

Vendor Risk Management Policy

Which third parties touch case data, what they are certified to, and how that is checked.

Version 1.0, effective 2026-08. Owner: Himaja Prabhala. Next scheduled review: 2027-02.

1. Purpose and scope

This policy inventories every third-party service that TRACE Nexus depends on, states what data, if any, flows through each one, and records the security certifications each vendor independently holds. It also sets the standard any future vendor addition must meet before it is allowed to touch case data.

2. Current vendor inventory

Vendor	Role	Case data exposure	Independent certifications
Supabase	Database, authentication, file storage	Yes, this is the system of record for all case data.	SOC 2 Type II, ISO/IEC 27001:2022
Cloudflare	Network edge, tunnel, edge authentication	In transit only, terminates and routes encrypted traffic; does not store case data.	SOC 2 Type II, ISO 27001, ISO 27018, ISO 27701
Oracle Cloud Infrastructure	Virtual machine hosting the application and detection engines	Yes, the VM's disk holds the running application and, transiently, files during processing.	ISO/IEC 27001:2013, SOC 1, SOC 2, SOC 3

3. What deliberately has no vendor in this table

No AI or large-language-model provider appears in this inventory, because none is called with case data. This is an architectural fact, not a policy promise: the detection engines are deterministic, rule-based Python functions running inside the Oracle Cloud VM already listed above, not a call to an external model API. There is no fourth row to add here for "the AI vendor" because there isn't one in the case-data path.

4. Standard for adding a new vendor

Before any new third-party service is given access to case data, or added to the infrastructure path case data travels through, it must be added to this table with:

- A written statement of exactly what data it would touch and why that access is necessary.
- Its own independent security certifications (SOC 2 Type II and/or ISO 27001 at minimum for anything touching case data directly).

- A data processing agreement, if the vendor is not already covered by one.
- Sign-off recorded in this document's revision history, not just a verbal decision.

5. Ongoing monitoring

Each listed vendor's security and status page is checked at each policy review for any material change (a lapsed certification, a disclosed breach, a change of ownership). This is currently a manual check performed at review time, not an automated feed, given the small number of vendors involved.

6. Review cadence

This policy and the vendor inventory are reviewed at minimum every six months, and immediately before onboarding any new vendor with access to case data.

TRACE Nexus. Internal governance document. Not for external distribution without review. Copyright 2026 Himaja Prabhala. All rights reserved.