aiio GmbH
Klausenerstraße 10a
39112 Magdeburg

Operation of the application

"aiio®"

Security Whitepaper

Version 3.0

Status: 14.08.2025

1 Purpose of this Document

This document describes the IT security aspects of the application architecture and the usage-related security features for the aiio product.

Table of contents

2 Authors and changes of the document

Document history

Date	Change	Author	Version
24.03.2023	First Version	Moser P.	1.0
31.05.2023	Add cooperation with OpenAI	Moser P.	2.0
14.08.2025	Revision of AI partners, introduction of APM and CNAPP, addition of export functions, refinement of encryption and disaster recovery concepts	Moser P.	3.0

3 Application description

Aiio is a web browser-based modeling tool that enables processes to be drawn and responsibilities to be assigned within a team, using the familiar Microsoft 365 look and feel.

3.1 Description of Services

Aiio allows the direct linking of documents and structures with process steps, ensuring process accuracy through simple feedback options. Users can actively share comments on processes and related problems. Aiio can be integrated into web browsers or MS Teams for access to information at any time.
Aiio enables the inclusion of AI support, making it possible to identify potential for process improvement.

3.2 Responsibilities

Microsoft Ireland Operations, Ltd. is responsible for the operation of the data center hosting the environment at:
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

aiio GmbH is responsible for the operation of the hosting environment at:
Klausenerstraße 10a
39112 Magdeburg
Germany

The provider chosen by the customer is responsible for operating the AI model and processing the associated data. The customer can choose between:

OpenAI, L.L.C., San Francisco, United States of America

Anthropic, PBC, San Francisco, United States of America

Google Cloud EMEA GmbH , hosted in Germany

3.3 User Training

Getting started with aiio is designed to be as simple as possible. The familiar Fluent UI and alignment with M365 make the tool easy to learn. The aiio Academy provides the opportunity to learn about the basic functions and start working with aiio.

Specific user training can be booked for a fee upon request, tailored to the individual's requirements.. The focus can be on:

- Introductions to aiio®
- Training in process management methodology
- Training in process modeling
- Introduction to previously unused functions and further developments of aiio®

Responsible: Consulting Services of aiio GmbH

3.4 Development

aiio is subject to continuous development. The development team follows the agile software development process, based on the Scrum methodology. The features and content of further development largely following the needs of aiio users or by new market or regulatory requirements.

3.5 Contact and Support

For support, users can visit https://www.aiio.de/support, contact via the provided form, or email support@aiio.de.
Customer Success Service of aiio GmbH is responsible for providing support.

Further information on incident management can be found in Chapter 8.

4 Technical Description

The entire aiio application architecture is based on a combination of React (front-end) and Django (back-end) connected to a MySQL database. The entire environment is hosted in a fully virtualized Microsoft® Azure™ tenant, utilizing an Azure Kubernetes Cluster.

4.1 Architecture

The environment is structured as follows:

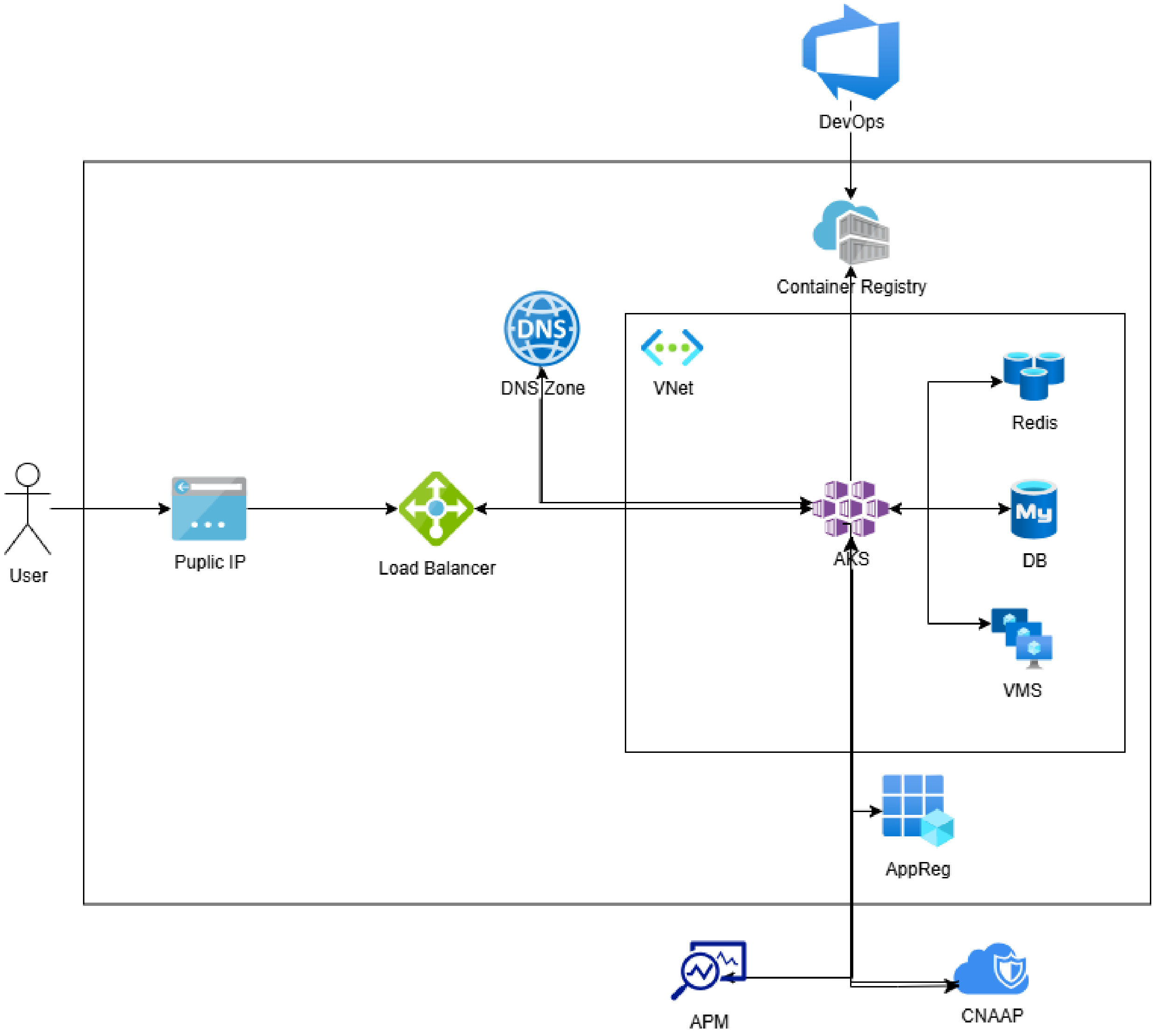

Figure 1: scheme aiio architecture

The environment is essentially segmented into two areas to ensure maximum information security for all users. The main segment comprises a virtual network that includes an Azure Kubernetes cluster and its corresponding Virtual Machine Scale Set. The MySQL database and Redis Cache are also located in this network, which is only accessible by the applications within the cluster.

The architecture is hosted in a tenant specifically created for aiio. The only regular access point to the application is a public IP accessible via the DNS app.aiio.de. Users are then redirected to the deployments within the cluster via a load balancer. Additional access is only possible through the aiio internal DevOps platform - for automated platform updates - or trained administrators.

During operation, the Azure Kubernetes cluster itself constantly ensures that the application is executable and maintains performance for everyone even under high load. Depending on the number of users and operations, both the database and the number of

virtual machines are scaled. If errors or other important information occur at application level during operation, these are reported to a specialized service for application performance monitoring (APM) and error logging.
A Cloud-Native Application Protection Platform (CNAPP) is also used for the comprehensive security monitoring of the cloud infrastructure and the proactive detection of threats

The following services are used for the architecture:
Azure Kubernetes Cluster
Azure Database for MySQL flexible server (MySQL Version 5.7)
Azure Cache for Redis (Redis Version 6.0)
Virtual Machine Scale set (Image: AKSUbuntu-2204gen2containerd-202505.14.0)
Azure Container Registry
Application Performance Monitoring (APM)
Cloud-Native Application Protection Platform (CNAPP)
DNS Zone

The services are updated automatically through the use of Azure. The impact of updates to these components is tested in a test environment before being applied to the live system.

4.2 Operational description

The environment generally operates fully automatically and without user intervention, unless errors occur that require user intervention by the administrators.
Operational readiness is displayed to the administrators via integrated monitoring (see Fig. 2). In the event of an error, the administrators are also immediately notified by email. Monitoring is part of the standard scope of the Microsoft® Azure™ environment.
In addition, operation is secured by two specialised levels: An application performance monitoring (APM) and error logging service continuously monitors application performance and immediately reports errors or bottlenecks. This is complemented by a leading Cloud-Native Application Protection Platform (CNAPP), which proactively protects the environment by analysing cloud misconfigurations, vulnerabilities and active threats around the clock and alerting security-critical incidents.
Monitoring the operational readiness of the environment is the sole responsibility of specially trained personnel at aiio GmbH.

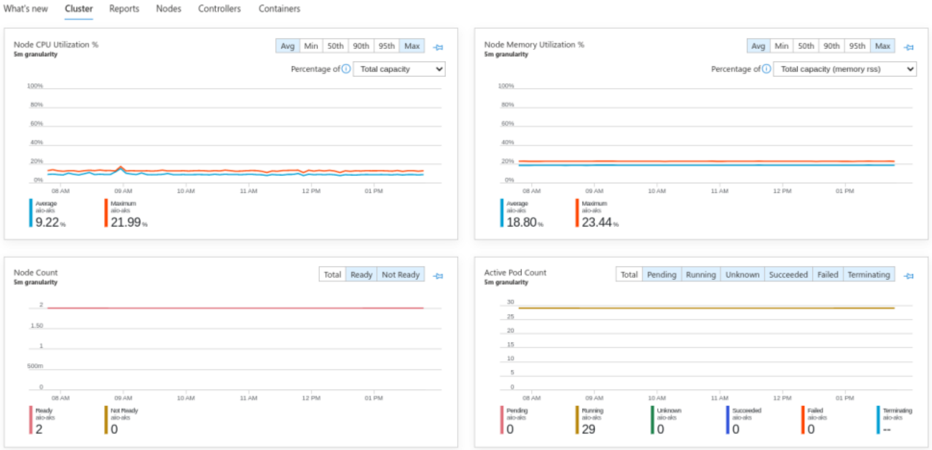

Figure 2: Monitoring Overview

4.3 Requirements

To use aiio, a completed service agreement is required. There are no special technical requirements. aiio can be used via any commercially available office PC workstation with an internet connection.

4.4 Internal interfaces

The internal standard interfaces between the individual architecture areas are explained in section 4.1 "Architecture".

4.5 External interfaces

Data is transmitted to the AI provider selected by the customer (OpenAI, Anthropic or Google) via an API. No personal data is transmitted in the process. The transmitted data is not used for training or to improve the models and services of the respective provider. Corresponding DPAs have been agreed with all AI providers.
In addition, aiio® has its own API interface that allows customers and partners programmatic access to the platform. This interface can be used, for example, for integration into third-party systems or for user-defined analyses. Access to the API is possible for customers in "Excellence Mode" and above.

4.6 Physical security

The security of the application guaranteed by aiio is described in Annex 1 "aiio TOM". The application itself is operated on the Microsoft Azure cloud platform, which means that Microsoft is responsible for the physical security of the underlying data centre infrastructure. Microsoft ensures compliance with the latest security and compliance standards through a comprehensive system of controls and regular audits. The relevant valid certifications, audit reports and proof of physical security are provided by Microsoft centrally and up to date in the Microsoft Trust Centre.

4.7 Storage locations

In principle, all customer data is stored on servers within the European Union. An exception may be the optional use of AI functions, where data may be transferred to a third country depending on the provider selected.

4.8 Data export

Aiio provides various options for exporting data.

- PDF export for processes and process graphics
- SVG export for organisational charts
- CSV or Excel export for process lists, requirements, resources, locations and employees
- API interface.

5 Installation and Configuration

To make an aiio® instance available to a new customer, no new environment installation is required. A customer user visits the aiio application and can initiate a test system himself/herself with the help of a button click. Necessary entries are automatically entered into the database, allowing the user to use an operational aiio in a short period.

6 Application operation and security

In the context of application operation, aiio customers have no tasks. Application operation is usually fully automated, as described in Figure 1 aiio architecture schema. The VMs necessary for operation are active 24/7. Application security is based on the standards of Microsoft Azure technology.

6.1 Role and rights administration

The role assignments and user rights required for aiio® follow a defined scheme.

For this purpose, aiio® provides several predefined user roles with specific authorization levels. The administration and assignment of these roles to the respective users is the responsibility of the customer and is carried out by one or more named aiio executive users of the customer in the application itself.

As the exact authorizations of these roles may change with the further development of the software, a static list is not provided in this document. The current and detailed description of the individual roles can be viewed on the official aiio® website in the price and service description section.

6.2 Authorization/Authentication

The Microsoft Authentication Library (MSAL) is used entirely for user authentication. When visiting aiio, the customer is immediately asked to log in with their Microsoft Entra ID account. This account belongs to the customer's tenant.
All security-relevant functions, such as the enforcement of password policies or multi-factor authentication, are provided and managed by Microsoft Entra ID. aiio only receives confirmation from the Microsoft servers that it is a valid user of the customer's tenant. This ensures that users use their usual corporate identity for seamless and secure access to aiio. All internal Tennant information (e.g. other users, SharePoint files) is then only visible to the logged-in user, provided they have the rights in the customer Tennant.

6.2.1 Single Sign-on „SSO“

Authentication via Microsoft Entra ID enables a seamless single sign-on (SSO) experience. If a user is already logged in to their Microsoft account in their work environment, for example in the browser or within Microsoft Teams, they are automatically authenticated with aiio® without having to enter their access data again.

6.2.2 Multi Faktor Authentication

aiio® itself does not implement its own multi-factor authentication, but is fully integrated into the customer's security architecture. All authentication guidelines configured by the customer in Microsoft Entra ID, in particular the obligation to use MFA, are automatically and directly enforced when logging on to aiio. The customer therefore retains full control over the security of the login process.

6.3 Data Backup

Data is backed up fully automatically using daily database backups, which are stored for 30 days. Monitoring the process is ensured.

Backups are stored geo-redundantly to ensure maximum security. This means that they are automatically replicated from the primary region (Western Europe) to a geographically separate partner region of Azure. This approach protects the data from an unlikely but possible failure of an entire data center region and ensures recoverability in the event of a disaster.

6.4 Change-Management

Changes/adaptations to the aiio® product essentially follow the development scheme as described in section 3.4.
The adjustments to the product are rolled out at irregular intervals. These iterative changes are made available to customers seamlessly. No effort is required on the part of the customer. Customers are informed of relevant changes.
Hot fixes are carried out at the discretion of aiio GmbH to rectify acute error situations.

6.5 Deletion concept

Alle Daten können in erster Linie vom Kunden selbst bei Bedarf gelöscht werden.
Sicherungsdateien aus der automatischen Datensicherung werden nach 30 Tagen gelöscht (siehe 6.3).
Die Vorgehensweise beim Löschen ist durch eine verbindlich zu verwendende Handlungsanweisung definiert.
Nach dem Löschen erhält der Kunde ein Löschprotokoll.
Sicherungsdateien können auf Anforderung auch vor Ablauf gelöscht werden.
Bei Vertragsbeendigung werden die Daten des ausscheidenden Mandanten spätestens bei Deinstallation des Mandanten gelöscht. Auf Anordnung des Mandanten können die Daten zum Vertragsende sofort gelöscht werden.
.

6.6 Tenant Separation Concept

The tenant separation concept is ensured by assigning each record within the database to a tenant. For API requests, the tenant information is automatically taken from the logged-in user and filtered on all records. The tenant information is issued by the Microsoft authentication servers and cannot be changed.

6.7 Connection security

The web servers are only accessible to users via a certificate and encrypted connection (SSL) with the specified authentication. If a client is shut down (end of contract, etc.), all accesses are blocked, and the tenancy is no longer accessible.

6.8 Encryption concept

Our encryption concept protects data both during in transit and at rest.
Encryption at rest:

All virtual hard disks of the VMs as well as their backups and snapshots use Azure Storage Service Encryption (SSE). All data is automatically encrypted with a 256-bit AES key managed by Microsoft before it is written to the storage media. This ensures that data at rest is protected at the physical level.

Encryption in transit:
All communication between the end user and the aiio application is secured by TLS 1.2 or higher. Similarly, all internal communication between the various services within the Azure Kubernetes cluster and to the databases is encrypted using TLS connections.

6.9 Logging

All processes on the database, the Azure Kubernetes cluster and the associated VMs are logged in the Azure standard event logs. A specialized Application Performance Monitoring (APM) service is used to monitor and log application-internal errors and performance issues Our CNAPP platform captures and analyzes security-related events across all cloud resources, detects anomalies in workload behavior and identifies potential threats.

6.10 Emergency concept

In principle, a system failure is unlikely. The Azure Kubernetes cluster constantly checks whether the deployment of the front or back end is running without errors. If this is not the case, it tries to start another instance of the application on a self-healing basis. Constant health checks by our APM service and continuous threat analysis by our CNAPP platform ensure that specialist personnel are alerted immediately in the event of security-critical incidents, performance problems or anomalies.

In the event of a serious database failure, recovery is initiated from the last available geo-redundant backup (see section 6.3). During this recovery process, temporary unavailability of the application (downtime) is to be expected. However, the possibility of recovery is ensured with the highest probability by the geo-redundant storage.

In the event of data loss or data inconsistency, the backup concept takes effect (see 6.3).

6.11 Certifications and AI-Compliance

6.11.1 Certifications of the infrastructure

The aiio application is operated on the Microsoft Azure cloud platform. The security and compliance of the underlying infrastructure is guaranteed by Microsoft and documented by numerous certificates and attestations verified by independent third parties.

These include fundamental standards such as ISO/IEC 27001 (information security) and ISO/IEC 27701 (data protection).

To ensure that these certificates are up to date and to avoid enclosing potentially outdated documents, aiio refers to the Microsoft Trust Center. Microsoft makes all valid certificates and audit reports centrally available there.

aiio GmbH itself does not maintain its own formal certification, but ensures the operation of the application through the processes and controls described in this document and the Technical and Organizational Measures (TOM, see Appendix 1)

6.11.2 Dealing with AI providers and contractual basis

aiio GmbH is actively following the developments surrounding the EU AI Act and has a clear strategy to ensure compliance.

Careful selection of providers:

We rely exclusively on market-leading AI providers (see 3.2) who have committed themselves to compliance with the EU AI Act. We rely on the assurances of these providers that their base models meet the requirements for "General Purpose AI Models" (GPAI).

Risk minimization in the application:

The AI functions implemented in aiio are used for process analysis and optimization, process summarization and summarizing process changes for versioning. In our understanding, these use cases do not fall into one of the high-risk categories of the AI Act.

Irrespective of this, we have implemented the following protective measures:

- Data protection:

  No personal data is transmitted to the AI services.

- Customer Sovereignty:

  The AI functions are deactivated by default and must be actively switched on by the customer. The customer can also deactivate the functions at any time.

  The customer retains sovereignty by choosing the provider and can evaluate the provider's specific data protection and compliance commitments. For providers with a hosting location in the EU (e.g. Google in Frankfurt), data residency is additionally strengthened.

- Transparency:

  The use of AI functions is always clearly visible to users.

We have concluded corresponding data processing agreements with the AI providers we use. To ensure that these documents are up to date, they are not included as static attachments. All relevant and always up-to-date data processing agreements with the AI providers can be viewed on the aiio website.

6.12 Possibility of inspection by the customer

The client is fully entitled to the audit rights granted in accordance with Art. 28 GDPR (order processing).
We grant further audit rights arising from other regulatory provisions, such as certification requirements or special legal provisions applicable to the customer (e.g. WPO, SGB or

similar), insofar as any planned audit is carried out with a sufficient lead time of 4-6 weeks in such a way that it does not jeopardize the business operations of aiio GmbH.
Unannounced audits are not permitted.

6.13 Exit concept

At the end of the contract, the customer has an unrestricted right to receive or immediately delete data in accordance with Article 28 of the GDPR. The customer's termination rights are subject to the contractually agreed provisions.

7 Application Fault Management

Faults are typically detected through automatic monitoring (see Fig. 2) of the aiio environment before they can impact our customers, allowing aiio to react promptly to faults within the environment.

Faults that arise during the customer's use or are detected during such use must be reported to the support addresses specified in3.5.

The duration of resolution is determined by the contractually agreed SLA.

7.1 Availability and Procedure

The support units of aiio GmbH are available from Monday to Friday during normal business hours.
The person reporting the fault will be kept informed of the progress of the resolution.

7.2 Contractual Provisions and Order Processing

The provisions contained in the service agreement shall apply.
The services, hosting, operation and support of the environment and application contractually agreed with aiio are to be regarded as order processing within the meaning of Art. 28 GDPR.

8 Annex

Annex 1 „aiio-TOM“, Catalog of technical and organizational measures

9 List of figures