INFORMATION SECURITY POLICY

How Bossete identifies, mitigates, and monitors information-security risk for systems that process customer and financial data.

DOCUMENT ID	BOS-ISP-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/information-security

1. Governance and responsibility

Bossete is an operator-led systems practice. Accountability for information security sits with the Principal Operator:

- Harumi Miyagi -- Principal Operator, Information Security
- Email: security@bossete.com (monitored)
- Legal / privacy: legal@bossete.com

This policy applies to production systems, secrets vaults, cloud infrastructure, developer workstations used for production, and third-party processors (including banking data providers when integrated).

2. Risk management (operational program)

Bossete maintains a documented, operational security program. Risks are identified, mitigated, and monitored as follows:

- Identify -- threat modelling at design time; maintenance of a written risk register for availability, data loss, lockout, vendor concentration, and access abuse.
- Mitigate -- least-privilege credentials; multi-factor authentication on critical systems; private secrets storage; environment separation; human approval for high-blast actions that can spend money or send outbound communications.
- Monitor -- deployment and service health checks; periodic connector health; incident review after anomalies; continuous improvement of policy and controls when gaps are found (including vendor diligence feedback).

The program is intentionally compact, proportional to a small practice, and is revised when systems or vendors change--not a paper policy left unopened.

3. Access control (summary)

Full procedures live in the Access Control & Authentication policy (https://bossete.com/legal/access-control). In brief: production assets and sensitive data require unique credentials, MFA where supported, secrets outside application repositories when practical, and no shared generic production logins.

4. Encryption

In transit

Yes. Public web applications and APIs are served over HTTPS with TLS 1.2 or better (modern edge/CDN and hosting defaults; TLS 1.0/1.1 disabled at the platform). Administrative access to infrastructure uses encrypted channels (SSH or equivalent management plane encryption).

At rest

Yes for consumer and financial data we store. Data received from bank-data and payment processors (when used), and other sensitive records, are stored with encryption at rest using platform-managed encryption for disks/databases where available (e.g. cloud provider default encryption for storage and databases), plus access-controlled private secret stores for tokens and keys. Application secrets are not committed to public repositories.

5. Vulnerability management

Bossete performs regular, automated vulnerability identification across application code, production runtimes, and operator endpoints used for production work:

- Application dependencies -- lockfiles plus automated dependency vulnerability alerts (repository Dependabot or equivalent) on production application codebases; high-severity advisories are reviewed and patched or mitigated promptly.
- Production assets -- hosted applications and infrastructure run on maintained platform images; OS and runtime security updates are applied as part of normal operations and rebuilds.
- Operator and contractor endpoints -- machines that hold production credentials run with full-disk encryption, MFA on the identity provider, and the operating system automatic security-update channel enabled.
- Configuration review -- least privilege for tokens and cloud roles; deny-by-default patterns for outbound integrations that can cause financial or privacy harm.
- Monitoring of production health -- service uptime and deploy pipeline signals; investigation of unexpected failures that could indicate compromise or misconfiguration.

This program is proportional to a small practice: automated dependency scanning and OS / platform update channels are the primary continuous controls. A separate commercial agent on every device is not required when those channels already deliver security patches and alerts.

6. Development practices

- Version control with restricted repository access.
- Review of changes that touch authentication, payments, or personal financial data.
- Separation of public marketing surfaces from private operational systems whenever possible.
- Secrets managed as vault material, not hard-coded in frontend bundles.

7. Incident response (procedure)

- Contain -- revoke or rotate affected credentials and tokens immediately.
- Assess -- determine scope (systems, data classes, users affected).
- Notify -- inform affected individuals and required partners (including banking data vendors when their tokens are involved) without unreasonable delay.
- Remediate -- patch root cause; update this policy if controls must change.
- Record -- keep an incident note for post-mortem learning.

Report suspected incidents to security@bossete.com.

8. Vendors and processors

Third parties that process infrastructure or sensitive data (hosting, DNS, payments, bank data aggregation) are selected for security posture and contractual terms. API keys and webhooks are stored as secrets; production scopes are limited to what the product requires. Vendor security feedback is treated as an input to continuous improvement of this program.

9. Review and maturity

This policy is reviewed at least annually, and sooner when a new class of personal financial data is introduced, a material security incident occurs, or a vendor diligence process identifies a control gap we agree to remediate.

Related: Privacy Policy (https://bossete.com/legal/privacy); Data Retention (https://bossete.com/legal/data-retention); Access Control (https://bossete.com/legal/access-control).