

Access Control Policy

Who can reach what, and how that is actually enforced, not just intended.

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

1. Purpose and scope

This policy defines how access to TRACE Nexus and the case data it holds is granted, enforced, and reviewed. It covers three distinct layers, deliberately stacked rather than relied on individually, so that a failure in one layer does not by itself expose the system.

2. The three enforcement layers

Layer	What it enforces	Where it lives
Edge authentication	Single sign-on before any request reaches the application at all.	Cloudflare Access, network edge
Application gate	A shared workspace password, independent of individual accounts.	Next.js middleware
Per-user authentication and role	Individual identity and what that identity is permitted to see and do.	Supabase Auth plus row-level security

The public marketing pages are a deliberate, narrowly scoped exception to the first layer, carved out as separate, specifically-path-matched exceptions rather than by loosening the layer itself. No other route is exempt from all three layers.

3. Row-level security is the real boundary

Access control in this system is not application logic that happens to check permissions, it is enforced at the database level through row-level security policies, so that even a bug in the application code cannot return a row a policy does not permit. Append-only tables (the audit log, the decision-trace hash chain) have no update or delete policy defined for them at all, immutability by construction, not by convention.

4. Roles

Role	Intended access
Principal	Full access, including cross-case oversight views (Practice MI, Second review).
MLRO	Same oversight access as Principal, for anti-money-laundering sign-off responsibilities.
Analyst	Case workspace access. No oversight views.

Every account defaults to Analyst on creation. Elevation to Principal or MLRO is a manual action taken by the account owner, not a self-service option, and is itself an auditable event.

5. Provisioning and deprovisioning

This is currently a single-analyst tool, so provisioning is manual rather than a formal workflow. Before real client data or a real team is involved, this section needs to become a documented request-and-approval process with a defined owner who is not also the requester.

6. Credential handling

- No case data or credentials are placed in a URL or query string.
- Passwords are never handled or stored in plain text by application code; authentication is delegated to Supabase Auth.
- The shared workspace password (the application-gate layer) is treated as a genuine secret, not a formality, rotated if there is any reason to suspect it has been shared beyond its intended audience.

7. Audit logging

Every upload, view, edit, and disposition decision is written to the append-only audit log, including which account performed it and when. This log is the authoritative record for any access review, not a convenience feature.

8. Review cadence

Role assignments and this policy are reviewed at minimum every six months. Until a formal multi-user access review process exists, this review is the sole owner confirming that the single active account still has the access it should, and no more.

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