



LEXACOM[®]

Lexacom Service Definition



Lexacom Service Definition

Page	Content
2	Service Description
2	Service Features
2	Service Benefits
3	Hosting Location
3	Operation
3	System Requirements
4	Security
4	Resilience
6	Governance
7	Analytics
7	Onboarding and Offboarding
9	Support
11	After Sales Support
12	Outage and Maintenance Management
12	Data Extraction
12	Contract Expiry



Service Description

Lexacom is a comprehensive platform that helps organisations make the most of their time. It brings tasks, data, systems, and people together by combining speech recognition, ambient voice technology, digital dictation, AI, workflows, and text messaging, and letting users choose the features that suit their role and digital confidence.

Service Features

- Real-time, 99% accurate speech-to-text across all applications
- Dictation for all document types and clinical workflows
- Optional AI workflows and configurable documentation modes
- Medical vocabulary and automatic clinical coding
- Single platform combining dictation, AI, workflows, and reporting
- Fully configurable specialty specific workflows
- Mobile, tablet, and desktop applications included
- Configurable usage and activity reporting built in
- UK MDR Class I device, ISO 27001 / ISO 9001 accredited
- Simple installation and updates

Service Benefits

- All professional documentation tools in one secure platform
- Save time, reduce admin, improve productivity and wellbeing

- Work in the office, at home, and on the go
- Quicker, more accurate, and complete data entry
- Simpler working on one platform instead of several
- Faster turnaround for letters, notes, and referrals
- Easy adoption for users of all digital confidence levels
- Data security onboarding packs for simplified compliance
- Lower operational costs through automation and efficiency
- Flexible pricing and licensing to suit your organisation

Hosting Location

Both the Lexacom application and its data are hosted in Microsoft Azure UK South (London) and UK West (Cardiff).

Operation

The Lexacom application has been developed to have consistent appearance and functionality across desktop, tablet, and mobile clients, providing a fully cross platform experience.

System Requirements

Client PC Minimum Specification:

Operating System	CPU	RAM	Disk	Network
Windows 10	2 GHz Dual Core CPU	4GB	2GB	Gigabit ethernet

Security

All dictation audio and related data are transmitted from the client application to Lexacom's UK-based Microsoft Azure environment over encrypted HTTPS connections using TLS 1.2 or higher.

Audio is uploaded securely once a dictation is completed and is stored only for the minimum period required to support processing and workflow requirements, in line with configured retention controls. Where speech recognition is used, audio is transmitted in encrypted segments during dictation to support transcription.

All communications between client applications and Lexacom services are encrypted in transit, and data at rest within the platform is protected using AES-256 encryption. Network access is restricted to required ports and services, with traffic protected by Azure-native security controls.

Data is processed solely within UK datacenters, and secure disposal is applied in accordance with retention and lifecycle management policies.

Regular penetration testing is carried out on the Lexacom infrastructure.

Resilience

Lexacom has a detailed and comprehensive Business Continuity Policy. This policy provides a flexible response so that Lexacom can:

- Respond to a disruptive incident (incident management)
- Maintain delivery of critical activities/services during an incident (business continuity)

We ensure high service resilience by leveraging Microsoft Azure cloud, which embodies robust asset protection and resilience measures in line with the UK Government's cloud security principles.

Hosted in Azure UK South/UK West, our service benefits from built-in redundancy to safeguard against failures, ensuring continuous service availability. Azure's comprehensive security includes multi-layered defenses, stringent access controls, and continuous network monitoring, mitigating risks from physical and cyber threats.

Our architecture is designed to automatically scale and reroute traffic between Azure's resilient frameworks, minimizing downtime and performance bottlenecks. Data is encrypted both at rest and in transit, with regular backups stored securely across multiple locations to enable rapid recovery in case of an incident.

Microsoft Azure complies with key certifications, ensuring that our infrastructure meets high standards for security and data protection.

Responsibilities and Process

Persons with authority during and after an incident must be assigned roles. The process follows these steps:

1. An incident is logged when an event occurs
2. The event is identified as a business continuity event
3. A team is created, based on the following roles:
 - a. Incident Commander - responsible for owning the incident and facilitating any changes that need implementing
 - b. Subject Matter Expert - responsible for applying the changes required
 - c. Senior Management Team - escalation point
 - d. Relevant Third Parties

Data backup, restore and disaster recovery

Customer data consisting of binary large objects (blobs) is held in Azure Storage. Blobs are stored using Locally Redundant Storage (LRS). LRS means that data is replicated to multiple storage scale units within a single

datacentre. As such, Azure Storage highly available service, so no traditional backup or recovery procedures are required.

Azure offers point-in-time-recovery (PITR) backups. PITR backups allow restoration to a specific point in time and occur every 5-10 minutes.

Governance

Lexacom are dedicated to providing the most robust security policies utilising technology and best practice. A comprehensive collection of security policies is maintained, which cover:

- Acceptable use
- Data access and handling
- Cryptography
- Telecommunications
- Information handling
- Incident response
- Data (backup and antivirus)
- Data protection (employee and customer)
- Disaster recovery
- Business continuity
-



Policies are reported within an information security management system, and all security policies are reviewed and updated by the Head of IT and senior management team.

Lexacom software meets or exceeds all applicable safety, regulatory and assurance requirements, including:

- DTAC (Digital Technology Assessment Criteria)
- DSPT (Data Security and Protection Toolkit, organisation ID: 8J566)

- Cyber Essentials Plus
- Regular CREST-approved penetration testing
- ISO 27001 (Information Security)
- ISO 9001 (Quality Management)
- DCB0129 clinical safety standard - led by a GMC-registered Clinical Safety Officer
- UK GDPR and the Data Protection Act 2018
- Clinical system integration via IM1
- MHRA Class 1 medical device
- Clinical safety case reports
- Technical architecture summaries

Analytics

Lexacom provide customers with detailed service metrics. These are important to monitor application usage and return on investment. This can include activity levels and productivity gain measurements.

Reporting Types

- Real-time dashboards
- Regular reports
- Reports on request

Onboarding and Offboarding

To help users start using our service, we offer a range of comprehensive support and training options designed to meet diverse needs. We offer tailored onboarding sessions that can include both onsite and online training, allowing users to choose the format that best suits their requirements and learning preferences.

Our onsite training is available at an additional cost, and is delivered by experienced professionals who provide hands-on guidance, ensuring users are fully comfortable with our technology.

For clients who prefer remote learning, we host regular interactive webinars to accommodate various time zones and work schedules.

In addition to our robust training programs, all users have access to extensive user documentation. This includes easy-to-follow manuals, FAQs, and troubleshooting guides, available on our website and within the application itself. We also maintain a dedicated support team ready to assist via phone or email.

For larger projects our aim is to provide a flexible implementation, tailored specifically to the requirements and timescales of the customer, ensuring the smoothest solution roll out and user onboarding.

A project plan is created and shared with the customer. This clearly defines roles and responsibilities within the project.

Lexacom provide a dedicated Account Manager and Project Manager to work with the customer to ensure successful delivery of services.

Project progress is documented in a Project Initiation Document (PID) which acts as the contract or central reference point throughout the project lifecycle.

Outcomes of the project are evaluated against expected benefits, sign off obtained once agreement is reached that all scope has been delivered. Project Closure and Business as Usual documentation is supplied, and a formal handover takes place with Account Management and Operational teams.

Support

Lexacom are committed to providing efficient and friendly technical support for end users and support teams.

We provide a Helpdesk facility and can be contacted by telephone, email or via our website. The Helpdesk is manned with appropriately trained personnel, both from a user and technical perspective. It provides from first line to third line support.

Users are entitled to service and support from the Helpdesk team, who act as the single point of contact for service user issues and feedback, supplying the following services as standard within the hours of 9am-5pm, Monday to Friday, with 24/7 access to online Helpdesk resources:

- Manned telephone support
- Monitored email support
- Remote assistance using remote control where required
- Planned or emergency on-site assistance



We use a range of secure user-friendly remote support tools and will be directed by customer preference, if remote access is necessary or desirable to provide technical support.

The Supplier Helpdesk team receive continued professional

development within their roles. The team are experienced in providing technical assistance to healthcare organisations including NHS Trusts, and appreciate the importance of clear communication, active listening, and timely responses and resolutions.

All technical enquiries are documented and recorded within our internal CRM system. These are given unique case numbers that are shared with the customer so they can easily monitor ticket statuses. End users are notified directly when any case is closed.

Customer specific reports can be provided periodically and on request to measure against the standard service level agreement or agreed KPIs.

Lexacom also enables self-help for more confident end users, and provides guides, training videos, and answers to the most frequently asked questions on its website.

Helpdesk Business Continuity

Cross training is performed which means additional fully trained personnel are available from other business areas that can assist with the Helpdesk should the need arise. Active communication with other internal teams, such as research and development, provide insight and allow collaboration for challenging cases.

Issue Resolution & Timelines

Lexacom operates the following standard industry break-fix times for all issue types including configuration and hardware:

Severity	Response Time	Resolution Time
High (critical service impact)	0-8 hours	Within 2 working days
Medium (significant impact)	2 working days	Within 5 working days
Low (low service impact)	5 working days	Within 5 working days

Escalation Process

When needed, system critical issues go directly to the Supplier's SMT (senior management team) for prioritisation of resources, and emergency support will be made available out of hours if necessary.

Functionality During Outages

Helpdesk personnel working at different locations, and multiple methods of contact reduce the impact on service during any outages. Lexacom provides detailed user manuals, and via its website, guides, training videos, and answers to the most frequently asked questions which can mitigate the impact on technical support during an outage.

Helpdesk KPI

- 95% of calls are resolved on the initial contact.
- Average time of 15 minutes to resolve a case at first line contact.
- 98% user satisfaction, via after-call survey, with the handling and outcome of the call.

After Sales Support

Each Lexacom subscription provides customers with full helpdesk support. This includes telephone, email, and remote access assistance. The subscription also includes access to our training team. Remote training is available at no extra cost. All customers have access to an account manager for enquires not related to software support.

Our website and support centre also provide online support and training resources such as videos and quick start guides. Software updates are included in the subscription price and Lexacom auto updates to ensure users are on the latest release.

Outage and Maintenance Management

We are committed to transparency and prompt communication in the event of service disruptions.

We employ multiple methods to ensure our users are well-informed and can plan accordingly during outages. We include information on the nature of the outage, the services impacted, the expected time for resolution, and any recommended actions for users.

We add details of any service outage to our website in a prominent place. Our help desk telephone lines also plays a recorded message to callers. We have the capability to send email alerts to all affected users in the event of an outage.

Data Extraction

For Lexacom customers, data extraction at the end of a contract is only applicable to users who use the workflow elements of Lexacom. These customers retain full ownership of their data and can request an export before or at contract termination.

On request, we provide a secure export of the workflow data in standard, interoperable formats so it can be transferred to another system. Our team manages the extraction process and supplies the data via secure transfer.

Contract Expiry

At the end of the contract, users are given advance notice of the contract expiry. On the final day of the contract period, access to all elements of the application is removed. If a customer decides to return, access can be re-initiated within a defined period after expiry, allowing them to resume use of the service without disruption.