

ENDPOINT PROTECTION

Terms and Conditions

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	Scope of Services	4
1.2	Governing Law.....	4
2	Third-Party Software and Licensing.....	5
3	Licence Commitments and Billing	5
4	Customer Responsibilities	5
5	Suspension of Services	5
6	Service Availability and Dependency.....	5
7	Support & Managed Detection and Response	6
8	Information Security	6
9	Data Ownership and Access	6
10	Exit and Transition.....	6
11	Liability.....	6
11.1	Third-Party Platform Dependency	6



1 Introduction

These Terms and Conditions (“Supplier Terms”) apply to the provision of Acronis Endpoint Protection services, including Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) (“Services”) provided by Dolphin IT Solutions (UK) Ltd (“Supplier”) to the customer (“Customer”).

The Services are provided under the G-Cloud 15 framework and are subject to the G-Cloud Call-Off Contract. In the event of any conflict:

- The G-Cloud Call-Off Contract takes precedence;
- then these Supplier Terms;
- then applicable Acronis licence terms and end-user agreements.

These Supplier Terms do not replace or override the G-Cloud Call-Off Contract.

1.1 Scope of Services

The Supplier provides Acronis endpoint security licensing, configuration, monitoring, and managed detection and response services as an authorised Acronis service provider and reseller.

The Services include endpoint threat monitoring, alerting, investigation, and response activities as described in the applicable Service Definition, where MDR is specified.

The Supplier does not develop, host, or operate the Acronis core software platform or underlying infrastructure.

1.2 Governing Law

These Supplier Terms are governed by the laws of England and Wales, in accordance with the G-Cloud Call-Off Contract.



2 Third-Party Software and Licensing

Acronis endpoint security software is proprietary software owned and licensed by Acronis International GmbH.

Use of the software is governed by Acronis licence terms and acceptable use policies, which apply directly between Acronis and the Customer.

The Supplier does not grant any intellectual property rights in Acronis software and has no authority to amend or vary Acronis licence terms.

The Customer agrees to comply with all applicable Acronis licence terms and usage requirements.

3 Licence Commitments and Billing

Service features are determined by Acronis licensing and commercial models; pricing is determined by the Supplier in alignment with those models.

Licences are automatically calculated based on the number of protected endpoint devices onboarded to the service.

All services are supplied on a minimum twelve-month commitment term and cannot be cancelled during the applicable term.

The Supplier will confirm licence quantities, pricing, commitment periods, and billing arrangements at the point of order.

4 Customer Responsibilities

The Customer is responsible for:

- ensuring endpoint devices to be protected are authorised for onboarding;
- maintaining appropriate administrative access to deploy and manage endpoint agents;
- managing users, roles, and access permissions within the service;
- complying with applicable Acronis licence terms and acceptable use policies;
- ensuring lawful use of the Services.

The Customer remains the data controller for all endpoint data and telemetry processed using the Services.

The Customer is responsible for monitoring the number of endpoint devices onboarded to the service, as licence quantities are automatically calculated based on device count.

5 Suspension of Services

The Supplier may suspend access to all or part of the Services where required to:

- comply with Acronis policies or contractual obligations;
- address security, legal, or compliance risks;
- prevent misuse of the Services;
- comply with applicable law or regulatory obligations.

Any suspension will be proportionate, limited to the affected Services where possible, and managed in accordance with the G-Cloud Call-Off Contract.

6 Service Availability and Dependency

The availability and performance of the Services depend on the Acronis platform and associated third-party infrastructure.

The Supplier does not guarantee uninterrupted availability of the Services and is not responsible for service interruptions or failures caused solely by faults, outages, or changes within Acronis systems or third-party infrastructure outside the Supplier's reasonable control.



7 Support & Managed Detection and Response

Support and managed services are provided in accordance with the applicable Service Definition.

Where Managed Detection and Response (MDR) is included, this consists of security monitoring, alert triage, investigation, escalation, and response actions performed by security analysts during agreed service hours. MDR is a managed service and does not guarantee prevention of all security incidents.

Platform-level issues may be escalated to Acronis where required.

Support hours for coordination and escalation are 7am-7pm UK time, Monday to Friday, unless otherwise agreed.

8 Information Security

The Supplier operates under documented information security policies aligned with recognised standards, including ISO 27001.

Access to customer environments is restricted to authorised personnel and controlled using role-based access and strong authentication. All access for support and / or MDR purposes is logged and monitored.

9 Data Ownership and Access

All endpoint data, security telemetry, alerts, and incident information remain the property of the Customer.

Data is processed within the Acronis platform in accordance with the Service Definition and Acronis security controls.

The Supplier accesses customer data only where required to deliver the Services, including support, monitoring, investigation, escalation, and response activities.

10 Exit and Transition

On expiry or termination of the Call-Off Contract, the Supplier will:

- provide security reports and incident records generated during the service, on request;
- provide reasonable assistance to support transition to another supplier or service.

Following confirmation from the Customer, remaining endpoint telemetry and service data will be securely deleted in line with the service data sanitisation process.

Termination does not remove the Customer's obligation to pay for services supplied during the applicable commitment term.

11 Liability

Liability between the parties is governed by the provisions set out in the G-Cloud Call-Off Contract.

Nothing in these Supplier Terms limits or excludes liability beyond what is permitted under the G-Cloud Call-Off Contract.

11.1 Third-Party Platform Dependency

To the extent permitted under the G-Cloud Call-Off Contract, the Supplier is not responsible for service failures caused solely by faults or outages in third-party platforms or infrastructure outside the Supplier's reasonable control, including the Acronis platform.

