



DEFENDED SOLUTIONS

Terms and Conditions:

Cloud Hosting

1. Document Control	2
2. Confidentiality	2
3. Introduction.....	3
4. Service Overview.....	3
1. Definitions	3
2. Scope of Services.....	3
3. Term and Termination.....	3
4. Customer Responsibilities	3
5. Service Provider Responsibilities.....	3
6. Service Levels and Support.....	3
7. Incident and Fault Management.....	3
8. Escalation	4
9. Onboarding and Offboarding	4
10. Data Backup and Disaster Recovery.....	4
11. Security and Governance	4
12. Data Access and Exit.....	4
13. Confidentiality	4
14. Complaints.....	4
15. Limitation of Liability	4
16. Governing Law.....	4

1. Document Control

Document Change Control		
Document Title:	ds_terms_conditions_cloud_hosting.docx	
Issue Date:	23 January 2026	
Date Printed:	23 January 2026	
Created by:	Alexander Delaney	
Document Distribution:	Defended Solutions	Alexander Delaney

Document History			
Date	Description/Comments	Created by	Version
18 th April 2024	Initial Draft Document Created	Alexander Delaney	V1.0

2. Confidentiality

All information shared between the customer and the service provider during the integration of cloud services is considered confidential and will be treated as such. Both parties agree to maintain the confidentiality of sensitive information, including but not limited to business processes, technical details, and proprietary data, unless required by law or mutually agreed upon for specific purposes related to the service integration.

3. Introduction

This document sets out the Terms and Conditions governing the provision of Cloud Hosting services by Defended Solutions. It defines the contractual framework under which cloud hosting services are delivered, including responsibilities, limitations, and obligations of both the Service Provider and the Customer.

4. Service Overview

1. Definitions

"Service Provider" means Defended Solutions.

"Customer" means the organisation purchasing the services.

"Services" means the cloud hosting and integration services described in the Service Definition.

"Agreement" means these Terms and Conditions together with the Service Definition and any Order Form.

2. Scope of Services

The Service Provider shall deliver cloud hosting and integration services in accordance with the Service Definition document, including IaaS, PaaS, SaaS, storage, networking, security, and related professional services. Services are tailored following an agreed discovery and design process.

3. Term and Termination

The Agreement shall commence on the effective date stated in the Order Form and continue for the agreed term unless terminated earlier. Either party may terminate for material breach subject to reasonable notice. On termination, data access and extraction will be provided in line with Section 12.

4. Customer Responsibilities

The Customer shall provide accurate information, maintain appropriate security controls, comply with applicable laws, and cooperate with testing, onboarding, and operational activities.

5. Service Provider Responsibilities

The Service Provider shall deliver the Services with reasonable skill and care, provide documentation and guidance, monitor service performance, and respond to incidents in line with agreed service levels.

6. Service Levels and Support

Service levels, response times, and availability targets are defined in the Service Definition and applicable SLAs. Support is provided via designated ticketing and communication channels.

7. Incident and Fault Management

Incidents will be logged, categorised, prioritised, investigated, and resolved in accordance with the Service Definition. The Service Provider will provide updates during incident resolution.

8. Escalation

Escalation paths for unresolved incidents are defined in the Service Definition, including technical, management, and executive escalation where required.

9. Onboarding and Offboarding

The Service Provider will support onboarding, configuration, and training. On offboarding or termination, reasonable assistance will be provided to support data migration and service exit.

10. Data Backup and Disaster Recovery

Data backup, restore, and disaster recovery arrangements are provided as described in the Service Definition. Recovery objectives depend on the selected service options.

11. Security and Governance

The Service Provider operates security and governance controls aligned with recognised standards, including access control, encryption, monitoring, and regular reviews.

12. Data Access and Exit

Upon termination, the Customer may securely access and retrieve their data for an agreed period, subject to contractual and regulatory requirements.

13. Confidentiality

Both parties shall treat all confidential information as confidential and shall not disclose it except as required by law or agreed in writing.

14. Complaints

Complaints may be raised through designated support channels and will be handled in accordance with documented procedures.

15. Limitation of Liability

Liability shall be limited to the extent permitted by law and as set out in the Order Form. Neither party shall be liable for indirect or consequential losses.

16. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of England and Wales.