

Trust begins with controlled access.

Afterbase brings business information, users and applications together. Security therefore includes authentication, authorization, integrations and shared responsibilities. This overview describes the approach at a high level; it is not an audit or certification statement.

Access permissions and data connections are configured for each organization and use case.

Identity and access

Afterbase supports roles and permissions for customers, employees and suppliers. Actual access is configured per customer environment.

Secure communications

Platform connections use HTTPS/TLS. Integration points require appropriate management of keys and tokens.

ERP and other data sources

Afterbase supports connections to cloud and on-premises systems. Network routing, permissions and data flows depend on the integration.

Operations and responsibilities

Customers decide which information, accounts and roles are used. Secure operations also require change management, incident handling and periodic access reviews.

Security questions for implementation

- Which systems will be connected and what information is required?
- Who needs access and who approves permissions?
- How are access keys, tokens and user accounts managed?
- Which logging, retention and personal data requirements apply?
- Who should be contacted if a security incident occurs?

For technical details or security review, request the documentation and agreements applicable to your Afterbase environment.

This overview does not claim ISO 27001, SOC 2 or other certification and does not replace contractual security or data processing agreements.