Accred

Accred security whitepaper

How the Accred suite is hosted, how it protects your data and your clients' Microsoft 365 tenants, and where it stands against common security frameworks.

Accred Products, LLC · accredproducts.com/security
Version 1.0 · November 6, 2026 · Describes the production services as of that date.
Every statement in this paper is backed by code or a live check recorded in Accred's internal security review of November 6, 2026.

1. Summary

Accred is a suite of Microsoft 365 tools for managed service providers (MSPs): Hub (sign-in, organizations, billing), Consult, Migrate, Connect, Manage, Assess, Protect, Devices, Aware, and Fleet. MSPs use it to run their own business and to act on their clients' Microsoft 365 tenants.

- Everything runs on Cloudflare and Supabase, behind HTTPS with HTTP Strict Transport Security.
- People sign in once, through Hub; each app opens with a signed launch that works once and expires within five minutes.
- Organizations are kept apart by row-level security on every Supabase table and by organization-scoped queries in the apps on Cloudflare D1.
- Credentials Accred keeps to reach other services are encrypted in the application with AES-256-GCM; tokens for AI assistants and sign-in handoffs are stored only as hashes.
- Nothing touches a client tenant until a tenant administrator grants Microsoft consent, and each app asks only for the permissions listed in section 5.
- Accred has self-assessed its controls against SOC 2, ISO/IEC 27001:2022 Annex A, NIST CSF 2.0, and CIS Controls v8 IG1.

2. Architecture and hosting

App	Runs on	Records	Files
Hub	Cloudflare Workers, Supabase Edge Functions	Supabase PostgreSQL	—
Manage	Cloudflare Workers	Supabase PostgreSQL (Hub project)	—
Manage Licensing	Cloudflare Workers	Cloudflare D1	—
Consult	Cloudflare Workers, Supabase Edge Functions	Supabase PostgreSQL	Supabase Storage (private buckets)
Migrate	Cloudflare Workers, Supabase Edge Functions, Migrate runner	Supabase PostgreSQL	Microsoft Azure Blob Storage (SharePoint and OneDrive staging, deleted within 7 days)
Connect	Cloudflare, Supabase Edge Functions, Connect relay on DigitalOcean behind a Cloudflare tunnel	Supabase PostgreSQL	Supabase Storage (private)
Assess	Cloudflare Workers	Cloudflare D1	Cloudflare R2 (evidence)

App	Runs on	Records	Files
Protect	Cloudflare Workers	Cloudflare D1 (backup index)	Cloudflare R2 (backup content)
Devices, Fleet, Aware	Cloudflare Workers	Cloudflare D1	—
accredproducts.com	Cloudflare Pages	—	—

Accred sends its own email (invitations, notices, Aware lessons and practice emails) from its own Microsoft 365 tenant, with Resend as a backup sender for Hub. Payments are processed by Stripe; Accred never stores card numbers.

3. Encryption

In transit

- Every Accred site and app is served over HTTPS and sends HTTP Strict Transport Security (up to two years, with `includeSubDomains`; the apps on accredproducts.com also send `preload`). Plain HTTP requests redirect to HTTPS.
- The Connect agent refuses to talk to a relay or service that is not HTTPS, except a local test relay on a private network address.
- Connect session traffic is encrypted with TLS between the computer, Cloudflare, the relay server (through an encrypted Cloudflare tunnel), and the technician. It is not end-to-end encrypted: the relay, which Accred operates, handles session content in memory.

At rest

- Supabase encrypts its databases and storage at rest. Cloudflare encrypts D1 and R2 at rest. Microsoft encrypts Azure Blob Storage at rest.

In the application

What	How it is stored
Microsoft 365 refresh tokens and cloud-source credentials (Consult, Migrate, Assess)	AES-256-GCM with a random 96-bit IV per value
AI provider keys an organization brings, integration tokens, webhook secrets, Slack bot tokens (Hub)	AES-256-GCM, bound to the organization and record so a copied value will not decrypt elsewhere; versioned keys so the key can be rotated without re-entering secrets
Manage's Microsoft sign-in tokens	Sealed with AES-256-GCM in the person's own browser cookie; never written to a database
App-only Microsoft tokens (Protect, Devices, Aware, Fleet, Manage)	Never stored; held in memory for minutes

What	How it is stored
AI assistant (MCP) access and refresh tokens, sign-in handoff nonces, Connect enrollment and join tokens	One-way SHA-256 hashes only
Connect device keys	Generated on the computer and never exported; Accred stores only the public key

4. Identity and access

- **Sign-in.** Hub signs people in with Microsoft (Entra ID) or with email. Microsoft sign-ins follow the organization's own multifactor and Conditional Access policies. Hub does not add its own second factor today.
- **App launches.** Hub signs each launch with a secret unique to that app (HMAC-SHA256), with issuer, audience, nonce, and a five-minute expiry. Each launch is recorded and refused if used twice. Apps check membership and role with Hub again while people work.
- **Roles.** Owner, Admin, Member, and Viewer. Destructive actions check the role on the server. Manage needs a second Owner or Admin to approve onboarding, offboarding, and access-review removals.
- **Organization isolation.** Row-level security is enabled on every table in the four Supabase projects (Hub 80, Consult 115, Migrate 109, Connect 45 tables at review time). Sensitive tables have no browser access at all. Apps on Cloudflare D1 carry the organization on every row and scope every query to it. An anonymous request to the Consult database for every one of its tables returned no rows (live check, November 6, 2026).
- **Per-tab organization.** Each browser tab holds its own organization, and servers check membership against that organization.
- **AI assistants.** Assistants such as Claude connect through Hub with OAuth 2.1 and PKCE. An organization chooses read or read-and-write access, an owner can turn assistants off, and every change an assistant makes is written to the audit log.

5. Microsoft 365 permissions

Nothing connects to a client tenant until a tenant administrator grants consent. Consent flows use PKCE, signed state, and a nonce, and bind the tenant to one Accred organization.

App	Access	Writes to the tenant
Hub	Sign-in only (`openid profile email offline_access`). Optional: Teams app install and Teams channel read for IT help.	Only the Teams app install, when an admin adds it
Assess	Application, read-only: directory, policies, audit logs, security, reports	None

App	Access	Writes to the tenant
Manage	Read access to directory, policy, security, and Intune data; group membership changes	Group membership (access reviews, onboarding, offboarding, playbooks), after confirmation or second approval. Manage Plus, a separate app, adds broader write access when an organization buys it.
Protect	Application: users, mail, and files	Restore only; a restore never replaces an existing item
Devices	Application: Intune read; device sync and app assignment	Only after an admin turns actions on; wipe and retire are never sent
Aware	Application: Attack Simulation Training read; optional launch	Launches Microsoft simulations only after someone confirms the client agreed
Migrate	Application and one-time delegated consent: broad read and write in source and destination tenants, as any tenant-to-tenant migration needs	Copies into the destination tenant; changes the source only in Cutover steps an operator runs
Consult	Read-only directory data; optional per-user mail for client communications	Sends mail only for the person who connected it
Fleet	Reads GDAP relationships (planned; not live yet)	None

6. Remote support (Connect)

- **Consent.** For an attended session, the person at the computer chooses Allow or Deny. Deny is the default, and no answer in 60 seconds denies. Unattended access skips the prompt; a full install turns it on unless the organization turns it off.
- **Device identity.** Each computer has a P-256 key that never leaves it. Heartbeats, tickets, and claims are signed with it.
- **Tickets.** A technician’s session ticket is issued only after Hub re-checks access and role, works once, expires in two minutes, and opens only the computer whose key it names.
- **Updates.** The agent and technician app install an update only after its RSA-PSS signed manifest, version, size, and SHA-256 hash check out.
- **AI-assisted support.** Off by default for an organization. Assistants need an Owner or Admin role; read-only triage needs no approval, and risky or destructive steps wait for a technician to approve. Command output is redacted for keys and tokens. Every step is kept in an append-only log.
- **Recording.** A technician can record a session to their own computer after confirming a notice. Accred does not store recordings.

7. AI and your data

- The Hub assistant sends the question and the app data needed to answer it to the provider the organization picks: Anthropic through Accred, OpenRouter (which routes to Anthropic, OpenAI, Google, and DeepSeek models), or the organization's own key for Anthropic, OpenAI, Google, or OpenRouter. Accred does not log request bodies.
- Keys an organization brings are encrypted with AES-256-GCM, checked when saved, and never shown again.
- An assistant changes something only after a person presses Run on a confirmation Accred builds on the server.
- Assess asks OpenRouter to route only to providers that do not keep the data, and never uses AI to compute a score.
- Manage, Protect, Devices, Fleet, and Aware call no AI provider themselves; their data reaches an assistant only through Hub, to the assistant a person connects.

8. Logging

- Hub and each app keep an audit log of changes: who, what, when, and the target. Browsers cannot write to Hub's audit log.
- Manage Licensing's audit log is append-only and hash-chained (HMAC-SHA256 per organization), so a changed or removed entry shows when the chain is verified.
- Connect's AI-assisted actions are kept in a table that refuses edits and deletes, even from Accred's own services.

9. Building and running the software

- Changes go through pull requests with automated tests, type checks, and builds before release, and every release is recorded in each app's changelog.
- Strict Content Security Policies: scripts load only from Accred with hashes or nonces, framing is blocked, and plugins are off.
- No secrets are kept in source code; a review of every repository found none committed.
- Accred checks dependencies across every repository with `npm audit` and `dotnet list package --vulnerable`.
- Each app publishes a `security.txt` with Accred's security contact.

10. Data retention and deletion

- Accred Protect keeps backups for the period the organization picks (30, 90, or 365 days, or 7 years), and deletes content no version uses after a 24-hour grace period.
- Migrate's staged files are deleted after the batch completes, and in any case within 7 days.

- Connect log bundles are deleted after 7 days, and screen previews after one hour.
- Other customer data is kept while the organization uses Accred. When an organization leaves Accred, its data is deleted on request.

11. Subprocessors

Cloudflare, Supabase, Microsoft (Microsoft 365 email and Azure storage), Resend, Stripe, DigitalOcean, OpenRouter, and Anthropic. The current list, with what each one does, is at accredproducts.com/subprocessors. Accred gives at least 30 days' notice before a new subprocessor starts processing personal data.

12. Compliance

Accred has self-assessed its controls against the SOC 2 Trust Services Criteria, ISO/IEC 27001:2022 Annex A, NIST Cybersecurity Framework 2.0, and CIS Controls v8 Implementation Group 1, and has prepared a CSA CAIQ-Lite questionnaire. The Data Processing Addendum covers GDPR, UK GDPR, and CCPA, with Standard Contractual Clauses. Customers can ask for the self-assessments.

13. Reporting a security issue

Email hello@accredconsulting.com with "Security" in the subject. Include steps to reproduce, and do not access other customers' data. Accred acknowledges every report and keeps the reporter informed. The contact is also published at accredproducts.com/.well-known/security.txt.