High	Done	2026-07-03	2026-07-10
S-405	#61/62/64 Branch protection on main across all repos	Thomas Picauly	Urgent	In Progress	2026-08-22	—
S-411	#67/68 Collect vendor DPAs and SOC 2 reports	Alessandro Cardinali	Medium	In Progress	2026-08-22	—
S-297	Security logging & audit trail (PII scrubbing, no raw token logging)	Olaf Jacobson	High	In Progress	2026-07-02	—
S-299	AWS cloud posture (Prowler): public RDS, EC2 public IPs, RDS backups	Olaf Jacobson	High	In Progress	2026-07-02	—
S-288	ISO 27001 / SOC 2 Type 1 readiness — tracking	Olaf Jacobson	High	In Progress	2026-07-02	—
S-305	Security & privacy hardening + pen-test readiness (frontend)	—	High	In Progress	2026-07-03	—
S-412	#60 First database restore test	Thomas Picauly	Urgent	Backlog	2026-08-22	—
S-406	#34 Require two-factor authentication org-wide in GitHub	Thomas Picauly	Urgent	Backlog	2026-08-22	—
S-407	#36/42 Stop sending PII to Sentry	Thomas Picauly	Urgent	Backlog	2026-08-22	—
S-416	Settle report mechanics with GetAgency (assertion, TSC scope, as-of date)	Olaf Jacobson	Urgent	Backlog	2026-08-22	—
S-438	Evidence-capture sprint and hand pack to GetAgency by 11 Sep	Olaf Jacobson	Urgent	Backlog	2026-08-30	—
S-377	User MFA: passkey / TOTP, recovery codes, team "require MFA"	—	Urgent	Backlog	2026-08-17	—

Issue	Title	Owner	Priority	Status	Opened	Closed
S-386	Verify Stripe webhook signature	—	Urgent	Backlog	2026-08-17	—
S-415	#59/66 IR + DR tabletop (90 min, minuted)	Olaf Jacobson	High	Backlog	2026-08-22	—
S-410	#2/3/4 Collect signed NDAs and contractor agreements	Alessandro Cardinali	High	Backlog	2026-08-22	—
S-408	#49 Revoke unused DeepSeek / Mistral / xAI API keys	Thomas Picauly	High	Backlog	2026-08-22	—
S-409	#8/10 Org chart and job descriptions	Alessandro Cardinali	High	Backlog	2026-08-22	—
S-442	#5 Restart weekly ISMS cadence; minuted all-founders oversight session	Olaf Jacobson	High	Backlog	2026-08-30	—
S-477	#24 Approve security objectives; select ISO 27001 certification body	Olaf Jacobson	High	Backlog	2026-08-30	—
S-481	#25 Correct and approve the annual risk assessment	Olaf Jacobson	High	Backlog	2026-08-30	—
S-482	#28 First internal audit with Andrea	Olaf Jacobson	High	Backlog	2026-08-30	—
S-483	#29 Create and seed the CAPA log	Olaf Jacobson	High	Backlog	2026-08-30	—
S-485	#33 Approve access control policy; access matrix	Olaf Jacobson	High	Backlog	2026-08-30	—
S-486	#39 First quarterly access review (AWS/GitHub/Workspace/WorkOS)	Olaf Jacobson	High	Backlog	2026-08-30	—
S-487	#45 Production network diagram	Olaf Jacobson	High	Backlog	2026-08-30	—
S-489	#46 First annual security-group review	Olaf Jacobson	High	Backlog	2026-08-30	—
S-490	#65 Write and approve the BC/DR plan	Olaf Jacobson	High	Backlog	2026-08-30	—
S-491	Fill blanks in 9 one-fix-away ISMS documents and approve	Olaf Jacobson	High	Backlog	2026-08-30	—
S-493	Separate staging vs production RDS data (R-09)	Olaf Jacobson	High	Backlog	2026-08-30	—
S-443	Full test suite as prod deploy gate; SHA-pin actions	Olaf Jacobson	High	Backlog	2026-08-30	—
S-444	Publish corrected Trust Center	Olaf Jacobson	High	Backlog	2026-08-30	—
S-467	#1 HR Security Policy TODOs, approve, signed acknowledgements	Olaf Jacobson	High	Backlog	2026-08-30	—
S-473	#14 First security awareness training round; training log	Olaf Jacobson	High	Backlog	2026-08-30	—

Issue	Title	Owner	Priority	Status	Opened	Closed
S-439	#52 Pin down GetAgency pentest scope, timing, deliverables	Olaf Jacobson	High	Backlog	2026-08-30	—
S-371	Attach dsync Lambda to the VPC	—	High	Backlog	2026-08-13	—
S-295	Unauthenticated / cross-tenant webhooks & OAuth token storage	—	High	Backlog	2026-07-02	—
S-374	Security notification emails (new device, email change, MFA)	—	High	Backlog	2026-08-17	—
S-447	#11 Approve background-check procedure; nil-hires attestation	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-448	#36 Data classification levels and procedure	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-449	#38 New-starter access-provisioning checklist	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-450	#40 No-premises Physical & Environmental Security Statement	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-453	#41 Secure disposal & re-use in the Device Security Standard	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-456	#42 Statutory retention periods; approve retention policy	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-458	#43 Customer-data deletion runbook	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-460	#53 Rewrite Configuration Management Policy around Terraform	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-462	#57 Linear "security" label; quarterly incident-log entries	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-464	Internal-audit independence position	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-469	AWS Chatbot → Slack #Security for GuardDuty	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-471	Per-founder device attestation round	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-488	Linear twins for GitHub-only compliance issues	Olaf Jacobson	Medium	Backlog	2026-08-30	—
S-428	Retire api.soon.works stale DNS	Olaf Jacobson	Medium	Backlog	2026-08-25	—
S-300	Dependency & supply-chain remediation; Dependabot/secret scanning	—	Medium	Backlog	2026-07-02	—
S-301	Secrets hygiene: rotate & scrub	—	Medium	Backlog	2026-07-02	—
S-317	GDPR data export before deletion	—	Medium	Backlog	2026-07-03	—

Issue	Title	Owner	Priority	Status	Opened	Closed
S-379	Impersonation hardening	—	Medium	Backlog	2026-08-17	—
S-381	Compliance surface: security activity, admin log export, access review	—	Medium	Backlog	2026-08-17	—
S-290	Stripe webhook signature (duplicate of S-386)	Olaf Jacobson	Urgent	Duplicate	2026-07-02	—

Live tracker: <https://linear.app/soon> (team S). Statuses reflect Linear at export time; some items marked Backlog/In Progress were completed in the repositories before the ticket was updated (e.g. S-405 branch protection, evidenced separately under rows 61/62/64).

Rendered from SoonHQ/isms — ../../../../private/tmp/claude-501/-Users-olafjacobson-s-isms--claude-worktrees-iso-soc2-evidence-system-3febee/63d260ab-8eda-4043-a7d7-d392fe5f23b8/scratchpad/deficiency-log.md — source SHA-256
cb35233abe65bce4bbeabf64a0a8665de41e864c501261f9f6cc5cef2986cb84