ACCESS CONTROL AND AUTHENTICATION

How Bossete limits access to production systems and consumer financial data, including identity, roles, reviews, offboarding, and MFA.

DOCUMENT ID	BOS-IAM-001
CLASSIFICATION	Public
EFFECTIVE DATE	5 August 2026
LAST REVIEWED	5 August 2026
NEXT REVIEW	Within 12 months of last review
SECURITY CONTACT	Harumi Miyagi, Principal Operator, Information Security (security@bossete.com)
PUBLISHED AT	https://bossete.com/legal/access-control

1. Centralized identity and access management

Bossete uses a primary identity provider (Google accounts with multi-factor authentication) as the hub for authenticating operators to email, source control, cloud consoles, and other vendor systems that support that identity. Where a vendor does not support federation, access is still tied to a named individual account under the same operator identity program—not shared anonymous logins.

Disabling or locking the primary identity (and rotating any non-federated secrets) removes that person’s effective access to Bossete systems.

2. Production access controls

Access to production assets (virtual machines, hosted applications, databases) and sensitive data is limited by the following practices:

- Unique individual credentials — named operator accounts; no shared anonymous production users for day-to-day work.
- Least privilege — API tokens and cloud roles scoped to the minimum actions required; separate tokens per system where practical.
- Multi-factor authentication — required on identity providers for systems that can access or store consumer financial data.
- Encrypted control planes — administrative connections over encrypted channels (TLS/SSH).
- Secret isolation — production secrets kept in access-controlled vault storage, not in public websites or unencrypted team chat.
- Human approval for high-blast actions — outbound messaging and spend that can harm users or reverse cash without intent require gated tooling.

- Workload isolation — public marketing sites separated from private operational workloads so unauthenticated visitors cannot reach financial vaults.

3. Role-based access control (RBAC)

Permissions are assigned by role and function, not by copying another person's full access:

- Cloud and hosting providers use role or policy attachments scoped to the job.
- Source control uses repository and organisation roles appropriate to the work.
- Application and API tokens are issued per system with the minimum scopes required.
- The same role model applies when additional people are onboarded: grant only the roles needed for their function.

4. Periodic access reviews and audits

At least once per calendar quarter, the Principal Operator reviews who (and which service principals) can reach systems that hold consumer or financial data, and removes or reduces access that is no longer needed.

- Identity provider accounts and MFA enrolment for people with production access
- Cloud console users and roles; hosting and DNS admin lists
- Source-control organisation and repository collaborators
- Banking-data and payments dashboards (when used)
- Secret-store holders and long-lived API tokens

Findings are remediated in the same review window. Review completion is recorded internally with the quarter and date.

5. De-provisioning and access modification

When a person leaves, transfers roles, or should no longer access Bossete systems, access is revoked the same day using a fixed checklist. There is no waiting for a later cleanup sprint.

- Disable or lock the person's primary identity-provider account (and recovery paths).
- Revoke session tokens and OAuth grants; rotate any shared or long-lived secrets they could have used.
- Remove cloud roles, source-control membership, hosting admin seats, and vendor dashboard users for that person.

Role changes use the same checklist. When headcount grows enough to use a formal HR system, offboarding remains driven by that same-day revoke path and is integrated with HR departure notifications. The authorised human set is intentionally small today; the checklist still applies to any contractor, collaborator, or future hire who is granted access.

6. Multi-factor authentication (critical systems)

Yes — multi-factor authentication is required for access to critical systems that store or process consumer financial data.

Where the provider supports it, we prefer phishing-resistant factors: passkeys / WebAuthn or hardware security keys; platform authenticator biometrics bound to those providers; authenticator app TOTP as a baseline where stronger factors are not yet enrolled.

Critical systems in scope include cloud consoles, source control, domain registrar, hosting dashboards, and vault access that can reveal bank-data API keys. Email recovery paths for those systems are also MFA-protected where the vendor allows.

For inquiries about access documentation, contact security@bossete.com.

7. Authentication before bank-data Link

Where an end-user facing Bossete application surfaces a third-party bank-data Link flow, the user must complete authentication to that application first. Link is not presented as an anonymous public widget on the open marketing homepage.

For production multi-user applications: MFA is enforced on the application account before banking connection UI is available, using phishing-resistant factors where the platform stack supports them (passkeys or equivalent). Bank-side authentication remains in effect in addition to Bossete session authentication.

For single-operator / account-holder tooling that uses bank data on behalf of the same natural person who operates the systems, MFA is enforced on the critical systems that hold tokens (above), and the operator is the only authorised user.

8. Handling of tokens and keys

- Bank-data client secrets and access tokens are stored only in private secret stores.
- Production keys are not embedded in public front-end bundles.
- Rotation follows incident or suspected exposure without delay.

Parent policy: Information Security Policy (https://bossete.com/legal/information-security).