Cloud Assist

G-Cloud 15 Service Definition

1. Overview

Jisc is the UK digital, data and technology agency focused on tertiary education, research and innovation.

We are a not-for-profit organisation and believe education and research improves lives and that technology improves education and research.

Cloud technologies can help you to enable digital change for the benefit of staff and students – transforming your organisation as you move closer to Education 4.0.

Our sectors are increasingly challenged by the complexity of managing Microsoft 365 environments, with rising demands for cybersecurity, compliance, and governance frameworks like Cyber Essentials. Manual processes for policy updates, tenant health checks, and compliance monitoring are time-consuming, error-prone, and lack automation, consuming valuable resources, leading to risks of non-compliance, security gaps, inefficient licensing, and potential data breaches. This results in lost productivity, budget pressures, and reduced confidence in frameworks like Cyber Essentials.

2. General Service Provision

2.1 Overview

Cloud assist is a Software as a Solution (SaaS) tool that simplifies, streamlines, and adds automation to the management of Microsoft 365 tenants for FE/HE institutions, schools, and research bodies in the UK. Cloud assist is an essential aid to IT teams that are responsible for organisation's Microsoft 365 tenancies. Cloud assist' automating and reporting features alleviate what would otherwise are tedious manual tasks.

Cloud Assist is made up of two main components:

- Health checks, which provide recommendations for optimising a Microsoft 365 tenant in areas like licensing, email security (SPF, DKIM, and DMARC protocols), alignment with Microsoft's security and directory recommendations, and evaluation of Teams and Power Platform configurations in alignment with Jisc cloud recommendations.

- Intune policy management, automated policy management - enabling Intune policy updating and device reporting.

2.2 Features and Functionality

- Microsoft 365 tenancy health checks

- Automation and reporting features:
  - Automatic updates of Microsoft Entra devices with warranty / support information;
  - Automated Entra device clean up to remove stale devices;
  - Automated renaming of fully managed android devices to match a naming scheme;
  - Automate Intune policy updating for OS version requirements;
  - Policy update scheduling;
  - Logging device lifecycle information, (model start/end dates);
  - Microsoft 365 Tenancy health checks - free of charge;
  - Reporting designed to help identify devices which don't comply to policies;
  - See which devices are connected to the tenant (otherwise this could be unknown unless it was done by manual request, response and logging);
  - View devices are out of date - and therefore need addressing through policy management.

3. Service Eligibility Criteria

3.1 Customer Licencing, Authentication and Access Requirements

The prerequisites for Cloud assist are as follows:

Minimum requirements (basic functionality)	Health Check Functionality: • Microsoft 365 A/E/G1 • Microsoft Entra ID (basic) – formerly Azure Active Directory Reporting and Automation Functionality, Device and Application Management: • Microsoft 365 A/E/F3 (includes Intune for Education) • Microsoft Entra ID P1
Recommended requirements (full suite of features)	Reporting and Automation Functionality, Health Check Functionality, Device and Application Management: • Microsoft 365 A/E/F5 (includes Intune for Education) • Microsoft Entra ID P2 • Intune P1 or P2

Jisc makes no warranty or representation that the Services will perform identically across all Microsoft 365 Tenant configurations. Performance, functionality, and User experience may vary depending on:

- The type and licencing level of the Customer's Microsoft 365 Tenant;
- The specific features and capabilities enabled within the Customer's Microsoft 365 environment; and
- The Customer's Microsoft 365 configuration and settings.

Nothing in this Agreement shall be construed as requiring the Customer to upgrade or modify their Microsoft 365 tenant configuration, and Jisc's obligations under this Agreement remain in full force regardless of the Customer's chosen Microsoft 365 licensing tier.

The Customer acknowledges that optimal performance and access to the Services' full suite of features requires adherence to the *recommended requirements* outlined in this section 3.

As a condition precedent to accessing and using the Services, the Customer shall:

- Install and configure the Jisc Cloud assist application within its Microsoft Entra ID (formerly Azure Active Directory) environment;
- grant the necessary permissions and access rights to enable the Jisc Cloud assist application to authenticate users;
- grant Jisc permission to access the Customer's Tenant data for the purpose of providing the Services under this Agreement.

The permission and configurations granted must remain in effect for the duration of the Term between the Customer and Jisc.
The Customer shall:

- maintain an active and compliant Microsoft 365 Tenant throughout the duration of the Term;
- ensure it has access to a Microsoft Global Administrator account (through which all User accounts are managed) with the requisite administrative privileges for such Tenant;
- retain sufficient Microsoft 365 licencing to cover all Users accessing or benefitting from the Services;
- enable network connectivity permitting API access to Microsoft's cloud services;
- configure the Services to meet organisational requirements;
- manage and maintain security settings, permissions and access controls within respective Microsoft Entra ID; and
- ensure configuration changes do not compromise security or functionality.

The Customer warrants that it has the necessary authority and technical capability to install and configure the Jisc Cloud assist application within its Entra ID environment and to grant the required permissions.

The Customer acknowledges and agrees that:

- the addition of the Jisc Cloud assist application to its Entra ID is essential for the proper functioning and User authentication of the Services. Failure to comply will prevent access to the Services;

- the Customer is solely responsible for all prerequisite Microsoft 365 licencing and Tenant costs and obligations;
- the Services' functionality is contingent upon Microsoft 365 services being operational and accessible at the time of use;
- any interruption, suspension, or failure of Microsoft 365 services may result in corresponding interruption, suspension, or failure of all or part of the Service;
- Jisc has no control over the availability, performance, or operation of Microsoft 365 services;
- Jisc shall not be liable for any loss, damage, or failure of the Service that results directly or indirectly from the unavailability, malfunction, or failure of any Microsoft 365 services, regardless of the cause of such unavailability, malfunction, or failure;
- Jisc shall not be liable for any service interruptions or degradation resulting from the Customer's failure to maintain adequate Microsoft 365 licencing and Tenant status.

3.2 Customer Development Requirements

Frameworks and Libraries:

Frontend: React, Fluent UI	*Backend:* .NET Core, C#
Database: Azure Cosmos DB	*Integration:* Microsoft Graph API

Microsoft Graph API compliance

The Customer acknowledges that the Services utilise Microsoft Graph API and other Microsoft APIs (the "Microsoft APIs") to access and manage the Customer Tenant.
Both Parties shall comply with:

- Microsoft's APIs Terms of Use as published and updated from time to time;
- rate limiting and throttling requirements imposed by Microsoft;
- data usage restrictions specified in Microsoft's Overview of metered APIs and services in Microsoft Graph; and
- all technical requirements for API integration and usage.

The Customer hereby consents to Jisc's use of Microsoft APIs to:

- read, modify, create, and delete data within the Customer Tenant as necessary for the Services;
- access User and Customer information required for the Services functionality; and
- perform administrative actions on the Customer's behalf.

Jisc shall:

- implement appropriate error handling and retry mechanisms for API calls;
- respect Microsoft's usage limits and implement exponential backoff procedures;
- maintain secure storage and transmission of API tokens and credentials; and
- promptly address any API compliance violations identified by Microsoft.

The Customer shall not, and shall not permit any third party to:

- reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of the Services;

- copy, reproduce, modify, or create derivative works based on any part of the Services;
- remove, alter, or obscure any proprietary notices, labels, or marks on the Services; and use the Services to develop competing products or services.

4. Service Onboarding

Jisc will use reasonable endeavours to onboard the Customer to the Services within one (1) to two (2) business days, but in no event later than ten (10) business days, following execution of this Agreement by the Customer.

If onboarding is delayed subject to the Customer's provision of required information, Jisc shall not be liable for any resulting delays and the completion timeline may be extended accordingly. Jisc will provide reasonable notice of any such delays and revised timelines.

The technical onboarding process shall include:

- initial consultation and requirements assessment to understand the Customer's Microsoft 365 environment and specific needs;
- configuration of the Services to align with the Customer's existing Microsoft 365 setup and organisational requirements;
- establishment of necessary integrations and API connections with the Customer's Microsoft 365 environment;
- creation of user accounts and assignment of appropriate access permissions;
- customisation of workflows and automation processes according to the Customer's operational requirements;
- provision of initial training materials and documentation.

5. Service Levels

Jisc will use reasonable endeavours to maintain availability of the Services at ninety-nine (99%) uptime, calculated on a monthly basis (the 'Uptime Target).

For the purposes of this section, uptime shall be calculated as the percentage of time during any given calendar month that the Services are available and accessible to Customers, excluding:

- scheduled maintenance or update windows notified to Customers as follows:
  - bug fixes (made without notification): minor disruption to the Services for up to one (1) minute;
  - major updates, including addition of new features: at least twenty-four (24) hours in advance, where downtime of more than one (1) minute is expected.
- emergency maintenance required for security or stability purposes;
- outages caused by factors outside Jisc's reasonable control, including but not limited to internet service provider failures, Microsoft 365 service disruptions and distributed denial of service attacks;
- outages resulting from the Customer's failure to comply with the Agreement or misuse of the Services.

The Uptime Target represents Jisc's commitment to provide reliable service, but does not constitute a service level agreement. The Uptime Target is provided as a measure of Jisc's performance objectives.

Monitoring of the Services will be carried out on a twenty-four (24) hours per day, seven (7) days per week basis with any outages communicated to Customers via email.

System changes will be made within 48 hours of customer notification. Customers will be notified of batch updated features and major functional updates via email.

5.1 Updates and upgrades

The Services include a release note feature to enable Customers to remain updated on new functionality, system updates and resolved issues.

6. Support

The Customer will be able to log tickets for support requests at all times to cloudsolutions@jisc.ac.uk (Jisc Cloud support team).

Jisc will respond to and use reasonable endeavours to resolve support requests if the Customer reports an issue with the Services on a Business Day. For the avoidance of doubt, working hours on a Business Day are between 8:00 and 18:00.

If the Customer discovers a vulnerability within the Services, the Customer shall notify such vulnerability to Jisc at cloudsolutions@jisc.ac.uk. If the Customer discovers a vulnerability within any Microsoft API utilised by the Services (including any such Personal Data Breach involving Microsoft API), the Customer shall report such vulnerability to Microsoft at secure@microsoft.com.

7. Security and Compliance

The Services are included within the scope of our ISO9001 and ISO27001 certificates.

Jisc is fully Cyber Essentials certified.

8. Ancillary Services

8.1 Cloud Professional Services

The Jisc Cloud Professional Services provide specialist technical consultancy to organisations using, or planning to use, the cloud. We draw on our experience of AWS, Azure, and Microsoft 365, Microsoft Intune, etc. to offer organisations skilled resources to meet tactical projects or and aid in the delivery of cloud-centred digital transformation programmes.

8.2 Cloud Professional Services - Security Reviews

Jisc's Cloud Professional Services - Security Reviews, provides specialist technical consultancy to review and benchmark an organisations cloud-based infrastructure against security industry standards and best practice, such as NCSC, CIS as well as some of our own checks. Jisc has a broad range of practical experience in the cloud security domain. We draw on this experience to offer organisations skilled, flexible and pragmatic resources to meet short-term business challenges and/or to contribute to, or lead, longer-term projects or cloud-centred IT

transformation programmes. The Cloud Professional Services - Security Reviews are applicable to the following cloud infrastructures:

- AWS
- Microsoft 365
- Microsoft Azure
- Google Workspaces
- GCP
- Active Directory

Once our Cloud Professional Services - Security Reviews have been completed, we will provide you with a comprehensive report stating what requires remediation and how that remediation might be implemented alongside an impact analysis. Additionally, our Cloud Security team will be able to help you with the remediations (subject to resource availability).