Cyber Security as a Service
(CSaaS)

Service Description Document

Supplier: **Sailotech UK Limited**
Version – V 1.1
Date: 27th January, 2026

Table of Contents

+44 1296 841116
marcom@sailotech.com
G12, The Gatehouse, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 8DB, United Kingdom

1. Service Overview

Cyber Security as a Service (CSaaS) provides continuous, proactive protection for public sector organisations. The service combines monitoring, threat detection, vulnerability management, compliance support, and incident response. Delivered by certified professionals, it helps organisations reduce cyber risk, strengthen resilience, and protect critical systems, data, and services.

2. Service Scope

The service includes:

- Security monitoring and alerting
- Vulnerability and risk management
- Incident response and recovery support
- Security architecture and system assurance
- Compliance and governance guidance
- Third-party and supply chain risk assessments

Coverage is limited to systems and environments agreed in the contract.

3. Service Features

- 24/7 monitoring and real-time threat detection
- Vulnerability scanning and penetration testing
- Incident response, containment, and forensics
- Security architecture design and assurance
- Cloud, network, and identity protection
- Compliance readiness (ISO 27001, GDPR, NCSC)
- SOC services with SIEM and analytics
- Vendor and system security advisory
- Risk reporting and dashboards
- Continuous security improvement

4. Service Benefits

- Reduces cyber risk and operational disruption
- Improves security visibility and decision-making
- Simplifies compliance with public sector standards
- Accelerates secure cloud adoption

- Reduces incident impact and recovery time
- Enhances organisational resilience
- Reduces internal security workload
- Improves governance and risk management
- Enables faster threat detection
- Supports continuous security maturity

5. Service Constraints

The service is primarily delivered remotely unless otherwise agreed. Buyers must provide timely access to systems, logs, and stakeholders. Remediation requires buyer approval. Effectiveness depends on accurate information. Third-party systems may limit monitoring. Hardware and licences are excluded unless stated.

6. Support Levels

- **Standard**: Mon–Fri 09:00–17:30, email/ticket, 1-hour response (included).
- **Enhanced**: 07:00–20:00, priority support, quarterly reviews (+15%).
- **Premium**: 24/7, named Technical Account Manager and Cloud Security Engineer, monthly reviews (+25%).

7. Onboarding & Offboarding

Onboarding includes scope definition, access setup, risk baseline, and configuration. Offboarding includes data handover, secure deletion, and final reporting.

8. Security & Compliance

Aligned to ISO 27001, GDPR, UK NCSC guidance, and public sector standards. Staff are security screened. Data is handled securely and confidentially.

9. Accessibility

All service communications and portals follow WCAG 2.2 AA and GOV.UK accessibility guidance.

10. Service Hours

Standard: Monday–Friday, 09:00–17:30 UK time.
Out-of-hours support available under Enhanced and Premium tiers.