

Service Definition Document - Cloud Service Support

Service Description

Quantum Secret's Cloud Service Support service provides ongoing operational support for public, private and hybrid cloud systems operating in high-threat environments. This is a streamlined, security-focused support service designed to maintain availability and integrity without the overhead of traditional enterprise support models.

The service is designed for organisations operating in defence, government, and critical infrastructure sectors who require assured support from appropriately vetted personnel, without the complexity and cost of heavyweight managed service arrangements.

The service covers infrastructure deployed across public cloud platforms (AWS, Azure, GCP), private cloud, and on-premises environments including OpenShift and Proxmox Virtual Environment (PVE), with particular emphasis on maintaining security posture across hybrid boundaries.

Scope of Service

The service includes:

- Incident response and resolution for infrastructure issues
- Configuration changes within agreed parameters
- Patching coordination and implementation
- Performance troubleshooting and optimisation
- Vendor liaison and escalation management
- Security event triage and initial response coordination
- Routine health checks and proactive maintenance
- Documentation updates and configuration management

The service operates on a direct-to-engineer model with minimal ticket bureaucracy, using secure communication channels and rapid triage. This provides a focused scope covering infrastructure and platform layers rather than application code.

Support Levels

Three support tiers are available:

Standard Support

- Business hours support (0900–1700 UK local time, Monday to Friday excluding UK public holidays)
- Ticket-based requests via secure portal or email
- Prioritised response based on severity
- Suitable for non-production environments or organisations with internal first-line capability

Enhanced Support

- Business hours support with faster response times
- Named Cloud Support Engineer as primary point of contact
- Monthly service review and proactive health checks
- Suitable for production environments requiring assured response

Premium Support

- Extended hours or 24/7 support by arrangement
- Named Cloud Support Engineer with Technical Account Manager oversight
- Priority response and proactive monitoring coordination
- Quarterly strategic reviews
- Suitable for high-threat, mission-critical deployments

Response times vary by support tier and incident priority. Specific response time commitments are detailed in the Pricing Document.

Engineering support

Our Enhanced and Premium support tiers include direct access to our engineering function.

- **Engineer.** Primary technical point of contact for day-to-day support matters, incident escalation, and hands-on troubleshooting. Available on Enhanced and Premium tiers.
- **Technical Lead.** Oversight, service reviews, roadmap alignment, and escalation management. Available on Premium tier.

Standard support doesn't include a named contact but provides access to the team via our service management tool.

OFFICIAL

Data Backup and Disaster Recovery

The support service assists with backup and disaster recovery operations within customer environments, including monitoring backup success, coordinating restore testing, and supporting recovery activities during incidents.

Design and implementation of backup and disaster recovery solutions is provided through our Cloud Solution Development service. The support service maintains and operates solutions already in place.

Onboarding and Offboarding

Onboarding includes initial environment assessment, documentation of supported infrastructure, access provisioning, establishment of secure communication channels, and agreement of support procedures. A dedicated point of contact is assigned for the duration of the engagement.

Offboarding includes handover of all documentation and configuration records, knowledge transfer sessions where required, and removal of supplier access to customer environments.

Service Constraints

The following constraints apply:

- Support is delivered remotely by default; on-site attendance is available by prior arrangement and may incur additional charges
- Support covers infrastructure and platform layers only; application-level code fixes and development work are excluded unless separately agreed
- Access to customer environments is required for effective support delivery; constraints on connectivity or access may limit service scope
- For air-gapped or disconnected environments, support is provided through agreed secure communication methods and may require on-site presence for certain activities
- Out-of-hours and 24/7 support is available by prior arrangement and subject to contract
- Response times are dependent on the priority level assigned and the support tier contracted
- Third-party vendor support (e.g., AWS, Azure, Microsoft) is coordinated but not replaced by this service; vendor support contracts remain the customer's responsibility
- Security clearance requirements beyond BS7858 screening

OFFICIAL

may extend onboarding timescales for personnel

- Maximum supported environment complexity and scale is agreed during onboarding; significant changes may require contract review

Service Levels

Standard support hours are 09:00 to 17:00 UK time, Monday to Friday, excluding UK public holidays. Extended or out-of-hours support is available on Premium tier or by prior arrangement.

Response times by priority (Enhanced tier shown as example):

- P1. Critical (service down, security incident). Response within 1 hour
- P2 High (significant degradation). Response within 4 hours
- P3 Normal (minor issues, requests). Response within 1 business day
- P4 Low (queries, information requests). Response within 2 business days

Specific response time commitments for each support tier are subject to contract agreement. Service levels may be adjusted by mutual agreement to meet specific customer requirements.

After-Sales Support

This is an ongoing support service. Contract renewal and adjustment is available at the end of each contract term. Transition support to alternative suppliers or in-house teams is typically provided during offboarding.

Technical Requirements

This is subject to contract and requirement but typically customer responsibilities include:

- Provision of appropriate access to supported environments and systems
- Maintenance of up-to-date documentation of the supported environment
- Timely communication of changes to the environment that may affect support
- Appropriate vendor support contracts for third-party platforms and software
- Secure communication channels for support interactions where required

OFFICIAL**Outage and Maintenance Management**

The support service coordinates planned maintenance windows with the customer in advance. Emergency maintenance is communicated as soon as practicable through agreed channels.

The supplier does not control cloud provider maintenance schedules but will assist in managing the impact of such events, including coordinating failover activities and customer communication.

Hosting Options & Locations

Support is provided for environments deployed to any cloud region or on-premises location. The supplier is UK-based and can support deployments worldwide.

For high-threat environments, support delivery methods are tailored to classification and connectivity constraints, including support for air-gapped, segmented, and cross-domain architectures.

Access to Data on Exit

All customer data remains the property of the customer throughout and following the engagement. Upon contract termination:

- All documentation and configuration records are handed over to the customer
- Supplier retains no copies of customer data beyond the agreed retention period
- Transition support is provided to alternative suppliers or in-house teams
- Supplier access to customer environments is revoked

OFFICIAL

Security

Security measures include the following:

- Staff screening performed in accordance with BS7858:2019
- Cyber Essentials Plus certification maintained
- Secure support delivery methods appropriate to classification and connectivity constraints
- Experience with air-gapped, segmented, and cross-domain architectures
- Alignment with NCSC guidance and secure-by-design principles
- Encryption of data in transit and at rest as standard
- Access controls based on least privilege principles
- Regular security awareness training for all personnel

Additional security requirements, including security clearances, can be accommodated subject to contract.

OFFICIAL

Page 6 of 6