

Agility PIM Service Definition Document – January 2026

Agility PIM

Agility is a true multichannel Product Information Management and Publishing platform designed with a procurement and distribution business model at its core. From supporting multiple taxonomies to the flexibility and openness of the data model, Agility is THE PIM for Distribution.

Agility provides a single-tenant, closed source solution built on Microsoft Azure. This provides all the typical benefits of a SaaS solution with the added benefit of increased information security (no sharing of resources with other customers), and more flexibility with regards to software updates & upgrades. You are not obliged to take each update or upgrade and can be selective over those you wish to take.

The Agility SaaS offering includes environment management, system monitoring and corrective action, patching, tuning, the application of service pack releases, and back-ups.

Agility supports all the stated requirements in the published specification and is comprised of the following elements:

- Agility PIM: a mature, feature rich cloud-based PIM solution. SaaS deployments are hosted in Microsoft Azure.
- Agility DAM: add-on module to PIM that provides traditional DAM functions such as image transformation, metadata management and collaboration features.
- Agility DI: our data integration platform, an ETL (extract, transform, load) tool used for integrating business systems and for performing data validation and quality checks, along with corrective actions.
- Agility Connector for InDesign: native plug-in, developed in-house that connects InDesign users to the Agility PIM & DAM for catalogue page production.

Data backup and restore, disaster recovery and business continuity and disaster recovery plans

Agility uses Microsoft Azure Recovery Services Vault features for snapshots of Virtual Machines and storage accounts. Agility databases (Azure SQL Database) are protected by automatic backups.

Full backups are taken every week, differential backups every day, and log backups every 5 minutes. Backup files are stored in a geo-redundant storage account with read access (RA-GRS) to ensure backups are availability for disaster recovery purposes. When a database is restored, the required backup files are retrieved in the same data centre and applied.

Daily backups are stored for 7 days which can be extended on request. Daily snapshots of server virtual machines are being generated with 7 days retention. May be extended on request. Daily snapshots of Azure File Shares are being generated with 7 days

retention. May be extended on request to meet your policies. Client data and backups are stored in an Microsoft Azure data centre in the UK

Our Business Continuity plan covers the recovery strategies for different scenarios of major disruptions to different parts of the organisation and to our suppliers, Microsoft Azure being the major one. The details of who is responsible in the organization for each of the tasks of activating, executing, and deactivating the plan is stated in the BCP document attached to the tender. Our CISO is responsible for keeping the BCP document up to date.

Planned technical support including security patching of operating systems and third-party applications is primarily scheduled in a two (2) hours monthly recurring service window agreed with the customer.

The service window is ideally planned outside of normal business hours and outside of time when integration jobs are running. Planned service windows are excluded from availability calculations and reporting.

Monitoring systems are used extensively by the Hosting Services team to mitigate issues before affecting the delivery of our service. The monitoring scripts are improved on a regular basis to further improve availability.

In addition to planned service windows for recurring installations of recommended security patches, occasionally critical security patches are applied on an ad-hoc basis on directives from our CISO. In these cases, the client may be contacted on short notice before the patch is applied, all to secure the system and avoid security breaches. In the case of unforeseen issues that affect the availability of the service we always assign appropriate resources to mitigate the issue as fast as possible to meet targeted SLAs.

Onboarding and offboarding support provided

Our implementation methodology follows a three-phase approach, wherein the project requirements, scope, and the proposed solution design are defined and approved by the client during the (1) Planning & Design phase. This is followed by the (2) Execution phase and, upon go-live, the (3) Go-Live & Hypercare phase where support is provided during the set-in period.

During the Planning & Design phase, we will conduct a number of pre-study and discovery sessions with various client stakeholders and subject matter experts (SMEs) to document requirements and determine how our solution can best fulfill these requirements. Stakeholders and SMEs are to be appointed by the client, and typically include the following:

Role	Responsibilities	Skills Needed
Executive Sponsor	Help with securing budgets; serve as project champion; assist with priorities, issue escalation	Leadership
Project Lead	Manage communications with Agility; coordinate client project team, primary contact for Agility project manager	Project management, negotiation, leadership

Change Authority	Review and consider change requests and approve them within a designated budget	Negotiation, decision making
Interface Expert[s]	Define connectivity requirements; assist with connectivity issues to and from Agility PIM and client interfaced systems	Expert knowledge of client interfaced applications
PIM Power User[s]	Identify product information management requirements; serve as the client leader for defining the product data model (taxonomy categories, attributes, choice lists) to be implemented in the PIM; ensure project Design documents are accurate and provide clarification; co-lead internal workflow discussions; deliver end user PIM training; conduct user acceptance testing	Logical thinker; troubleshooting skills; ability to impart knowledge; understanding of scripting and technical concepts can be helpful
DAM Power User[s]	Identify DAM and asset requirements; serve as the client leader in this area; ensure project Design documents are accurate and provide clarification; co-lead internal workflow discussions; deliver end user DAM training; conduct user acceptance testing	Understanding of client asset requirements; troubleshooting skills; ability to impart knowledge
Design Power User[s]	Identify design and style requirements; serve as the client leader for mapping PIM data to product catalogue templates; ensure project Design documents are accurate and provide clarification; co-lead internal workflow discussions; deliver end user InDesign plug-in training; conduct user acceptance testing	Understanding of Adobe InDesign; understanding of (or willingness to learn) scripting; troubleshooting skills; ability to impart knowledge
eCommerce Expert	Identify eCommerce workflow and product data requirements; serve as the client leader in this area; ensure project Design documents are accurate and provide clarification; co-lead internal eCommerce workflow discussions; conduct user acceptance testing	Understanding of client eCommerce workflow and product data requirements; troubleshooting skills; ability to impart knowledge
Other SMEs, incl. End Users	Advise where needed on their areas of specialisation	Often this comes down to expertise in specific product categories or business requirements for product data in interfaced systems.

From the discovery sessions with these users, we will create an implementation Design document for the clients review and approval. Once adjustments are made and the Design document is accepted, it will be used to guide the project's execution. Project work will not initiate until the completion of the Planning & Design phase and clients agreement to and acceptance of the Design document.

A Quality Management Approach document is also created during the Planning & Design phase and becomes part of the project Design document. This includes the complete scope of the project, what is out of scope, clear and realistic acceptance criteria that will be used to assess the project and definition of how the product will be assessed. The Quality Management Approach also defines the various responsibilities for achieving the required quality levels. Once agreed to, the Approach will be used to throughout the project. A Risk Management Approach document is also created during the Planning & Design phase and becomes part of the project Design document. This document defines the project procedures for risk management in terms of how risk will be identified, assessed, controlled, and communicated in the project. Client and Agility will jointly use this format to capture, assess and address any risks identified throughout the course of the project.

Once the Design document is accepted, we will begin the Execution phase by creating the clients Agility PIM environment.

All client data remains client property. At the termination of the contract, data will be exported and transferred to client in a mutually agreed-upon, supported format prior to the client Agility application and Azure environment being decommissioned.

Service constraints & maintenance windows

Planned technical support including security patching of operating systems and third-party applications is primarily scheduled in a two (2) hours monthly recurring service window agreed with the customer. The service window is ideally planned outside of normal business hours and outside of time when integration jobs are running. Planned service windows are excluded from availability calculations and reporting.

Service availability

Agility guarantees 99.5% availability, but it is highly unusual to experience less than 99.8% availability, excluding maintenance windows or planned updates.

After sales support

Our helpdesk is provided via an online ticket-based system (using Salesforce.com). Your nominated System Administrators (maintenance and support contacts) are responsible for 1st line support to your business users and are able to raise tickets for issues that they cannot resolve themselves. This may include system availability, system performance, unexpected results from actions in the software, or suspected bugs. Ticket generation also includes the selection of a priority level (P1, P2 etc). The system is available 24/7 and tickets are acknowledged immediately.

The support team monitoring and working the tickets to resolution are based in York and London (UK), Malmo (Sweden), Bengaluru (India), Vancouver (Canada), and Chicago (USA). This provides near round-the-clock coverage for the initial triage and potential solution.

The support team is predominantly contacted through the helpdesk system which also allows for email communication. Support team members may request a call or screenshare via Teams if they need early sight of the problem.

We would anticipate that the UK and Sweden teams would be most involved in supporting UK clients due to proximity and time zone, but evening coverage will be available using our teams in North America.

Out of hours (weekend) support is by arrangement using on-call staffing. This is chargeable over and above standard SaaS fees.

Technical requirements

Agility private SaaS is accessed via a web browser and most major Chromium-based browsers are supported, in addition to Safari for Mac.

A site-to-site VPN is recommended to connect the clients AD to Agility to facilitate single-sign-on (SSO).

Hosting options and locations

Agility PIM is offered as a private SaaS solution via Microsoft Azure. UK data centres are used for UK clients. Agility is also available to be deployed on-premise or in your own private cloud.

Access to data (upon exit)

Full support is provided when a customer cancels a software subscription for the export and transfer of their data. The system will remain available to the client for an agreed period, and when this expires the data will be securely deleted and the virtual machines will be decommissioned. Evidence of deletion and decommissioning can be provided upon request.

Security

A significant part of our business involves supplying technology to Microsoft, Amazon, Google, SAP and Palantir among others. This technology is embedded in Azure, AWS, Google Cloud and many other offerings that are certified under ISO 27001, ISO 9001, Fedramp, SOC1/2 and many other standards globally. Given the criticality of the technology we provide, to support these certifications at our customers we have participated in their certifications and are subject to regular automated and process audits of both process and data security. At this time, there are no open concerns from any of those audits.

As security and compliance have become much bigger concerns the cost and time of participating in these audits has reached the point we have agreed with our major customers to certify under ISO27001 and ISO9001 and audit against any requirements we agree to maintain beyond those certifications.

1. Authorized staff including the Support team and Hosting Services team access customer environments via strict firewall rules, using MFA-enabled VPN servers. All staff equipment is protected by antivirus tools, disk encryption tools and remote management tools controlled by the centralised IT organisation. The IT organisation performs threat prevention and cyber security training for all staff on a regular basis. Most staff working remotely, and our offices around the world are all protected with entrance control systems.
2. The Hosting Services team and Development team use a vulnerability scanning tool to identify, manage, fix and control vulnerabilities in our web applications and APIs. In addition to this, each customer has their own separate hosted environment, protected either with IPsec VPN tunnels to the customer network, or IP range whitelisting to further increase security. In practice this means the endpoints are not publicly available.