

Cloud IT Support

Service Definition Document

Interested Parties

Interested Party	Name	Position
Dolphin IT Solutions	Andy Taylor	Director

Modification history

Version	Description of Change	Author	Date
1.0	Initial drafting	Joshua White	26-01-2026

Referenced Documents

Version	Document Name	Author	Date



CONTENTS

1	Introduction	4
1.1	About Dolphin IT Solutions	4
1.2	Our Team	4
2	What the Service Is	5
2.1	Service Scope	5
2.2	Exclusions	5
3	Service Levels and Support Hours	6
3.1	Service Levels	6
4	Onboarding	7
5	Incident Management	7
6	Change Management	7
7	Reporting and Governance	7
8	Exit & Transition Support	7
9	Security	7
10	Customer Responsibilities	7



1 Introduction

This document sets out the scope, service levels, operating models key features and benefits of our cloud IT support services for Microsoft 365 and cloud-managed devices.

1.1 About Dolphin IT Solutions

Dolphin IT Solutions is a specialist managed security services provider with deep technical expertise in the Microsoft ecosystem. We deliver a wide range of enterprise-grade solutions, including:

- Microsoft 365 and Google Workspace licences
- Hosting in Microsoft Azure, Google Cloud Platform and Amazon Web Services
- Hardware – computers / laptops / mobiles
- End user IT Support for M365, Google Workspace, and third-party applications
- Security products and solutions, accreditations
- Low code business process management solutions through our partner company WEBCON
- Bespoke software development and AI-driven solutions

Our in-house development team also delivers bespoke software solutions, including AI-driven applications, tailored to the specific needs of our clients. Our developers hold Microsoft certifications to prove our expertise and commitment to delivering high quality output. We are Cyber Essentials Plus certified and hold ISO 9001 accreditation for quality management, and ISO 27001 accreditation for data security.

1.2 Our Team

Dolphin IT Solutions is a small enterprise with an organisational structure that allows us to deliver projects end-to-end without relying on a single individual. Our team structure is as follows:

- **Project team** – engineers covering bespoke development, cloud hosting (Azure), AI, security and low-code solutions such as Microsoft Power Platform and WEBCON BPS.
- **Support team** – end user IT support, operational support including customer onboarding assistance, incident triage, and first line troubleshooting where needed.
- **Management** – project oversight and escalation handling.

We avoid having a single point of failure by ensuring each key responsibility has at least two people able to pick up work, maintaining continuity during leave or peak workload. We have a knowledge base for support issues, and our coding standards require high-quality coding documentation, so knowledge is not held by one person. All code changes are reviewed by another colleague to maintain knowledge of the system and changes to it across the team.



2 What the Service Is

Our IT support services are designed for UK public sector organisations. We provide remote, ongoing operational support for Microsoft 365 and cloud-managed Windows endpoints, helping organisations remain secure and operational, knowing their cloud services align with compliance requirements.

The service focuses on day-to-day support, incident management, user assistance, and minor configuration changes for supported cloud services. It does not include large-scale transformation programmes or major migration projects unless explicitly agreed.

2.1 Service Scope

The service provides remote operational support for cloud-based services, including:

- Microsoft 365 tenant administration and configuration
- End-user support for cloud services and managed devices
- Incident logging, investigation, and resolution
- Routine security monitoring and remediation
- Cloud-managed device configuration and compliance enforcement
- Backup monitoring and data protection for cloud-hosted services
- Reporting on service performance and security posture

Support is delivered in line with agreed priorities and response targets.

2.2 Exclusions

Unless explicitly agreed in writing, the service does not include:

- Hardware maintenance or repair
- Local network or on-premises infrastructure support
- Non-cloud applications or legacy systems
- Large-scale projects or migration programmes

Small changes or limited migrations may be delivered where agreed in advance.

On-site support may be provided upon request by prior agreement; a mileage charge will apply.



3 Service Levels and Support Hours

A dedicated Technical Account Manager is assigned to each customer. Support is provided remotely during standard operating hours:

- Support hours: 7am – 7pm UK time, Monday to Friday
- Standard response targets:
 - Urgent issues: within 30 minutes
 - Low-priority issues: within 4 hours
- Out-of-hours and weekend support can be provided by agreement through our extended support plan.

Response targets relate to initial acknowledgement and triage and do not constitute guaranteed resolution times. Bespoke development and major system changes fall under consultancy services.

3.1 Service Levels

The service is available in the following support tiers.

3.1.1 Core IT Support

Our Core IT Support plan provides standard end-user and operational support for cloud-based services, including Microsoft 365 administration, routine security monitoring, updates, and compliant configuration. This tier supports stable day-to-day cloud operations aligned with UK public sector expectations.

A dedicated Technical Account Manager is assigned to provide service oversight and coordination.

3.1.2 Managed IT & Support

Our Managed IT & Support plan provides enhanced cloud support with proactive security monitoring and remediation activities, including cloud-managed device configuration and application patching.

This tier is designed for public sector environments with higher security and operational assurance requirements.

A dedicated Technical Account Manager provides ongoing optimisation and governance support.

3.1.3 Extended Support

Extended Support is available as an optional add-on to both support tiers. It provides:

- Support outside standard operating hours
- Prioritised response handling (outside of our standard response times)

Time spent providing support outside standard hours or responding to prioritised requests is charged at enhanced support rates.

Enhanced support rates are defined in the Pricing Document.



4 Onboarding

Customers are supported through a structured onboarding process, which is typically delivered remotely, and may include:

- Initial service setup and access configuration
- Review of supported services and environments
- Agreement of support priorities and escalation routes
- Introduction to support channels and reporting

5 Incident Management

Incidents are logged and managed through our internal business management system; incidents are prioritised based on urgency and business impact.

6 Change Management

Minor configuration changes and routine updates are included as part of the service. Planned maintenance and change activities are scheduled in advance and communicated to customers in line with agreed change management processes.

7 Reporting and Governance

The service includes regular reporting, which may include:

- Incident volumes and trends
- Security events and remediation activity
- Service performance summaries
- Ticket activities and patterns

Monthly or quarterly governance reviews can be arranged at no additional cost.

8 Exit & Transition Support

On termination or expiry of the contract, we will provide reasonable assistance to support an orderly transition of services. This may include knowledge transfer and handover of documentation where applicable.

Any additional transition or migration activity beyond standard handover may be provided as a chargeable service by agreement.

9 Security

The service operates in line with documented information security policies and recognised good practice. Access to customer environments is restricted to authorised personnel and controlled using role-based access and strong authentication.

Security monitoring and remediation activities are proportionate to the selected support tier.

10 Customer Responsibilities

The customer is responsible for:

- Providing accurate and timely information
- Maintaining appropriate licences for supported cloud services
- Managing users and access approvals
- Using supported services in accordance with applicable laws and policies

The customer remains responsible for the data they store or process within supported cloud services.

