

# Access Control Policy

DOVRI TECHNOLOGIES LLC · VERSION 1.0 · EFFECTIVE 9 OCTOBER 2026 · NEXT REVIEW 9 OCTOBER 2027

This policy states who may access Dovri systems and member data, how that access is granted and authenticated, and how it is changed, reviewed and removed. It sits under the Dovri Information Security Policy and expands its access control section.

## SCOPE AND OWNERSHIP

This policy applies to every account, credential and key that can reach a Dovri production system or member data – human or machine – and to everyone who works on Dovri in any capacity. Maurice Ugbe, Founder and Chief Executive Officer, is accountable for access control and owns this policy. Dovri Technologies LLC is a Virginia limited liability company and currently has no employees other than the founder; where a control below describes handling a departure or transfer, it applies from the first time a person's access changes. This policy is reviewed at least annually and whenever responsibilities, systems or partners change.

## 01 Named accounts

- Every person with access to a Dovri system has a unique account in their own name.
- Shared or generic logins are not permitted on any system that stores or processes member data.
- Personal accounts are not used for Dovri systems where the provider supports an organisation or team account.
- An account is created only after the access it needs has been identified and recorded.

## 02 Least privilege

Access is granted at the minimum level needed to do the work, and no broader. Where a provider offers scoped permissions, the narrowest scope that satisfies the need is used rather than a general administrative role.

- Administrative access is granted only where the task cannot be completed without it.
- Read-only access is preferred wherever reading is sufficient.
- Access to production is separate from access to development and test systems.
- A request for broader access is granted only with a recorded reason, and is reduced again once the work is done.

### 03 Authentication

- Multi-factor authentication is required on every system that stores or processes member data and on every administrative console – hosting, DNS, source control, database, error monitoring, and payment and data partner dashboards.
- Where a provider offers more than one second factor, an authenticator application or hardware key is used in preference to SMS.
- Passwords are unique per system, generated at length by a password manager, and never reused.
- Credentials are stored only in the password manager. They are not written into documents, spreadsheets, notes, chat messages or email.
- Recovery codes are stored in the password manager, separately from the password they recover.

### 04 Machine and service credentials

Systems authenticate to one another with tokens and certificates, not with human accounts.

- Service-to-service calls use OAuth access tokens or API keys over TLS. Partner integrations use the authentication method the partner specifies.
- Secrets and API keys are held in the platform's secret store. They are never committed to source control, and automated secret scanning runs against the repository and its history.
- Keys are scoped to the narrowest set of permissions the integration requires, and separate keys are used for test and production.
- Keys are rotated when a holder's access ends, when a key may have been exposed, and otherwise at least annually.
- Production credentials are never used in development or test environments.

### 05 Member authentication

Members authenticate to Dovri before they reach any screen that moves money or links a bank account.

- Identity is verified at sign-up, and a one-time code sent to the member's phone is confirmed before a bank account can be linked.
- Bank credentials are entered with Plaid, not with Dovri. Dovri never receives or stores a member's bank username or password.
- A member sees only their own circles. Members of a shared circle see each other's first name, last initial, turn position and contribution status, and nothing else.
- Session tokens expire, and signing out invalidates the session.

### 06 Granting, changing and removing access

- Access is granted only for a stated purpose, and what was granted is recorded.

- When responsibilities change, access is adjusted in the same week, and access no longer needed is withdrawn rather than left in place.
- Access is removed within 24 hours of a person ceasing work on Dovri. Removal covers every system, not only the ones used most recently.
- On removal, any shared secret or key the person could have seen is rotated.

## 07 Review

Access is reviewed at least annually and whenever responsibilities, systems or partners change. A review lists every account and key that can reach production or member data, confirms each is still needed at the level it holds, and removes or reduces the rest. The outcome is recorded with the date and what changed.

Authentication events and administrative actions are logged and retained for 13 months, so access can be reconstructed after the fact.

## 08 Exceptions and enforcement

Any departure from this policy requires a recorded, dated decision by the policy owner stating the reason, the compensating control and the date the exception ends. Exceptions are revisited at each review.

Access granted outside this policy is withdrawn on discovery, and the circumstances are recorded in the risk register.

---

### APPROVED BY

**Maurice Ugbe**  
Founder & Chief Executive Officer

**security@joindovri.com**  
Security contact

**9 October 2026**  
Date of approval

Dovri Technologies LLC, a Virginia limited liability company. The current version of this policy is published at [joindovri.com/access-control](https://joindovri.com/access-control). Dovri is not a bank and does not take deposits. Money movement, identity verification and settlement are provided by regulated partners; Dovri does not hold member funds.