MAXRES General Terms of Service

Last Updated: 03/01/2025

These Terms of Service (ToS) govern your access to and use of MAXRES's software and services, and any MAXRES owned or operated online portals that point to offers provided by MAXRES (collectively, including any updates to or successor products or services). By utilizing the Products and Services, you accept these Terms of Service. MAXRES may update these Terms of Service at any time and will notify you of such changes by updating the last updated date. By continuing to use the Products and Services after the changes become effective, you agree to the new terms. If you do not agree to the new terms, you must cease use of the Products and Services.

1 CONTENTS

2 INTRODUCTION

2.1 EXECUTIVE SUMMARY OF THE MAXRES TERMS OF SERVICE

The MAXRES **Terms of Service** outline the rights, responsibilities, and expectations governing the use of MAXRES software and services. Designed to ensure clarity, compliance, and mutual understanding, the document is structured into key sections that address service deployment options, user obligations, and privacy policies, underpinned by the legal framework of England and Wales.

2.1.1 Key Points:

- **Introduction**:
  - Establishes the document's purpose and scope.
  - Defines essential terms and clarifies the applicability of the terms across all deployment models: SaaS, Azure Managed Application, and On-Premises.
- **Service Deployment Options**:
  - **SaaS**: Provides cloud-based access, prioritising scalability and automatic updates with minimal user-side management.
  - **Azure Managed Application**: Integrates with Microsoft Azure infrastructure, offering enhanced performance and security.
  - **On-Premises**: Grants users' full control over the environment, ideal for organisations with stringent data sovereignty requirements.
- **User Obligations**:
  - Details user responsibilities, including adherence to legal standards, maintenance of account security, and respectful use of services.
  - Lists prohibited activities such as reverse engineering, abuse of the platform, and intellectual property violations.
  - Stresses the importance of safeguarding credentials and reporting breaches promptly.
- **Privacy Policy**:
  - Describes the data collected (personal, usage, and feedback) and its uses (support, improvements, compliance).
  - Explains data retention and deletion policies, ensuring users' rights to request data removal under specific conditions.
  - Outlines scenarios for data sharing, including service provision, legal compliance, and platform security, while maintaining user privacy.
- **Governing Law**:
  - Emphasises that the terms are subject to the laws of England and Wales, with any disputes resolved under the exclusive jurisdiction of these courts.

2.1.2 Purpose:

The Terms of Service aim to balance the operational requirements of MAXRES with the rights and responsibilities of its users. By clearly delineating deployment-specific details, acceptable usage, and privacy safeguards, the document fosters a transparent and secure user experience while ensuring legal compliance and operational efficiency.

This document serves as a cornerstone for all engagements with MAXRES software and services, setting a clear framework for accountability and collaboration.

3 DEFINITIONS

Definitions List for MAXRES Terms of Service:

1. **MAXRES**: The software platform and services offered by MAXRES Limited, a company based in England and Wales, providing tools for managing digital learning environments and other organisational software needs.
2. **User**: Any individual or entity that accesses or uses the MAXRES platform and its services, whether as a subscriber, administrator, or end-user.
3. **Service**: The functionalities, tools, and support provided by MAXRES, including software applications, updates, integrations, and support services.
4. **SaaS (Software as a Service)**: A cloud-based deployment option for MAXRES, where users access the software through the internet without needing to install or maintain it on their own hardware.
5. **Azure Managed Application**: A deployment option where MAXRES is integrated into Microsoft Azure's infrastructure, leveraging Azure's security and scalability features for enterprise use.
6. **On-Premises**: A deployment model where MAXRES software is installed and run on the User's own servers, giving full control over the system but requiring local IT management.
7. **AI-Generated Content**: Content or outputs produced by artificial intelligence tools integrated into the MAXRES platform, such as automated reports, learning materials, or predictive analytics.
8. **Account Credentials**: The combination of usernames, passwords, and other authentication methods that a User uses to access MAXRES services.
9. **Data Sovereignty**: The principle that data stored within a system is subject to the laws and governance structures of the country in which it is physically located.
10. **Intellectual Property (IP)**: Legal rights that protect creations of the mind, including software, trademarks, logos, and any content developed by MAXRES or its Users on the platform.
11. **Prohibited Activities**: Actions explicitly forbidden while using MAXRES, such as hacking, sharing malicious software, or infringing intellectual property rights.
12. **Subscription Agreement**: A formal contract outlining the terms under which a User accesses MAXRES services, typically involving recurring payments for continued access.
13. **Multi-Factor Authentication (MFA)**: An enhanced security measure requiring Users to verify their identity through multiple methods, such as a password and a text message code.

14. **Data Retention**: The policy and practices related to how long MAXRES stores User data after it has been collected.
15. **Third-Party Vendor**: An external company or service provider that assists MAXRES in delivering parts of its platform, such as hosting services or technical support.
16. **Governing Law**: The legal framework (in this case, the laws of England and Wales) that dictates how the Terms of Service will be interpreted and enforced.
17. **Compliance Standards**: The rules and regulations that MAXRES and its Users must adhere to, including data protection laws (e.g., GDPR), cybersecurity protocols, and contractual obligations.
18. **Reverse Engineering**: The process of analysing software to replicate its functionality, which is strictly prohibited under the Terms of Service.
19. **User Rights**: The rights Users have regarding their interaction with MAXRES, including access to their data, privacy protections, and the ability to terminate their subscription.
20. **Resolution Time**: The maximum time within which MAXRES commits to resolving a reported issue, as outlined in the Service Level Agreement (SLA).
21. **Service Level Agreement (SLA)**: A document that defines the expected service standards, such as software uptime, response times, and technical support availability.
22. **Support Channels**: The methods through which Users can contact MAXRES for assistance, such as email, online portals, or dedicated support hotlines.
23. **Anonymised Data**: Information that has been processed to remove personal identifiers, making it impossible to trace back to an individual.
24. **Bug Fixing**: The process of identifying and resolving errors or defects in the software to ensure it operates as intended.
25. **Software Updates**: Improvements or fixes to the MAXRES platform, automatically applied in SaaS deployments, deployed with agreement with the customer on Managed Applications, or manually installed in On-Premises deployments.

This consolidated list, while not exhaustive, ensures a clear understanding of key terms and supports adherence to the MAXRES Terms of Service.

4 Scope and Applicability

4.1 Purpose of the Document:

The MAXRES Terms of Service establish the legal framework for the use of MAXRES software and related services. They outline the rights, obligations, and responsibilities of both MAXRES Limited and its Customers and Users to ensure compliance, accountability, and a seamless operational experience.

4.2 Applicability:

These terms apply to all Customers and Users who access or use MAXRES software and services, irrespective of their role or the deployment option selected. This includes:

1. **Customers**: Individuals or organisations who purchase MAXRES services, including administrators managing deployments.
2. **Users**: Employees, contractors, or third parties (as agreed with MAXRES) authorised by the Customer to use MAXRES services.
3. **Trial Customers and Users**: Individuals or organisations using the platform under a trial or evaluation agreement.

4.3 DEPLOYMENT OPTIONS:

The terms govern the use of MAXRES services across three primary deployment models:

1. **SaaS (Software as a Service)**: Cloud-based access to the MAXRES platform hosted and maintained by MAXRES. This option prioritises ease of use, scalability, and automatic updates but requires consistent internet connectivity.
2. **Azure Managed Application**: Integration of MAXRES into a Customer's Microsoft Azure environment, leveraging Azure-native features for enhanced performance, security, and compliance.
3. **On-Premises**: Local deployment of MAXRES software on the Customer's internal servers. This option grants full control over the software environment but entails higher responsibility for maintenance and updates.

4.4 GEOGRAPHICAL SCOPE:

The terms are universally applicable to all Customers and Users, regardless of geographic location, with specific stipulations for those in jurisdictions governed by additional data protection or compliance laws.

Disputes or legal matters arising under these terms fall under the exclusive jurisdiction of the courts of England and Wales.

4.5 COVERAGE:

The document addresses:

1. **Service Access**: Terms for accessing and using MAXRES services.
2. **Responsibilities of Customers and Users**: Expectations for ethical and lawful use of the platform.
3. **Support and Maintenance**: Standards for technical support and software updates.
4. **Privacy and Data Security**: Policies governing data collection, retention, and sharing.
5. **Dispute Resolution**: Mechanisms for addressing conflicts between Customers, Users, and MAXRES.
6. **Limitations**:
   - The terms do not apply to third-party integrations or software that Customers and Users independently procure and use in conjunction with MAXRES, unless otherwise specified.
   - Specific services or add-ons offered by MAXRES may include supplementary terms, which will take precedence where applicable.

7. **Customer and User Categories**:
   - **Enterprise Customers**: Large organisations deploying MAXRES across multiple teams or regions.
   - **Small and Medium-Sized Businesses (SMBs)**: Organisations leveraging MAXRES for focused operational needs.
   - **Individual Customers and Users**: Independent professionals or consultants using MAXRES for personal projects or limited-scale operations.
8. **Changes and Updates**:
   MAXRES reserves the right to modify the scope or applicability of the terms. Updated terms will be communicated to Customers and Users and will take effect upon publication, unless explicitly stated otherwise.

This section ensures all Customers and Users clearly understand the breadth and applicability of the MAXRES Terms of Service, fostering a cohesive and compliant engagement with the platform.

5 GENERAL TERMS AND CONDITIONS

5.1 ACCEPTANCE OF TERMS

By accessing and using MAXRES's services, you acknowledge and agree to abide by all terms outlined in this document including those of services provided by Third Parties. This includes any updates or amendments made to the terms, as communicated to you. Your use of the services signifies your acceptance of these terms, and if you do not agree, you must refrain from using the services. For continued use, you are encouraged to review these terms periodically to stay informed of any changes.

5.2 CHANGES TO TERMS

MAXRES reserves the right to amend or update these terms of service at any time without prior notice. Any such changes will be effective upon their publication. Where other agreements with MAXRES exist that conflict with these terms, those agreements will take precedence unless explicitly stated otherwise in this document or any subsequent updates.

5.3 GOVERNING LAW AND JURISDICTION

The agreement is governed by the laws of England and Wales, and any disputes arising from it shall be subject to the exclusive jurisdiction of the courts of England and Wales.

6 SERVICE OFFERINGS

6.1 MAXRES SOFTWARE DEPLOYMENT OPTIONS

6.1.1 Software as a Service (SaaS)

MAXRES provides its software as a service (SaaS) to customers, offering cloud-based access to the platform without the need for on-premises hardware.

1. **Conditions**: Requires a stable internet connection and compliance with subscription agreements.
2. **Benefits**: Automatic updates, scalable resources, and reduced IT management.
3. **Limitations**: Dependent on internet availability; offline access is restricted.

6.1.2 Azure Managed Application

MAXRES integrates seamlessly with Microsoft Azure, leveraging managed services for enhanced performance and security. This deployment is ideal for enterprises already utilising Azure infrastructure.

1. **Conditions**: Requires an active Azure subscription and adherence to Azure compliance standards.
2. **Benefits**: Increased security, integration inherited from running the application Microsoft Azure web services facilitating a simplified deployment.
3. **Limitations**: Additional Azure-related costs and regional service restrictions based on Azure availability.

6.1.3 On-Premises

MAXRES software can be deployed directly on a customer's internal servers, granting full control over the operating environment.

1. **Conditions**: Requires dedicated hardware, MAXRES & Customer IT personnel for maintenance, and adherence to MAXRES installation guidelines.
2. **Benefits**: Full data sovereignty, customisation options, and enhanced offline capabilities.
3. **Limitations**: Higher upfront costs, increased maintenance responsibilities, and limited access to automatic updates.

6.2 SERVICE DESCRIPTIONS

- **SaaS**: This deployment provides users with cloud-based access to the MAXRES platform. Services include real-time software updates, robust data security through MAXRES's cloud infrastructure, and scalable storage options. Users benefit from a low-maintenance setup requiring no local hardware and seamless remote access via web or mobile interfaces.

- **Azure Managed Application**: In this deployment, MAXRES is integrated with Microsoft Azure. Services include pre-configured application templates for easy setup, monitoring tools leveraging Azure's analytics capabilities, and enhanced security through Azure's compliance framework. Users gain the ability to use Azure-native services, such as backup and disaster recovery, alongside MAXRES's core functionality.
- **On-Premises**: This deployment involves installing MAXRES software on the user's internal servers. Services include installation assistance, periodic software updates provided through licensed downloads, and customisable configurations to meet specific organisational requirements. Users retain full control over their data and software environment, with MAXRES offering optional support for ongoing maintenance. ### 4. Account and User Obligations

6.3 User Responsibilities

Users are responsible for ensuring their use of MAXRES services is lawful, ethical, and in compliance with the terms set out in this document and all applicable laws. Specifically, users must:

1. **Adhere to Applicable Laws**: Ensure that all activities conducted through MAXRES services comply with local, national, and international laws, including but not limited to data protection, privacy, and intellectual property regulations.

2. **Use Services Lawfully**: Avoid using MAXRES services for any illegal, fraudulent, or harmful purposes, including the dissemination of malicious content or engaging in activities that may damage the reputation or operations of MAXRES.

3. **Respect Intellectual Property Rights**: Users must not upload, distribute, or otherwise use content that infringes on the intellectual property rights of MAXRES or third parties.

4. **Maintain Account Security**: Users are required to safeguard their account credentials and immediately report any unauthorised access or potential breaches.

5. **Avoid Unauthorised Access**: Refrain from attempting to gain unauthorised access to MAXRES systems, accounts, or networks, including through hacking, phishing, or similar activities.

6. **Provide Accurate Information**: Ensure that all information provided to MAXRES is truthful, accurate, and up to date.

Failure to meet these responsibilities may result in the suspension or termination of services, legal action, and the reporting of violations to appropriate authorities where required.

6.4 Prohibited Activities

The following activities are strictly prohibited when using MAXRES and any third-party services when using any MAXRES product or service:

1. **Reverse Engineering**: Attempting to decompile, disassemble, or reverse engineer any part of the MAXRES software or systems.
2. **Abuse of Services**: Engaging in activities that disrupt or interfere with the proper functioning of MAXRES systems, including denial-of-service attacks, spamming, or overloading network capacity.
3. **Unauthorised Access**: Attempting to gain unauthorised access to any accounts, systems, or networks associated with MAXRES.
4. **Use of Malicious Software**: Uploading or distributing malware, viruses, or any other harmful code through the platform.
5. **Violations of Intellectual Property**: Using MAXRES services to infringe upon the intellectual property rights of MAXRES or any third parties.
6. **Illegal Activities**: Engaging in any activity that violates local, national, or international laws or regulations while using MAXRES services.
7. **Misrepresentation**: Impersonating another user, organisation, or entity, or providing false or misleading information to MAXRES.
8. **Data Scraping or Harvesting**: Using automated tools or processes to collect data or information from MAXRES systems without express authorisation.
9. **Bypassing Security Features**: Attempting to disable, bypass, or interfere with any security mechanisms implemented in the MAXRES systems.
10. **Distributing Pirated or Illegal Content**: Sharing or distributing unauthorised copies of copyrighted materials through the platform.
11. **Engaging in Unauthorised Automation**: Deploying bots, scripts, or tools to automate interactions with the platform without permission.
12. **Data Tampering**: Manipulating, altering, or falsifying data to misrepresent outcomes or information.

Violation of these prohibitions may result in immediate suspension or termination of access to MAXRES services and could lead to legal action.

6.5 Account Security

Users must take all reasonable precautions to keep their account credentials secure, including using strong, unique passwords and enabling multi-factor authentication where available. Sharing account credentials with others is strictly prohibited.

1. **For SaaS Deployments**: Breaches or unauthorised access must be reported directly to MAXRES through the provided support channels. This ensures swift action to mitigate risks and address the issue effectively.

2. **For Azure Managed Applications and On-Premises Deployments**: Users are required to first escalate such issues to their internal LCMS management teams. The customer's internal team is responsible for initial triage and containment efforts before engaging MAXRES support for further investigation and resolution.

Failure to maintain the security of account credentials may result in the suspension or termination of services and could expose the user to additional liabilities for any harm caused by the breach.

7 SERVICE LEVEL AGREEMENT (SLA)

7.1 SERVICE AVAILABILITY COMMITMENTS

For MAXRES services, the uptime guarantees and maintenance windows vary depending on the deployment option:

7.1.1 Azure Managed Application and SaaS Deployments

These deployments inherit the Service Level Agreements (SLAs) from Microsoft's Azure platform, which guarantees a 99.9% uptime. These SLAs cover essential infrastructure availability, with specific remedies provided for any service interruptions due to Microsoft's systems. Regular maintenance windows, as outlined by Microsoft, may apply, during which brief service disruptions may occur. MAXRES coordinates with Microsoft to ensure users are notified in advance of any planned outages.

7.1.2 On-Premises Deployments

For on-premises instances, uptime and maintenance responsibilities lie primarily with the customer's internal IT or LCMS management team. MAXRES provides troubleshooting and issue resolution support during pre-agreed service hours, focusing on platform-related issues. However, MAXRES does not directly control the uptime of hardware or networks managed by the customer. Customers are encouraged to implement their own robust monitoring and maintenance schedules to ensure high availability.

For all deployments, MAXRES is committed to minimising disruptions by clearly communicating scheduled maintenance periods well in advance whenever possible. In the event of unscheduled downtime, MAXRES will adhere to the applicable SLA guidelines, ensuring efficient resolution based on the deployment type and associated responsibilities.

7.2 RESPONSE AND RESOLUTION TIMES

7.2.1 SaaS

Severity	Description	Response Time	Rectification Time
A (Critical Failure)	LCMS has failed and is not available for use due to usability issue or recurring instability issues requiring full & daily server reloads as a direct result of issues with the Software. The	Initial response within 2 days.	Workaround within 5 days. Firm resolution within 1 Month from the date

	deficiency has a major impact (work has stopped or tasks cannot be completed) on the overall training content production/management or on one or more training delivery outputs.		raised
B (Impacting Issue)	Deficiency has a major impact on the overall training production/management or on one or more key areas. Training output can be partially achieved but requires undesirable workaround procedures to be followed.	Initial response within 3 days.	Workaround within 5 days. Firm resolution within 2 Months from the date raised
C (Impacting Issue)	Training content production can be conducted however, usability issues or recurring instability issues can be suppressed using a workaround. Deficiency has a minor impact on the overall training output or on one or more sub-tasks of training production. Training content creation can be partially conducted in these areas, and no workaround can be found.	Initial response within 3 days or as agreed in a separate enhanced support agreement.	Workaround within 48 Hours (If required) Firm Resolution within 3 Months from the date raised
D (Non-Impacting Issue)	Deficiency indicates that either a minor adjustment to the workflow is required or a minor cosmetic issue must be addressed and otherwise has no impact on training content production.	Initial response within 30 working days or as agreed in a separate enhanced support agreement.	Firm Resolution within 4 Months from the date raised
E (Non-Impacting Issue)	Minor cosmetic issue to be addressed, otherwise has no impact on LCMS usage.	Initial response within 30 working days or as agreed in a separate enhanced support agreement.	Firm resolution within 5 months from the date raised

7.2.2 Managed Application

Notwithstanding issues that come about because of the Customer's management of their Azure Subscription and/or Resources (which are wholly independently managed by the customer), the Managed Application response and resolution times are as follows:

Severity	Description	Response Time	Rectification Time
A (Critical Failure)	LCMS has failed and is not available for use due to usability issue or recurring instability issues requiring full & daily server reloads as a direct result of issues with the Software. The deficiency has a major impact (work has stopped or tasks cannot be completed) on the overall training content production/management or on one or more	Initial response within 24 hours.	Workaround within 24 hours. Firm resolution within 1 Month from the date raised

	training delivery outputs.		
B (Impacting Issue)	Deficiency has a major impact on the overall training production/management or on one or more key areas. Training output can be partially achieved but requires undesirable workaround procedures to be followed.	Initial response within 24 hours.	Workaround within 24 hours. Firm resolution within 2 Months from the date raised
C (Impacting Issue)	Training content production can be conducted however, usability issues or recurring instability issues can be suppressed using a workaround. Deficiency has a minor impact on the overall training output or on one or more sub-tasks of training production. Training content creation can be partially conducted in these areas, and no workaround can be found.	Initial response within 48 hours or as agreed in a separate enhanced support agreement.	Workaround within 48 Hours (If required) Firm Resolution within 3 Months from the date raised
D (Non-Impacting Issue)	Deficiency indicates that either a minor adjustment to the workflow is required or a minor cosmetic issue must be addressed and otherwise has no impact on training content production.	Initial response within 30 working days or as agreed in a separate enhanced support agreement.	Firm Resolution within 4 Months from the date raised
E (Non-Impacting Issue)	Minor cosmetic issue to be addressed, otherwise has no impact on LCMS usage.	Initial response within 30 working days or as agreed in a separate enhanced support agreement.	Firm resolution within 5 months from the date raised

7.2.3 On Premises

Severity	Description	Response Time	Rectification Time
A (Critical Failure)	LCMS has failed and is not available for use due to usability issue or recurring instability issues requiring full & daily server reloads as a direct result of issues with the Software. The deficiency has a major impact (work has stopped or tasks cannot be completed) on the overall training content production or on one or more training delivery outputs.	Initial response within 24 hours.	Workaround within 24 hours. Firm resolution within 1 Month from the date raised
B (Impacting Issue)	Deficiency has a major impact on the overall training production or on one or more key areas. Training output can be partially achieved but requires undesirable workaround procedures to be followed.	Initial response within 24 hours.	Workaround within 24 hours. Firm resolution within 2 Months from the date raised
C (Impacting Issue)	Training content production can be conducted however, usability issues or recurring instability	Initial response within 48 hours	Workaround within 48 Hours (If required)

	issues can be suppressed using a workaround. Deficiency has a minor impact on the overall training output or on one or more sub-tasks of training production. Training content creation can be partially conducted in these areas, and no workaround can be found.	or as agreed in a separate enhanced support agreement.	Firm Resolution within 3 Months from the date raised
D (Non-Impacting Issue)	Deficiency indicates that either a minor adjustment to the workflow is required or a minor cosmetic issue must be addressed and otherwise has no impact on training content production.	Initial response within 30 working days or as agreed in a separate enhanced support agreement.	Firm Resolution within 4 Months from the date raised
E (Non-Impacting Issue)	Minor cosmetic issue to be addressed, otherwise has no impact on LCMS usage.	Initial response within 30 working days or as agreed in a separate enhanced support agreement.	Firm resolution within 5 months from the date raised

Notes:

1. For **SaaS** and **Azure Managed Applications**, MAXRES works within Microsoft's SLA for infrastructure-related issues.
2. **On-Premises**: Primary responsibility lies with the customer's internal team, with MAXRES providing escalation support for platform-specific issues.

7.3 Exclusions and Downtime

SLA commitments do not apply under the following circumstances:

1. **User-Caused Errors**: Issues arising from misconfigurations, misuse, or unauthorised modifications to the MAXRES platform by the user.
2. **Third-Party Failures**: Interruptions caused by third-party software, integrations, or hardware that are not under MAXRES's control.
3. **Scheduled Maintenance**: Downtime or service interruptions occurring during pre-notified maintenance periods.
4. **Force Majeure Events**: Events outside MAXRES's reasonable control, such as natural disasters, acts of war, terrorism, or governmental actions.
5. **Network or Connectivity Issues**: Problems arising from the user's internet connection, network infrastructure, or ISP-related issues.
6. **Unsupported Configurations**: Use of the platform in environments or configurations that are not officially supported or documented by MAXRES.
7. **Expired Subscriptions or Licenses**: Service interruptions resulting from non-payment or expiration of the user's subscription or license.

8. **Custom Modifications**: Problems caused by custom code, plugins, or extensions not developed or approved by MAXRES.
9. **Customer-Managed Infrastructure**: For on-premises deployments, issues stemming from hardware failures, insufficient resources, or other customer-managed infrastructure issues.
10. **Security Breaches Due to User Negligence**: Issues arising from weak passwords, failure to implement recommended security measures, or unauthorised access due to user actions.
11. **Software Obsolescence**: Problems encountered while using outdated versions of the MAXRES platform that are no longer supported.
12. **Unreported Issues**: Delays or failures caused by the user not reporting issues promptly or providing incomplete information during escalation.
13. **Non-Compliant Usage**: Violations of the terms of service, including unauthorised access, data scraping, or attempts to bypass security measures.

MAXRES remains committed to minimising disruptions and ensuring high service availability within the defined SLA parameters.

8 SUPPORT SERVICES

8.1 LEVELS OF SUPPORT

8.1.1 Basic Support

This level provides users with access to a self-service help desk, which includes an extensive knowledge base, FAQ sections, and email support. Users can troubleshoot common issues at their convenience with a focus on self-guided solutions. This option is ideal for organisations that primarily handle non-critical issues independently and require minimal intervention.

8.1.2 Enhanced Support

Enhanced Support offers up to 50 hours per year of expert call support. Users gain direct access to MAXRES's technical experts for more complex troubleshooting and specialised assistance. This support tier is well-suited for organisations that periodically face advanced issues requiring expert input but do not need continuous dedicated support. Or for smaller organisations that may not have a dedicated IT support team familiar with MAXRES products.

8.1.3 Premium Support

Premium Support includes 100 hours per year of call support, along with access to MAXRES's most experienced technical professionals for critical issue resolution. In addition, Premium customers are assigned a dedicated support manager, who acts as a single point of contact for all support-related needs. This level of support ensures prioritised attention, faster escalations, and tailored assistance, making it the best choice for organisations with high operational dependencies on MAXRES services.

8.2 Support Hours and Availability

Day	Support Hours
Monday	8:00 AM - 6:00 PM (UK Time)
Tuesday	8:00 AM - 6:00 PM (UK Time)
Wednesday	8:00 AM - 6:00 PM (UK Time)
Thursday	8:00 AM - 6:00 PM (UK Time)
Friday	8:00 AM - 6:00 PM (UK Time)
Saturday	Support available only by prior agreement
Sunday	Support available only by prior agreement

Support outside of these hours is not included in the standard service levels and must be arranged through a separate agreement. Any such agreements will outline the terms, conditions, and costs associated with extended support hours.

8.3 Escalation Process

The process for escalating unresolved issues depends on the deployment option and aligns with the general terms outlined in the SLA section:

8.3.1 For SaaS Deployments:

1. Initial issues should be submitted via the self-service portal or email support provided as part of the Basic Support level.
2. If unresolved, users may escalate to MAXRES technical support via Enhanced or Premium support channels.
3. Further escalations will involve assigning the issue to a dedicated support manager (if applicable) who will prioritise the resolution.

8.3.2 For Azure Managed Applications:

1. Issues must first be logged through Microsoft's support channels if they pertain to Azure infrastructure. Users should follow MAXRES-specific guidance for logging tickets with Microsoft.
2. Platform-related issues should then be escalated to MAXRES support via the provided communication channels.
3. Unresolved cases will involve collaboration between Microsoft's and MAXRES's support teams to ensure resolution.

8.3.3 For On-Premises Deployments:

1. Issues should initially be escalated through the customer's internal LCMS management or IT team.
2. If internal resolution is not possible, the issue may then be escalated to MAXRES support for assistance with platform-specific problems.
3. Further escalations will involve MAXRES assigning a technical expert or team to coordinate directly with the customer's IT resources.

Across all deployment options, unresolved issues are tracked using a ticketing system to ensure accountability, with regular updates provided to the user. MAXRES commits to resolving escalated issues in accordance with the severity levels and response/resolution timelines defined in the SLA.

9 SOFTWARE UPDATES

MAXRES may provide periodic updates to its software. Updates are mandatory to ensure the continuity and security of services. A list of supported software versions will be maintained and provided to customers. Legacy versions of the software will eventually become unsupported to maintain high service standards and security.

9.1 FEATURE UPGRADES

Additional features or premium upgrades may be offered at an additional cost. Customers will be informed of the terms and pricing before accessing such features.

9.2 DOWNTIME FOR UPGRADES

MAXRES will notify the Customer of any anticipated downtime due to upgrades at least 48 hours in advance, and such downtime will be scheduled outside of business hours where possible.

9.3 COMPATIBILITY

The Customer is responsible for ensuring compatibility of their systems with MAXRES updates and upgrades. This includes verifying that their hardware meets the minimum requirements for the updated software, and that operating systems, drivers, and other dependent software are appropriately updated. For example, an outdated operating system may no longer support security patches included in MAXRES updates, leading to vulnerabilities. Similarly, using unsupported configurations, such as custom integrations not tested with new versions, may cause failures in system functionality. MAXRES shall not be liable for failures resulting from such incompatible systems or outdated configurations.

9.4 USER OBLIGATIONS OF UPGRADES

Customers are required to review and implement upgrades provided by MAXRES within the timelines specified. Failure to adopt mandatory upgrades may result in degraded performance, security vulnerabilities, or loss of service. Customers must also ensure that their internal processes, personnel, and infrastructure are prepared to accommodate changes introduced by upgrades, including but not limited to training staff, adjusting workflows, and verifying system compatibility.

10 Change Management

10.1 Scope of Changes

Changes encompass any modifications, improvements, or updates made to the MAXRES Construct platform or its supporting infrastructure. This includes:

1. **Software Updates**: Regular updates aimed at improving performance, security, and stability.
2. **Feature Enhancements**: New functionalities or improvements to existing features based on evolving needs or technological advancements.
3. **Bug Fixes**: Resolutions to identified issues that may impact functionality or user experience.
4. **Infrastructure Upgrades**: Improvements to the underlying hardware, cloud infrastructure, or network configurations supporting MAXRES Construct.

Changes may be initiated by MAXRES as part of its continuous improvement strategy or requested by the Customer to address specific organisational needs.

10.2 Change Request Process

Customer-Initiated Changes:

1. **Submission Procedure**:
   a. Customers must submit a formal change request detailing the nature, purpose, and expected outcomes of the change.
   b. Documentation should include the business justification, timelines, and any relevant technical details.
2. **Review and Acknowledgment**:
   a. MAXRES will review the request within 5 business days and provide an acknowledgment outlining the next steps.

MAXRES-Initiated Changes:

1. **Notification Process**:
   a. MAXRES will notify Customers of planned updates or changes through formal communication channels (e.g., email, customer portal) at least 10 business days in advance for non-critical changes.
   b. Critical updates or security patches may be implemented with shorter notice to ensure platform integrity.
2. **Timeline Adherence**:
   a. All planned changes will adhere to predefined timelines to minimise disruptions.

10.3 Evaluation and Approval

1. **Feasibility and Impact Assessment**:

   a. Each change request undergoes a comprehensive evaluation to assess technical feasibility, potential risks, and associated costs.
2. **Joint Approval Process**:
   a. Significant changes require joint approval from MAXRES and the Customer to ensure alignment with operational goals and expectations.
   b. Approval decisions are documented for transparency and accountability.
3. **Additional Costs**:
   a. Bespoke change requests that do not align with MAXRES's product roadmap may incur additional costs, which will be communicated to the Customer during the evaluation process.
   b. Expediting features from MAXRES's product roadmap to align with the Customer's business needs may also involve additional charges. MAXRES will provide a cost estimate and timeline for prioritising such changes.

10.4 IMPLEMENTATION

1. **Deployment Steps**:
   a. Changes are deployed in a controlled environment to ensure stability and compatibility.
   b. Testing includes:
      i. Functional testing to verify the change works as intended.
      ii. Security assessments to ensure compliance with best practices.
      iii. User acceptance testing (UAT) involving key Customer stakeholders.
2. **Communication**:
   a. Customers receive a detailed implementation plan, including timelines, expected downtime (if any), and support contact information.
3. **Service Continuity**:
   a. Measures are taken to minimise service disruptions, including scheduling changes during low-usage periods and maintaining backup systems.

10.5 POST-CHANGE REVIEW

1. **Effectiveness Monitoring**:
   a. Changes are monitored post-deployment to evaluate their impact and effectiveness.
   b. Metrics such as performance improvements, issue resolution rates, and user satisfaction are analysed.
2. **Addressing Issues**:
   a. Any unforeseen issues or feedback from Users are promptly addressed, and corrective actions are taken as necessary.

10.6 VERSION CONTROL AND DOCUMENTATION

1. **Record Maintenance**:
   a. All changes are documented in a version control system, including details of the modification, the rationale behind it, and its impact.
   b. Version histories are maintained to track the evolution of MAXRES Construct.
2. **Customer Updates**:

a. Updated documentation reflecting the changes is provided to Customers, ensuring they are informed about new functionalities, workflows, or configurations.

11 INTELLECTUAL PROPERTY

11.1 OWNERSHIP AND USAGE RIGHTS

1. The MAXRES Construct software (the Software) platform and content involves valuable intellectual property rights which are owned by MAXRES Limited (MAXRES). No rights, title or interest or intellectual property rights in MAXRES or any other assets of MAXRES are transferred to the Customer by way of entering into this agreement.
2. MAXRES grants to the Customer royalty-free, non-exclusive, non-sub-licensable and non-transferable rights to use the Software as installed by MAXRES within the territories agreed upon in the contract.
3. MAXRES grants the Customer the rights to:
   3.1. Use, reproduce, distribute, modify, produce, publish, and display content provided by MAXRES or created using the Software within the territories agreed upon in the contract
   3.2. Register or establish accounts for users within the territories agreed upon in the contract

for the duration of the contract.

4. All intellectual property rights relating to improvements, modifications, customisations, menus, themes, components, plugins, or other code modules (the Plugins) that are created at the direction of and paid for by the Customer shall be wholly owned by the Customer with the following exceptions:
   4.1. Any improvements, modifications, customisations, menus, themes, components, plugins, or other code modules that are created by MAXRES at MAXRES's own internal investment and expense shall be wholly owned by MAXRES
   4.2. Any improvements, modifications, customisations, menus, themes, components, plugins, or other code modules that are created by MAXRES as a result of the Customer paying a product roadmap expediting fee shall be wholly owned by MAXRES
   4.3. MAXRES reserves the exclusive right to approach the Customer to license any of the improvements, modifications, customisations, menus, themes, components, plugins, or other code modules that are the intellectual property of the Customer to third parties, with details of licensing arrangements to be made on a case-by-case basis with agreements in place for either:
   4.3.1. A percentage of the revenues redeemed from the licensing of the intellectual property.
   4.3.2. An exchange of Software or hardware technology from MAXRES to the Customer.
5. All derivative works, modifications, enhancements, or adaptations of the MAXRES Software or Services created by or for the Customer, whether authorised or unauthorised, shall be the exclusive property of MAXRES. The Customer acknowledges that no rights, title, or

interest in such derivative works shall transfer to them without express written agreement from MAXRES.

6. The Software and provision of customer support and maintenance services (the Services) involves valuable intellectual property rights owned, by, or licensed to, MAXRES Limited. No rights, title, or interest or intellectual property rights in the Services, the Software, or any other assets of MAXRES are transferred to the Customer except as specified, the Customer has no proprietary or other interest in the Software and nothing in the agreement transfers any right, title, or interest in the Software to the Customer.
7. If the Services involve the creation or provision of Materials or know-how by MAXRES as part of the Service, MAXRES retains all rights, title, or interest in the intellectual property rights in and associates with the Materials and the know-how (Developed IP).
8. The Customer must not copy, alter, modify, or reproduce the Developed IP or any part of it without MAXRES's prior written consent.
9. MAXRES grants the Customer a royalty-free, non-exclusive, non-sub-licensable and non-transferable licence during the Term to:
   9.1. Use any Developed IP and other intellectual property rights subsisting in the service; and
   9.2. Use the Software

but only for the purpose of receiving the benefit of the Services, and subject to any additional conditions specified.

10. Except as expressly permitted, the Customer must not, and must not allow any other person to:
    10.1. Use the Developed IP, Software or other intellectual property rights subsisting in the Services (Existing IP) except for the purpose of receiving the benefit of the Services;
    10.2. Modify, vary, improve, translate, or adapt the Developed IP, Existing IP, or the Software;
    10.3. Sub-license, disclose, sell, distribute, publish, transmit, or otherwise make available to any third-party any part of the Developed IP, Existing IP, or the Software;
    10.4. Reverse engineer, disassemble, decompile, or otherwise reduce the Software into any human readable form, except to the extent authorised by any applicable law; or
    10.5. Use the Developed IP, Existing IP or the Software for hire or rental, timesharing, service bureau or other similar arrangements

without MAXRES's prior written consent.

Any other rights of the Customer in relation to the Developed IP, the Software or Services are excluded or limited to the fullest extent permitted by law.

10.6. To the extent that MAXRES (or its licensors, licensees, or assignees) develops any updates, new versions, or new releases of the Software, they will be, as between the Customer and MAXRES, owned exclusively by MAXRES and, unless otherwise agreed by the parties, licensed to the Customer.

12 Third-Party Involvement

12.1 Third-Party Providers

MAXRES may integrate third-party services into its offerings. The Customer acknowledges and agrees that the use of such services is governed by the third-party providers' terms and conditions.

12.2 No Liability for Third Parties

MAXRES shall not be liable for any failure or defect in services or products provided by third parties, including but not limited to cloud hosting providers, software vendors, and payment processors.

12.3 Authorised Subcontractors

MAXRES reserves the right to engage subcontractors for the fulfilment of its obligations under this agreement. MAXRES remains responsible for the performance of its subcontractors.

12.4 Notification of Third-Party Changes

MAXRES will notify customers of significant changes in the third-party services it uses, including changes to terms, service discontinuations, or transitions to alternative providers.

12.5 Dispute Resolution with Third Parties

In the event of issues with third-party services, MAXRES may assist customers in initiating communication with the provider to resolve the matter, although MAXRES does not guarantee resolution.

12.6 Indemnification

Customers agree to indemnify and hold MAXRES harmless from any claims arising due to the Customer's misuse of third-party services or violations of third-party terms.

12.7 Direct Access to Products and Services by Third Parties

1. Customers are strictly prohibited from granting direct access to MAXRES products and services to any third-party organisation or individual without obtaining prior written approval from MAXRES.
2. Any unauthorised access or use by a third party will constitute a material breach of these Terms of Service.
3. Customers are responsible for ensuring that any authorised third-party access complies with all terms and conditions outlined in this agreement.
4. MAXRES reserves the right to audit third-party access arrangements to ensure compliance and to take immediate corrective actions, including termination of access, where breaches are identified.

13 WARRANTIES AND DISCLAIMERS

13.1 LIMITED WARRANTY

13.1.1 Applicable Warranties

1. **Platform Availability**: MAXRES warrants that its services will meet the uptime commitments as specified in the SLA, subject to exclusions detailed in the SLA section. This includes both planned and unplanned outages, with service credits or other remedies applied where appropriate, in accordance with the SLA terms.

2. **Data Security**: MAXRES ensures that appropriate technical and organisational measures are in place to safeguard user data against unauthorised access, loss, or corruption. These measures include data encryption, secure access controls, and routine security audits. MAXRES complies with all applicable data protection regulations and commits to notifying affected parties promptly in the event of a data breach.

3. **Technical Support**: MAXRES guarantees the availability of support services as outlined in the Support Services section, tailored to the user's chosen support tier. Basic support includes access to knowledge bases and email assistance, while Enhanced and Premium tiers provide live support with varying levels of response time commitments.

4. **Software Functionality**: MAXRES warrants that its software will perform in substantial conformity with the specifications and documentation provided. This warranty assumes proper use, compliance with system requirements, and deployment within supported environments. MAXRES does not guarantee compatibility with third-party systems not explicitly tested or approved.

5. **Bug Resolution**: MAXRES commits to addressing reported bugs or defects in its software within the timelines defined in the SLA. Critical issues are prioritised to ensure minimal disruption, and non-critical issues are addressed in a structured manner to maintain long-term platform stability and reliability.

13.1.2 Extended Warranties:

1. **Service Continuity**: MAXRES ensures that all services include fallback and recovery mechanisms to mitigate potential downtimes.

2. **Custom Integrations**: For customers with approved customisations, MAXRES will provide limited warranties ensuring compatibility with future updates.

3. **Regulatory Compliance**: MAXRES warrants compliance with relevant industry standards, such as GDPR, ISO 27001, and other applicable regulations.

13.1.3 Limitations of Warranties:

1. **Third-Party Dependencies**: MAXRES is not responsible for failures or service disruptions caused by third-party systems, integrations, or infrastructure (e.g., Azure-managed environments or user-provided hardware).
2. **Custom Modifications**: MAXRES disclaims liability for issues arising from unauthorised or customer-implemented modifications to its software.
3. **Unsupported Configurations**: MAXRES's warranties do not cover deployments in environments or configurations that are not explicitly supported.
4. **Force Majeure Events**: Warranties do not apply during events beyond MAXRES's reasonable control, including but not limited to natural disasters, acts of war, or governmental actions.
5. **User-Caused Errors**: MAXRES does not warrant against problems resulting from user errors, misuse, or non-compliance with documented guidelines.
6. **Software Obsolescence**: MAXRES's warranties apply only to the latest supported versions of its software.
7. **AI-Generated Content**: MAXRES disclaims all warranties regarding the accuracy, quality, or reliability of content generated using AI functionalities within its platform.

By adhering to these warranties and limitations, MAXRES ensures clarity and transparency in its commitments to users, while setting realistic expectations for service delivery and functionality.

13.2 General Disclaimers

MAXRES disclaims all implied warranties or conditions to the fullest extent permitted by law, including but not limited to:

1. **Merchantability**: MAXRES does not guarantee that its software or services are fit for a general or specific purpose unless explicitly outlined in this agreement.
2. **Fitness for a Particular Purpose**: No guarantees are provided that MAXRES services will meet all of the user's specific requirements or objectives.
3. **Non-Infringement**: MAXRES does not warrant that its services or software will not inadvertently infringe on the intellectual property rights of third parties.
4. **Error-Free Operation**: While MAXRES strives to ensure a stable and reliable platform, it does not warrant that the software or services will be entirely error-free or uninterrupted.
5. **Data Accuracy**: MAXRES disclaims responsibility for the accuracy, completeness, or reliability of data processed or generated using its software or services, including AI-driven outputs.
6. **Third-Party Services and Integrations**: MAXRES does not make any warranties regarding third-party systems, plugins, or integrations that interact with its services.

7. **Custom Modifications**: MAXRES disclaims responsibility for issues arising from customisations, alterations, or modifications made to its software by users or unauthorised third parties.
8. **Loss or Corruption of Data**: MAXRES does not warrant against the loss or corruption of data, except where explicitly stated in a separate agreement.

These disclaimers ensure users understand the limitations of implied guarantees, allowing for transparent and realistic expectations regarding the use of MAXRES's software and services.

13.3 Specific Disclaimer for AI-Generated Content

1. MAXRES explicitly waives responsibility for the quality, accuracy, or veracity of AI-generated content produced using its platforms.

2. Users are responsible for reviewing and verifying the accuracy of AI outputs. While MAXRES provides the tools and platform for generating AI-driven content, the customer holds ultimate responsibility for the quality, relevance, and correctness of these outputs. It is the customer's obligation to ensure that any AI-generated content meets their specific requirements and complies with applicable standards, laws, and industry best practices. Additionally, customers must independently assess the outputs for appropriateness and suitability before use or distribution.

14 Limitations of Liability

14.1 Liability Cap

MAXRES shall not be liable for any loss or damage arising under or in connection with these Terms of Service exceeding the total fees paid by the Customer to MAXRES under this agreement in the 12-month period immediately preceding the event giving rise to the liability.

14.2 Direct Damages

MAXRES's liability for direct damages arising from its breach of these Terms of Service or any related agreements shall be limited to the actual, proven damages incurred by the Customer, not exceeding the amount specified in the Liability Cap.

14.3 Maximum Aggregate Liability

In no event shall MAXRES's aggregate liability for all claims arising under or in connection with these Terms of Service exceed an amount equal to the total fees paid by the Customer to MAXRES over the entire term of the agreement or the preceding 24 months, whichever is shorter.

14.4 Indirect and Consequential Loss

MAXRES shall not be liable for any indirect, special, or consequential damages, including but not limited to loss of profits, revenue, goodwill, or anticipated savings, regardless of whether such damages were foreseeable or MAXRES had been advised of the possibility of such damages.

14.5 Exclusions from Liability

MAXRES shall not be liable for:

1. Failures caused by third-party services, networks, or products.
2. Downtime caused by planned maintenance or updates notified in advance.
3. Customer's failure to comply with these Terms of Service, including but not limited to prohibited activities outlined in Section 6.4.

14.6 Force Majeure

MAXRES shall not be liable for any failure or delay in performing its obligations due to events beyond its reasonable control, including acts of God, war, terrorism, civil unrest, strikes, natural disasters, pandemics, and government actions.

15 Deployment and Acceptance

15.1 Overview

This section outlines the deployment process for MAXRES Construct across the three primary deployment models: SaaS, Azure Managed Application, and On-Premises. Each model is designed to meet different organisational needs while ensuring compatibility with the Customer's existing infrastructure. The deployment process prioritises a seamless setup and operational readiness.

15.2 2. Deployment Process

15.2.1 SaaS

1. **Steps for Deployment**:
   - Account creation and subscription activation through the MAXRES portal.
   - Immediate access to the cloud-based platform upon successful subscription confirmation.
   - Guidance for navigating the web interface for setup and initial configurations.

2. **System Requirements**:
   - Stable internet connection with sufficient bandwidth for platform usage.

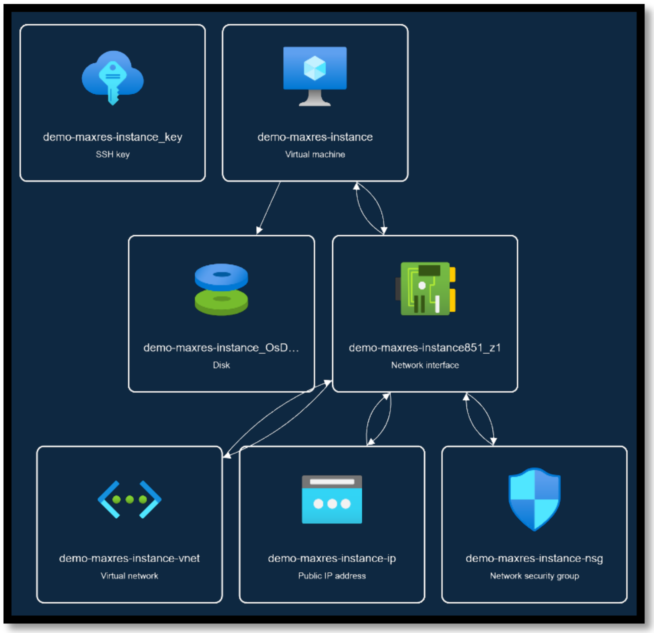
- Supported web browsers include modern web browsers such as Microsoft Edge, Mozilla Firefox, and Google Chrome (any Chromium or Quantum-based web browser). Please note that Internet Explorer is not and will not be supported.

15.2.2 Azure Managed Application

1. **Overview**:
   a. Azure Managed Applications enable MAXRES to deliver solutions that are fully integrated into the Customer's Microsoft Azure environment. These applications utilise Azure's robust infrastructure to ensure performance, security, and compliance. More details can be found *here*.
2. **Transactable Offers**:
   a. **Public Transactable Offers**: Available to all marketplace users with standard pricing and setup configurations. These offers simplify deployment for general use cases.
   b. **Private Transactable Offers**: Tailored to specific Customer needs with customised pricing and deployment settings. Private offers ensure flexibility for unique organisational requirements.
3. **Azure Resource Management Template (ARM Template)**:
   a. ARM Templates are pre-defined scripts used to automate the deployment of infrastructure resources required for the Managed Application. These templates streamline the setup process by defining resource configurations, dependencies, and policies.
   b. MAXRES utilises these templates to ensure consistency and efficiency during deployment.
4. **Integration Steps**:
   a. Customer selects the desired offer (public or private) through the Azure Marketplace.
   b. Permissions and access rights are configured to allow deployment within the Customer's Azure subscription.
   c. ARM Template execution initiates automated resource provisioning, including virtual machines, storage, and networking components.
   d. **Step 4**: Post-deployment validation ensures all resources are operational and configured according to specifications.
   e. **Step 5**: Handover to the Customer for operational use and ongoing management.
5. **Responsibilities and Duties**:

Customer Responsibilities	MAXRES Responsibilities
Managing and paying for Azure resources post-deployment.	Providing and maintaining the ARM Templates for deployment.
Ensuring the required permissions and compliance settings.	Offering technical guidance during the deployment process.
Monitoring deployed resources for performance.	Performing validation checks post-deployment.

6. **Default configuration:**



7. **Scaling Options:**
    a. Enable auto-scaling for virtual machines to handle workload variations.
    b. Use tiered storage solutions to optimise costs based on access frequency.

15.2.3 On-Premises

1. **Hardware and Software Installation**:
    a. Deployment performed using MAXRES hardware, integrated into the Customer's infrastructure.
    b. MAXRES retains root user access to hardware and software for security and operational integrity.
    c. Customer staff receive limited read-only access for diagnostics, verification, and acceptance purposes.
2. **Customisation**:
    a. Deployments are tailored to the specific requirements of each Customer. Typical configurations include:
        i. MAXRES server hardware hosting MAXRES Construct.
        ii. Customer-provided database server hosting a MongoDB database.
        iii. Customer file server for storing the MAXRES Construct filesystem.

This structure ensures MAXRES's intellectual property is protected while granting Customers full access to their data and assets during and after the contractual period.

3. **Support**:
    a. MAXRES provides comprehensive support for setup, testing, and troubleshooting to ensure smooth operations.

15.2.4 Acceptance Criteria for Deployment Completion

1. **System Functionality Checks**: Verification of all features and integrations, ensuring robust compliance with security protocols and enterprise requirements. Functional validation includes stress testing, performance benchmarking, and integration checks with existing systems.
2. **User Training**: Comprehensive, pre-agreed, training sessions tailored to the Customer's operational needs, focusing on role-specific functionalities, security best practices, and troubleshooting techniques. This training ensures that all relevant personnel are proficient in using MAXRES Construct.
3. **Confirmation of Operability**: Final sign-off from the Customer upon successful validation, which includes a review of system performance, security audit results, and end-user feedback. The Customer’s approval certifies readiness for production use in security-conscious environments.

15.2.5 Operational Acceptance Testing (OAT)

1. **SaaS**:
   a. Testing focuses on account activation, accessibility, and basic functionality verification.
   b. Timeframe: Within 2 business days post-deployment.
2. **Azure Managed Application**:
   a. Includes ARM template validation, resource provisioning, and functional tests of integrations.
   b. Timeframe: Within 5 business days post-deployment.
3. **On-Premises**:
   a. Involves hardware installation, configuration, and validation of system interoperability.
   b. Timeframe: Within 10 business days post-deployment.

Responsibilities and Duties:

Customer Responsibilities	MAXRES Responsibilities
Ensuring the availability of required infrastructure.	Delivering deployment assistance and detailed documentation.
Allocating personnel and resources for deployment.	Providing post-deployment support for initial operations.
Providing access to necessary systems and data.	Ensuring compliance with service-level agreements (SLAs).

16 Payment Terms

16.1 Fee Schedule

Payments are due in accordance with the fee schedule specified in the order confirmation or invoice. MAXRES reserves the right to withhold access to services in the event of overdue payments.

16.2 Late Payments

Late payments shall incur an interest charge of 4% per annum above the Bank of England base rate, compounded monthly, on the overdue amount until the payment is received in full.

16.3 Refund Policy

Refunds are only available in cases where MAXRES fails to deliver the contracted services in accordance with the agreed Service Level Agreement (SLA). No refunds are provided for services already rendered.

16.4 Taxes and Duties

The Customer is responsible for all taxes, levies, and duties associated with their use of MAXRES services, excluding taxes on MAXRES's income.

16.5 Microsoft Azure Marketplace

Applicable to Managed Application deployments only.

Payments for Azure Managed Applications purchased via the Azure Marketplace are processed directly by Microsoft. The Customer will be billed through their Azure subscription according to the pricing model displayed on the Azure Marketplace at the time of subscription. All fees are subject to Microsoft's billing and payment terms, and MAXRES does not directly handle payment processing for these transactions. Customers are responsible for ensuring their Azure subscription remains active and in good standing to avoid service disruptions. More information can be found on the *Microsoft Commercial Marketplace Customer Documentation portal*.

17 Compliance and Export Controls

17.1 Compliance with Laws

Customers agree to comply with all applicable local, national, and international laws and regulations, including but not limited to those governing data protection, intellectual property, and export controls.

18 Privacy Policy

18.1 Data Collection and Use

MAXRES collects a variety of data to facilitate and improve the services provided. This includes both personal data and non-personal data.

18.1.1 Personal Data Collected:

1. **Contact Information**: Names, email addresses, phone numbers, and organisational details, primarily used for communication purposes.
2. **Account Information**: Usernames, passwords, and other credentials required to provide secure access to the platform.
3. **Usage Data**: Logs of user interactions with the platform, including session times, activities performed, and accessed features.
4. **Support and Feedback Information**: Details provided during support requests, surveys, or feedback forms, such as issue descriptions and user preferences.

18.1.2 How Personal Data Is Used:

1. **Communication**: To respond to user inquiries, send notifications about updates or changes to the platform, and provide support services.
2. **Issue Resolution**: To diagnose and resolve technical problems or user-reported issues, ensuring the platform operates smoothly.
3. **Platform Improvements**: To analyse usage patterns and gather feedback, which helps in refining features and developing new services.
4. **Compliance and Security**: To monitor activities for security purposes, ensure compliance with applicable laws, and prevent misuse of the platform.
5. **Customisation**: To personalise user experiences by tailoring content, recommendations, or interfaces based on user preferences or past behaviours.

By collecting this data, MAXRES ensures the efficient operation of its services while maintaining a commitment to protecting user privacy. Users have the right to access, rectify, or object to the processing of their data as outlined in the privacy policy.

18.2 Data Retention and Deletion

MAXRES retains data only for as long as necessary to fulfil the purposes for which it was collected, comply with legal obligations, or resolve disputes. Specific retention periods may vary depending on the type of data and applicable legal or regulatory requirements:

18.2.1 Personal Data

Retained for the duration of the user's engagement with MAXRES services and for a reasonable period thereafter to address support requests or any post-termination issues as necessary.

18.2.2 Usage Data

Kept for a limited time to support platform analytics, troubleshoot issues, and improve services.

18.2.3 Support and Feedback Data

Maintained only as long as necessary to resolve the issue or act on the feedback provided.

18.2.4 Process for Deletion Requests

Users have the right to request the deletion of their personal data. Deletion requests can be submitted through MAXRES's support channels or data privacy request forms. Upon receiving a request, MAXRES will:

1. Verify the identity of the requester to prevent unauthorised actions.
2. Evaluate whether the requested data can be deleted without affecting legal or contractual obligations.
3. Confirm the completion of data deletion within the timelines prescribed by applicable laws.

Certain data may be anonymised rather than deleted if required for compliance or analytics purposes. Users will be informed if their data cannot be entirely erased and provided with reasons for the decision.

18.3 Third-Party Data Sharing

MAXRES may share user data with third parties under the following circumstances:

1. **Service Provision**: Data may be shared with trusted third-party vendors, contractors, or service providers who assist in operating the platform, delivering services, or supporting the functionality of MAXRES systems. These parties are required to use the data solely for providing services to MAXRES and are bound by strict confidentiality agreements.
2. **Legal Compliance**: MAXRES may disclose data when required to comply with applicable laws, regulations, or legal processes, such as responding to a court order, subpoena, or other legal request.
3. **Business Operations**: Data may be shared for internal business purposes, such as audits, data analysis, or system maintenance, and in aggregated or anonymised form for statistical or analytical purposes.

4. **Platform Security**: Information may be shared with external security experts or law enforcement to investigate and address security breaches, fraud, or unauthorised activities.
5. **User-Initiated Actions**: If users integrate MAXRES services with third-party applications or platforms, data necessary for the integration will be shared based on user consent and the third party's terms of service.
6. **Corporate Transactions**: In the event of a merger, acquisition, reorganisation, or sale of all or a portion of MAXRES assets, user data may be transferred to the acquiring entity. Users will be notified of such a transfer as required by applicable laws.

MAXRES ensures that data shared with third parties is protected through robust contractual agreements and only shared to the extent necessary for the specified purposes.

5.4 User Rights

Users of MAXRES services are entitled to the following rights concerning their personal data:

1. **Access**: Users have the right to request and obtain confirmation as to whether their personal data is being processed by MAXRES. Upon request, users will receive access to the data and details about how it is used, processed, and stored.
2. **Rectification**: Users may request correction of inaccurate or incomplete personal data. MAXRES will ensure that the necessary updates are made promptly to maintain data accuracy.
3. **Erasure**: Also known as the "right to be forgotten," users may request the deletion of their personal data under specific circumstances, such as when the data is no longer necessary for the purposes for which it was collected, or the user withdraws consent.
4. **Restriction of Processing**: Users have the right to request the limitation of their data processing if they contest the accuracy of the data, object to its use, or require it for legal claims while it is no longer needed by MAXRES.
5. **Data Portability**: Users can request a copy of their data in a structured, commonly used, and machine-readable format to transfer it to another service provider.
6. **Objection**: Users may object to the processing of their data for certain purposes, such as direct marketing or legitimate interests pursued by MAXRES, unless compelling legitimate grounds override such objections.
7. **Withdraw Consent**: Where processing is based on user consent, they have the right to withdraw that consent at any time without affecting the lawfulness of processing conducted prior to the withdrawal.
8. **Lodge a Complaint**: Users can file a complaint with a relevant data protection authority if they believe their data rights have been violated.

Requests related to these rights can be submitted via MAXRES's official support channels or data privacy request forms. Verification of identity may be required to prevent unauthorised actions, and MAXRES will respond within the timeframes prescribed by applicable laws.

18.4 Export Control Restrictions

MAXRES services and products may not be used, exported, or re-exported in violation of any applicable export laws or regulations, including but not limited to export restrictions to certain countries, end-users, or end-uses.

19 Confidentiality and Non-Disclosure

19.1 Definition of Confidential Information

1. Confidential information includes any non-public information disclosed between MAXRES and the Customer, either verbally, electronically, or in writing, that is identified as confidential or should reasonably be understood as confidential by its nature. This includes but is not limited to:
2. Proprietary software details, including source code, architecture, and deployment methodologies.
3. Business strategies, financial data, and operational plans.
4. User data collected or processed through MAXRES systems.
5. Intellectual property, including patents, trademarks, trade secrets, and copyrighted materials.
6. Documentation, training materials, and any other deliverables provided by MAXRES.

19.2 Obligations of the Parties

1. **MAXRES's Obligations:**
   a. Safeguarding all Customer data and ensuring it is not disclosed to any third party without the Customer's explicit written consent.
   b. Using Customer data solely for purposes agreed upon, such as service provision, troubleshooting, or improving MAXRES offerings.
   c. Implementing robust technical and organisational measures to prevent unauthorised access, disclosure, or misuse of confidential information.
2. **Customer's Obligations:**
   a. Protecting MAXRES's proprietary information, including but not limited to software source code, deployment methods, and documentation, ensuring it is not disclosed or shared without explicit consent.
   b. Restricting access to MAXRES's confidential information to authorised personnel only and ensuring such personnel are bound by similar confidentiality obligations.
   c. Using MAXRES's information solely for the purposes outlined in the contractual agreement.

19.3 Exclusions

The obligations of confidentiality do not apply to information that:

1. Is or becomes publicly available without breach of these terms.
2. Was known to the receiving party prior to disclosure by the disclosing party.

3. Is independently developed by the receiving party without use of or reference to the disclosing party's confidential information.
4. Is disclosed with the prior written consent of the disclosing party.
5. Is required to be disclosed by law, regulation, or valid legal process, provided the disclosing party is given prior notice (to the extent legally permissible) and an opportunity to contest such disclosure.

19.4 Duration of Obligations

The confidentiality obligations outlined herein shall survive the termination or expiration of the agreement between MAXRES and the Customer. The duration of these obligations extends for a period of five (5) years post-termination unless otherwise specified in writing.

19.5 5. Breach and Remedies

1. **Actions in the Event of Breach**:
   a. Upon discovering a breach, the non-breaching party must promptly notify the other party and provide details of the breach.
   b. Both parties shall cooperate in good faith to investigate and mitigate the effects of the breach.
2. **Legal Recourse**:
   a. The injured party reserves the right to seek injunctive relief to prevent further unauthorised use or disclosure of confidential information.
   b. The injured party may pursue legal action to recover damages or enforce specific performance under the terms of this agreement.
3. **Remedies**:
   a. Reimbursement for all costs and damages arising from the breach, including legal fees.
   b. Implementation of corrective measures to prevent recurrence of such breaches.

This Confidentiality and Non-Disclosure section ensures the mutual protection of sensitive information, fostering trust and compliance between MAXRES and the Customer.

20 Termination

20.1 Termination by MAXRES

MAXRES reserves the right to terminate this agreement with immediate effect if the Customer:

1. Breaches any material term of this agreement and fails to remedy the breach within 30 days of receiving written notice.
2. Becomes insolvent or enters into bankruptcy proceedings.

20.2 Termination by Customer

20.2.1 SaaS Deployment

Customers utilising the SaaS deployment model may terminate their subscription by turning off auto-renewal in their account settings. If auto-renewal is disabled, the subscription will not renew at the end of the current payment period, and the Customer's account will be deactivated.

20.2.2 Azure Managed Application

Customers using the Azure Managed Application deployment model may terminate their subscription by cancelling through the Azure Marketplace. The cancellation will take effect at the end of the current payment period, and the application will cease to operate. Customers are advised to ensure any necessary data backup or migration is completed prior to the end of the subscription period.

20.2.3 On-Premises Deployment

For Customers with an On-Premises deployment, the agreement will auto-renew with serial keys provided to maintain the operational functionality of the LCMS. Customers wishing to terminate the contract may do so by providing written notice to MAXRES at least 90 days prior to the end of the current term. If the agreement is not renewed, the LCMS will cease to function at the end of the current payment period, and any associated serial keys will be deactivated.

20.3 Post-Termination Obligations

Upon termination:

1. All outstanding fees become immediately due.
2. The Customer must cease use of all MAXRES services and delete or return any MAXRES-provided materials, including software and documentation.

20.4 Data Retention Post-Termination

1. MAXRES will retain customer data for a period of 30 days post-termination to facilitate data export. After this period, all customer data will be permanently deleted unless otherwise required by law.

20.5 Effect of Termination

1. Termination of this agreement shall not affect the accrued rights and obligations of either party as of the termination date. The Customer retains ownership of any data or intellectual property they provided to MAXRES, subject to any licenses granted under this agreement. However, the Customer loses access to MAXRES services and all associated benefits after termination. MAXRES will retain customer data for a period of 30 days post-termination to facilitate data export. After this period, all customer data will be permanently deleted unless otherwise required by law.

20.6 SURVIVAL

The following provisions of this Agreement shall survive termination or expiration for any reason and remain in full force and effect:

1. **Intellectual Property (Section 11) –** Protection of MAXRES's ownership rights and restrictions on use of the software and services.
2. **Confidentiality and Non-Disclosure (Section 18) –** Obligations to maintain the confidentiality of proprietary or sensitive information.
3. **Warranties and Disclaimers (Section 13) –** Disclaimers and limitations that apply to prior use of the services.
4. **Limitations of Liability (Section 14) –** Limitations on MAXRES's financial exposure, including caps on damages.
5. **Payment Terms (Section 16) –** Any outstanding payment obligations incurred prior to termination.
6. **Governing Law and Dispute Resolution (Sections 5.3 and 20) –** Jurisdictional provisions and dispute resolution procedures.
7. **Data Handling and Privacy Obligations (Sections 6.6 and 6.7) –** Terms related to data retention, deletion, and privacy compliance.

These clauses shall survive to the extent necessary to enforce or give effect to their intended purpose, including resolving any disputes arising from this Agreement.

21 DISPUTE RESOLUTION

21.1 GOOD FAITH NEGOTIATION

In the event of a dispute, the parties agree to first engage in good faith negotiations to resolve the issue. Each party shall appoint a representative with the authority to make decisions regarding the dispute. These representatives shall meet within 10 business days of receiving written notice to discuss the dispute. A mutually agreed agenda should guide the discussions, and outcomes shall be documented in writing. If necessary, the parties may involve a neutral third-party facilitator to enhance the negotiation process.

21.2 MEDIATIONS

If a resolution cannot be reached through negotiation, the parties agree to submit the dispute to mediation in accordance with the rules of the Centre for Effective Dispute Resolution (CEDR). The mediation shall take place in London, England. The costs of mediation, including fees for the mediator and administrative expenses, shall be shared equally by both parties unless otherwise agreed. Each party shall bear its own costs, such as legal representation or travel expenses, incurred in connection with the mediation process.

21.3 Arbitration

If mediation fails, the dispute shall be resolved by arbitration under the Arbitration Act 1996. The arbitration shall be conducted in London, England, by a single arbitrator appointed by mutual agreement or, failing agreement, by the President of the Chartered Institute of Arbitrators.

21.4 Jurisdiction

The courts of England and Wales shall have exclusive jurisdiction over any disputes that cannot be resolved through mediation or arbitration.

22 Contact Information and Notices

22.1 How to Contact MAXRES

Customers can contact MAXRES for support or legal notices via the following methods:

Email: Your organisation's account manager

Email: *support@maxres.ai*

Postal Address: MAXRES Limited, MAXRES Limited, Future Space, University of the West of England, Bristol, BS34 8RB, England

22.2 Notice Delivery Mechanisms

Legal or formal notices must be delivered through one of the following methods:

Registered Post: Notices sent via registered post are deemed received three business days after posting.

Email: Notices sent to the official email address listed above will be considered received upon acknowledgment of receipt.

23 Appendix

- *Microsoft Standard Contract*
- *Microsoft Commercial Marketplace Customer Documentation*
- *Microsoft Azure Legal Information*
- *OpenAI Terms of Use*