

Vertrouwen begint bij gecontroleerde toegang.

Afterbase brengt bedrijfsinformatie, gebruikers en toepassingen samen. Beveiliging vraagt daarom aandacht voor authenticatie, autorisatie, integraties en verantwoordelijkheden. Deze samenvatting beschrijft de uitgangspunten op hoofdlijnen; het is geen audit of certificeringsverklaring.

Toegangsrechten en dataverbindingen worden ingericht op basis van de organisatie en de toepassing.

Toegang en rollen

Afterbase ondersteunt rollen en rechten om klanten, medewerkers en leveranciers alleen toegang te geven tot relevante onderdelen. De daadwerkelijke rechten worden per klantomgeving ingericht.

Beveiligde communicatie

Communicatie met het platform verloopt via HTTPS/TLS. Integratiepunten vragen om passend sleutel- en tokenbeheer.

ERP en andere bronnen

Afterbase ondersteunt koppelingen naar cloudsystemen en systemen op locatie. De exacte netwerkroute, autorisaties en gegevensstromen verschillen per integratie.

Beheer en verantwoordelijkheden

De klant bepaalt welke informatie, accounts en rollen worden gebruikt. Voor veilige exploitatie zijn daarnaast procedures voor wijzigingsbeheer, incidentafhandeling en periodieke toegangscontrole belangrijk.

Securityvragen voor een implementatie

- Welke systemen worden gekoppeld en welke gegevens zijn daarvoor nodig?
- Welke groepen krijgen toegang en wie keurt hun rechten goed?
- Hoe worden toegangssleutels, tokens en gebruikersaccounts beheerd?
- Welke logging, bewaartermijnen en afspraken over persoonsgegevens gelden?
- Wat is de contact- en escalatieprocedure bij een beveiligingsincident?

Vraag voor technische details of een security review de actuele documentatie en afspraken op voor jouw Afterbase-omgeving.

Deze uitgave maakt geen aanspraak op ISO 27001-, SOC 2- of andere certificering en vervangt geen verwerkersovereenkomst of contractuele beveiligingsafspraken.