DOLPHIN IT SOLUTIONS

PASSIONATE ABOUT CLIENTS, METICULOUS ABOUT DELIVERY.

ENDPOINT PROTECTION

Service Definition Document

Delivered By DOLPHIN IT SOLUTIONS

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 Hosting 6

4 Availability and Resilience 6

4.1 Disaster Recovery 6

5 Support Model 6

6 Incident & Change Management 6

7 Onboarding 7

8 Data Access & Exit 7

9 Customer Responsibilities 7

10 Security 7

1 Introduction

This document sets out the scope, delivery model, support boundaries, and key features of our Endpoint Protection service, including Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR), provided to UK public sector organisations via the G-Cloud framework.

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 Endpoint Protection service provides advanced endpoint security using behavioural analysis, threat detection, security monitoring and response capabilities.

Where specified, the service includes Managed Detection and Response (MDR), providing human-led monitoring, investigation, and response to detected threats.

The service protects:

- Windows and macOS endpoint devices
- Physical and virtual servers

Dolphin IT Solutions does not develop or host the Acronis platform; it is operated by Acronis.

2.1 Service Scope

Included within the service:

- Endpoint protection and EDR deployment
- Continuous threat monitoring and alerting
- Incident investigation and response workflows
- Managed Detection and Response (where purchased)
- Policy configuration and tuning
- Access to a secure management portal
- Platform-level escalation to Acronis

2.2 Exclusions

The service does not include:

- End-user IT support or device troubleshooting
- Network infrastructure security
- Security consulting outside defined MDR scope
- Incident response beyond agreed service hours

End-user and device support is provided by Dolphin IT Solutions under a separate G-Cloud IT Support offering.

3 Hosting

The Acronis platform is cloud-hosted and operated by Acronis.

Security telemetry and service data are processed in UK-based data centres, subject to Acronis service architecture.

4 Availability and Resilience

The service is built on resilient cloud infrastructure with redundancy, monitoring, and automated recovery mechanisms provided by Acronis.

4.1 Disaster Recovery

The service includes platform-level redundancy and failover provided by Acronis. Disaster recovery for protected endpoints, including restoration decisions and timelines, remains the responsibility of the Customer.

5 Support Model

Support is provided during 7am-7pm UK time, Monday to Friday, via email, phone, and ticketing.

Where MDR is included, security analysts provide:

- Alert triage
- Threat investigation
- Escalation and response actions.

6 Incident & Change Management

Security incidents are detected automatically and investigated according to defined response procedures.

Configuration changes are controlled and documented. Platform changes are managed by Acronis.

7 Onboarding

The Supplier will:

- Deploy endpoint agents
- Configure security policies
- Validate monitoring and alerting
- Provide onboarding guidance

8 Data Access & Exit

Customers retain ownership of all endpoint data and telemetry.

At contract end:

- Security reports and incident records can be provided
- Data is securely deleted following confirmation from the Customer

9 Customer Responsibilities

Customers are responsible for:

- Authorising endpoint onboarding
- Maintaining administrative access
- Responding to escalated incidents
- Complying with security and regulatory obligations

10 Security

The Endpoint Protection service includes:

- Encrypted communications
- Role-based access control
- MFA-protected administration
- Continuous monitoring and logging

Dolphin IT Solutions operates ISO 27001-aligned security governance for all access to customer tenants. Administrative access is controlled using role-based access and MFA.