

DMZ-in-a-box – Terms and Conditions

1. Introduction

These Terms and Conditions apply to the provision of the DMZ-in-a-box service by the supplier to the customer under a G-Cloud contract. They should be read alongside the applicable G-Cloud Framework Agreement, Order Form, and Service Definition.

Where there is any conflict, the G-Cloud Framework Agreement takes precedence.

2. Definitions

"Service" means the DMZ-in-a-box appliance and service.

"Customer" means the organisation purchasing the Service.

"Supplier" means the organisation providing the Service.

"Service Definition" means the document describing the Service scope, features, and delivery model.

3. Service provision

The Supplier shall provide the Service in accordance with the Service Definition and the agreed Order Form.

The Service is deployed within the Customer's environment and operates in conjunction with existing customer systems, including VPN gateways and monitoring platforms.

The Supplier does not provide VPN termination, client software, or general network infrastructure services.

4. Customer responsibilities

The Customer is responsible for:

- Providing suitable infrastructure and network access for the Service
- Maintaining the availability and resilience of the hosting environment
- Ensuring appropriate access controls within their environment
- Operating and monitoring customer-owned systems, including SIEM platforms

5. Support services

Support is provided as an optional paid service unless otherwise stated in the Order Form.

Support may include: - Email and online ticketing support - Configuration and integration assistance
Incident investigation and troubleshooting

Support hours, response targets, and scope are defined in the Order Form.

6. Availability and service levels

The Service is designed to support high-availability deployments where implemented by the Customer.

Any availability service levels or service credits are defined in the Order Form and apply only to Supplier managed service components.

No availability guarantee applies to single-instance or Customer-managed infrastructure unless explicitly agreed.

7. Information security

The Supplier aligns its security practices with NCSC Cyber Essentials and Cyber Essentials Plus requirements.

The Customer retains responsibility for the security of their hosting environment and connected systems.

The Supplier shall notify the Customer of any security incident affecting the Service where applicable.

8. Data protection and data ownership

The Customer retains ownership of all data generated by or processed through the Service.

Service telemetry, logs, and packet capture data are provided in standard, non-proprietary formats.

The Supplier does not claim ownership of Customer data.

9. Data export and exit

At the end of the contract, the Supplier will support controlled service withdrawal in accordance with the Service Definition.

Customers may extract their data directly from their systems or request assistance during the agreed offboarding period.

10. Changes to the service

The Supplier may make changes to the Service to maintain security, performance, or compatibility.

Customer-impacting changes will be communicated where appropriate.

11. Liability

Liability is limited in accordance with the G-Cloud Framework Agreement.

The Supplier is not liable for issues arising from Customer-managed infrastructure, third-party services, or unsupported configurations.

12. Termination

Either party may terminate the contract in accordance with the G-Cloud Framework Agreement.

On termination, the Service will be decommissioned in a controlled manner.

13. Governing law

These Terms and Conditions are governed by the laws of England and Wales.

14. Document control

Document version: 1.0

This document is provided in an accessible format suitable for conversion to PDF/A or Open Document Format.