AMICIS GROUP

Together, we'll build cyber resilience.

Amicis Group Delivery
G-Cloud 15
Terms and Conditions –
CyberGuard
January 2026

hello@Amicisgroup.co.uk

www.Amicisgroup.co.uk

hello@Amicisgroup.co.uk
www.Amicisgroup.co.uk

Service Terms and Conditions

CyberGuard

Supplier: Amicis Group Limited
Framework: G-Cloud 15
Service Reference: [Service ID]
Last Updated: 07/01/2026

1. Purpose

These Service Terms and Conditions describe the operational and service-specific terms applicable to the **CyberGuard** service ("the Service").

These terms supplement the G-Cloud Call-Off Contract and do not replace or override it.

2. Relationship to G-Cloud Terms

These Service Terms and Conditions shall be read in conjunction with the G-Cloud Framework Agreement and Call-Off Contract.

In the event of any conflict, the G-Cloud Call-Off Contract shall take precedence.

3. Service Description

CyberGuard is a comprehensive managed cyber security service providing layered protection across people, processes and technology.

The Service includes, as applicable:

- Managed Detection and Response (MDR), including EDR/XDR
- Penetration testing
- Vulnerability scanning and management
- Cloud security posture management
- Identity security posture management
- Incident response retainer
- DNS and Dark Web monitoring
- Cyber Essentials and Cyber Essentials Plus support
- Security awareness and phishing training
- Workstation security reviews

- Backup as a Service (BaaS)
- Disaster Recovery as a Service (DRaaS)

The Service does not include:

- Remediation work outside the defined scope unless separately agreed
- Legal, regulatory or insurance advice

4. Service Scope and Assumptions

The Service is delivered on the basis that:

- The Customer provides accurate asset and user information
- Supported operating systems and platforms are in use
- Required administrative access is granted
- Third-party platforms operate as expected

Failure to meet these assumptions may impact service implementation and effectiveness.

5. Onboarding and Implementation

5.1 Onboarding Activities

Onboarding typically includes:

- Service scoping and configuration
- Deployment of required tools and agents
- Baseline security assessment
- Agreement of reporting and escalation paths

5.2 Customer Responsibilities During Onboarding

The Customer must:

- Provide timely access and approvals
- Nominate a primary technical contact
- Support deployment across agreed environments

6. Service Levels and Support

6.1 Monitoring and Support Coverage

- Security monitoring: 24x7
- Support hours: 09:00 – 17:00 Monday to Friday

6.2 Incident Handling

Security incidents are triaged, investigated, and responded to in line with the Service scope and agreed response targets.

6.3 Maintenance

Planned maintenance will be communicated in advance where reasonably possible.

7. Customer Responsibilities

The Customer is responsible for:

- Acting on remediation guidance provided
- Maintaining appropriate access controls
- Ensuring staff participation in security awareness training
- Informing the Supplier of material changes to the environment

8. Security and Compliance

The Service supports alignment with recognised security standards and UK public sector expectations, including Cyber Essentials where applicable.

Security activities are limited to defined systems, accounts, and environments.

9. Reporting and Visibility

The Customer will receive reporting which may include:

- Threat and incident summaries
- Vulnerability and risk metrics
- Compliance-related reporting
- Backup and recovery status

Reporting frequency and format vary by component and are agreed within the onboarding process.

10. Change Management

hello@Amicisgroup.co.uk
www.Amicisgroup.co.uk

The Supplier may enhance or modify the Service to:

- Improve security outcomes
- Address emerging threats
- Maintain platform compatibility

Material changes will be communicated in advance.

11. Service Limitations

The Service:

- Does not guarantee prevention of all cyber incidents
- Relies on third-party technologies and data sources
- Cannot remediate risks without Customer approval

12. Offboarding and Contract End

At contract end:

- Access to the Service will be withdrawn
- Customer data will be returned or securely deleted in accordance with the Call-Off Contract
- Reasonable transition assistance will be provided

13. Pricing Basis (Informational Only)

Pricing is based on:

- Per user, per endpoint, or per service component
- Scope defined in the G-Cloud service listing

Payment terms are governed by the Call-Off Contract.

14. Contact and Escalation

Support requests are raised via:

- [Support portal / email / phone]

Escalation paths are available on request.

hello@Amicisgroup.co.uk
www.Amicisgroup.co.uk

15. Pricing Definitions

CyberGuard is charged at £57 per user per month for a minimum contractual period of three years.

16. Entire Service Terms

These Service Terms apply solely to **CyberGuard** and must be read alongside the G-Cloud Call-Off Contract.