



SymTerra

Service Definition Document

G-Cloud 15

www.symterra.com

Last updated July 2025

1. Key Company Details

1.1. Business Details

- 1.1.1. Name: Keamore Limited
- 1.1.2. Business Address: 14 Fountain Street, Guisborough, United Kingdom, TS14 6PP
- 1.1.3. Main Office Address: Floor 1, C3 Bureau, Design District, 13 Soames Walk, London SE10 0AX
- 1.1.4. Company House details: 06689064

1.2. Relevant Financial Details

- 1.2.1. **VAT registration:** 938 5243 02
- 1.2.2. **Constructionline ID:** 1209644
- 1.2.3. **DUNS:** 211237215

1.3. Cyber Security & Data Protection

- 1.3.1. GDPR registration ZA770134
- 1.3.2. Cyber Essentials certificate
- 1.3.3. Certification: All data is hosted & processed in the UK on Google Cloud Platform (London)
- 1.3.4. ISO 27001 certified

2. Cloud Technology and Information Security

- 2.1. SymTerra's primary infrastructure is managed and provisioned through Google Cloud Platform (GCP); a widely adopted, market leading cloud platform and IaaS (Infrastructure as a Service) provider used by hundreds of thousands of businesses worldwide. GCP provide over 200 innovative, secure and robust services backed by over 30 different security standards and compliance certifications to support fast-growing businesses and government agencies.
- 2.2. We use the London (UK) cluster of locations to serve our application and store associated customer data. The availability zones are distinct, physically separated data centres. They offer redundant power and global connectivity, allowing us to develop, test and deploy the SymTerra platform with fault tolerance and scalability in mind. Furthermore, all traffic between availability zones is encrypted, so fault tolerance does not compromise on security.
- 2.3. SymTerra follows best practices for quality and information security management with a comprehensive system of procedures and controls maintained and reviewed regularly.
- 2.4. SymTerra also maintains a UK Gov NCSC Cyber Essentials Plus certification to guard against cyber threats and demonstrate our robust position to information security.

3. Compatibility & Accessibility

- 3.1. SymTerra works across iOS and Android and can be downloaded from the App Store or Play Store. The app is also available on tablet devices, excluding Amazon's tablet devices.
- 3.2. The SymTerra web platform is fully available through use of a modern web browser and requires no specialist software or requirements deemed unconventional in a typical office IT environment.
- 3.3. SymTerra provides Single Sign-on through Microsoft 365, which allows users to use their Azure Active Directory (AD) credentials to authenticate and access the system should this be required.

4. Data Protection & GDPR

- 4.1. We are registered with the Information Commissioner's Office under registration number ZA770134 and you can view more details about our registration by following the link to the ICO website [here](#).
- 4.2. For the DPA and in-line with the GDPR, John Ryan is the Data Controller. Our full privacy policy and information on cookies is available [here](#).

5. Security

- 5.1. All data is hosted on GCP and processed in the UK with redundancy and encrypted disaster recovery back-ups in place.
- 5.2. SymTerra holds a Cyber Essential Plus certificate and ISO 27001 accreditation.
- 5.3. A valid HTTPS certificate is used at all times.
- 5.4. SymTerra has implemented appropriate security measures and follows recognised industry standards for protecting information and managing cybersecurity risks. Our approach to compliance involves several key practices:
- 5.5. Regular Security Audits: We conduct regular security audits and assessments to ensure that our solution aligns with the latest NCSC security standards. This includes vulnerability assessments, penetration testing, and code reviews to identify and address potential security risks.
- 5.6. Secure Software Development: Our solution is developed using secure coding practices. We follow industry best practices to prevent common security vulnerabilities such as SQL injection, cross-site scripting, and others.
- 5.7. Access Control: We implement role-based access control, allowing Clients to define granular access permissions for users based on their roles and responsibilities. This minimises the risk of unauthorised access to sensitive information.
- 5.8. Regular Updates: We continuously monitor NCSC's updates and recommendations to ensure that our security practices remain up to date. Regular updates and patches are deployed to address any newly identified vulnerabilities.
- 5.9. DDoS Protection: Our systems are safeguarded against potential Distributed Denial of Service attacks.
- 5.10. Incident Response Plan: Our dedicated security team is always prepared to respond swiftly and effectively to any potential security incidents.
- 5.11. Continuous Security Training: Regular training sessions keep our team updated with the latest security threats and countermeasures.

6. Service Levels and KPIs

- 6.1. SymTerra's availability and uptime is 99.95%.
- 6.2. Our support team adheres to predefined response times based on the priority level assigned to each reported fault. Critical issues receive immediate attention, and response times vary for high, medium, and low-priority issues.
- 6.3. Upon receiving the reported fault, our support team will conduct an initial assessment to diagnose the issue's root cause. This assessment involves analysing system logs, configurations, and user interactions.
- 6.4. Our team will engage in systematic troubleshooting to identify the underlying cause of the reported fault. Our aim is to resolve the issue swiftly and effectively, minimising service disruptions. Throughout the resolution process, we maintain transparent communication and regular updates on the progress and expected resolution timeframe.

7. Back up

- 7.1. All data held within SymTerra's servers is backed up in real-time. Weekly and monthly snapshots are also taken and stored encrypted offline. These are retained for the lifetime of the contract with the Client.

8. Disaster Recovery Plan

- 8.1. We have a robust disaster recovery plan in place. In the unlikely event of a major incident, we have protocols to restore services and data with minimal downtime, ensuring continuity.

9. Software Development

- 9.1. Our in-house engineering team develops and maintains SymTerra using Agile methodologies. This provides for regular release updates and allows us to respond rapidly to our evolving product roadmap and client feedback.
- 9.2. SymTerra provides a live environment (production), which is where users complete their day-to-day operations. SymTerra also has a labs environment, which is a sand box testing environment and a replica of the production environment. Where applicable users can trial, test and learn existing and new features. This testing environment is to specifically mitigate the risk of impacting live operations and ensure the stability and reliability of SymTerra.

10. Helpdesk

- 10.1. We offer a comprehensive helpdesk service to ensure smooth operations and user satisfaction. This is a robust helpdesk accessible through multiple channels, designed to provide efficient support and issue resolution.
- 10.2. **Telephone:** Recognising the importance of immediate assistance, our helpdesk is also reachable via a designated mobile line that crucially isn't hidden from users. This is available 24/7 and provides prompt resolution of urgent issues and critical needs.
- 10.3. **Email:** We have established a dedicated email address, where authorised users can send support requests and report any issues. Our dedicated support team will actively monitor this email address to promptly address inquiries and provide timely assistance – within 2 hours.
- 10.4. **Online Application:** To streamline support processes, we offer a helpdesk ticketing system through Jira. This platform enables authorised users to submit support requests, track the progress of their inquiries, and engage in effective communication with our support team. This centralised system ensures efficient issue management and clear communication throughout the support process.
- 10.5. Our commitment to offering a comprehensive helpdesk service, accessible through email, an online application, and telephone, underscores our dedication to providing exceptional support and maintaining a positive user experience.
- 10.6. SymTerra has a dedicated internal support team based at our offices in London, UK. Customer support agents are available by telephone, SMS, email and via the web.
- 10.7. Our support agents manage requests via Jira, which is an integrated cloud-based customer service platform. Our integrated support system is available 24/7, 365 days.
- 10.8. We also have a knowledge centre with videos tutorials for all the main features of the platform, which is shared as a private YouTube link. These are walk-throughs and FAQ's relating to common queries.
- 10.9. Self-help knowledge base articles including tips and tricks are also available and are distributed via HubSpot.

11. Support hours and typical response and resolution time for support

11.1. We aim to respond to 90% of customer support tickets within 20 minutes and 100% within one hour during UK business hours, when our team are online.

	Severity 1 Critical	Severity 2 High	Severity 3 Medium
% of End Users Affected	75-100%	30-75%	15-30%
Response Time	1 hour or less	2 hours or less	8 hours – 1 business day
Resolution	24 hours or less from first response	36 hours or less from first response	3 business days from first response