

Information Security Policy

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

This policy states how Dovri identifies, mitigates and monitors information security risks, who is accountable for them, and what Dovri does when something goes wrong.

SCOPE AND OWNERSHIP

This policy applies to every system, device and third-party service that stores or processes Dovri member data, and to everyone who works on Dovri in any capacity. Maurice Ugbe, Founder and Chief Executive Officer, is accountable for information security and owns this policy. Dovri Technologies LLC is a Virginia limited liability company and currently has no employees other than the founder; the controls below are sized to that and are extended as the team grows. This policy is reviewed at least annually and whenever there is a material change to the product, a partner, or the regulatory environment.

01 Risk management

Dovri maintains a written risk register listing each identified security risk, its likelihood and impact, the control that addresses it, and the person accountable. The register is reviewed quarterly and updated whenever a new system, partner or product capability is introduced.

A risk is added to the register whenever Dovri takes on a new third-party service that touches member data, changes how money moves, adds a new category of data, or learns of a vulnerability affecting a component in use. Each entry is tracked to closure or to an explicit, dated decision to accept the risk.

02 Access control

- Every person has a unique named account. Shared logins are not permitted.
- Access is granted on least privilege — the minimum needed for the work, and nothing broader.
- Multi-factor authentication is required on every system that stores or processes member data, and on every administrative console, including hosting, source control, database and payment partner dashboards.
- Credentials are held in a password manager. Secrets and API keys are never committed to source control, never shared over chat or email, and are rotated when a holder's access ends or a key is suspected of exposure.
- Access is removed within 24 hours of a person ceasing work on Dovri.

- Access is reviewed at least annually and whenever responsibilities change.

03 Protecting data

- All data in transit between clients and servers is encrypted using TLS 1.2 or better.
- All member data at rest is encrypted, including database storage and backups.
- Dovri collects the minimum data needed to run the service and keeps it only for the periods set out in the Dovri Privacy Policy at joindovri.com/privacy.
- Bank credentials are never transmitted to or stored by Dovri. Members authenticate with their bank through Plaid, and Dovri receives only the account details required to move money.
- Production data is not copied into development or test environments. Testing uses synthetic data.

04 Secure development and vulnerability management

- Source code is held in a private repository with branch protection on the production branch.
- Automated dependency scanning runs against the codebase and raises alerts for known vulnerabilities in third-party packages.
- Automated secret scanning runs against the repository and its history.
- Workstations and production systems receive security updates automatically and run endpoint protection.
- Vulnerabilities are triaged on discovery. Critical issues are remediated within 7 days, high within 30 days, and medium and low at the next scheduled release.
- Changes affecting authentication, money movement or member data are reviewed before release.

05 Third parties

Before a third party is given access to member data, Dovri assesses its security posture, confirms it is contractually bound to protect that data and to use it only for the service it provides to Dovri, and records it in the risk register. That list is reviewed at least annually and access that is no longer needed is removed.

Money movement, identity verification and settlement are performed by regulated partners. Dovri does not hold member funds.

06 Monitoring

Application and infrastructure logs record authentication events, administrative actions and money movement. Logs are retained for 13 months. Error and availability monitoring is in place for production systems, with alerts routed to the security contact.

07 Incident response

A security incident is any confirmed or suspected unauthorised access to, disclosure of, or loss of member data, or any event that compromises the integrity of money movement. On discovery Dovri will:

- **Contain** — revoke affected credentials and isolate affected systems immediately.
- **Assess** — determine what data was involved, how many members are affected, and the root cause.
- **Notify** — inform affected members, payment and data partners, and the relevant regulators within the time limits the law and contracts set. Partner notification obligations are treated as the shortest applicable deadline.
- **Remediate** — fix the root cause and record the incident, timeline and corrective actions in the risk register.
- **Review** — conduct a post-incident review and update this policy and the related controls where the incident shows a gap.

08 Business continuity

Member and transaction data is backed up on an automated schedule, backups are encrypted, and restores are tested at least annually. Source code and infrastructure configuration are version-controlled so production can be rebuilt from scratch.

09 Coordinated disclosure

Security issues may be reported to security@joindovri.com with enough detail to reproduce them. Dovri acknowledges reports within 2 business days and keeps the reporter updated until the issue is resolved.

Dovri will not pursue legal action against anyone who reports a vulnerability in good faith, allows reasonable time to fix it before disclosing it publicly, and does not access, modify or delete data belonging to anyone else in the course of testing.

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/security. 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.