

Central Support, Patching and Monitoring Schedule

 info@centralnetworks.co.uk

 +44 (0)1706 747474

 www.centralnetworks.co.uk



1. Introduction

1.1. This Support, Patching and Monitoring Schedule defines the services to be provided to the Client by Central in relation to IT Support Services and is subject to:

1.1.1. The Order Form.

1.1.2. The Master Services Agreement

2. Central Support Service

2.1. The service is to be supported during the service hours as defined below:

2.1.1. 8am – 6pm (Monday to Friday) standard business hours

2.1.2. Central is expected to maintain the following access channels during the Service Hours:

2.1.3. An email address direct through to Central helpdesk system

2.1.4. Internet-based access to the Central helpdesk system to provide end user self service facilities

2.1.5. Business hours telephone number - 01706 747444

3. Performance Levels

3.1. The tables below indicate the minimum performance criteria that will be delivered by Central for the services documented in this Schedule. These criteria are in addition to any that may be contained in the general description of the services as contained in below.

3.2. Target Response and Resolution Times –

Priority Level	Description	Response Time	Target Time for Full Fix	Reporting
Priority 1 Urgent	Disaster – Business non-operational, severe customer impact threatening future business productivity	30 minutes	4 hours	updates hourly until repair / preliminary report 1 day / final report 5 days
Priority 2 High	Critical – High impact to operation of business with no workaround available	1 hour	8 hours	updates hourly until repair
Priority 3 Medium	Very Important – Serious problem impacting on efficient running of daily tasks	4 hours	20 hours	updates after progress made or upon request
Priority 4 Low	Important – Important issues that are not significantly affecting business operations	10 hours	30 hours	updates after progress made or upon request
Priority 5 Informational	Normally cosmetic incidents or events that require logging	3 days	90 days (this is rarely used)	updates after progress made or upon request

4. Extensions to Services

4.1. Extensions to the availability of the services indicated above may be provided upon request. In order to facilitate the arrangement of such extension, requests should be submitted to Central at least 10 working days in advance of the requirement.

- 4.2. Central will formally confirm that any such extension is available and advise the client of any additional charges that would apply.

5. Service Failures

- 5.1. In the event of a major service failure, the problem will in the first instance be escalated to the ServiceDesk Manager who will oversee Central's response to the service failure, in event that the ServiceDesk Manager is unavailable the Operations Director will be alerted.
- 5.2. Central will keep the client updated at regular intervals until normal service has been resumed.

6. Incident Prioritisation

- 6.1. Incident Priority agreed between the client and Central at point of logging. All incidents will be logged with a reference number which will be supplied to the end user by the same channel as the call was logged.
- 6.2. Incidents will be treated in strict rotation by priority i.e. highest priority dealt with first; all incidents with equal priority addressed in chronological order of receipt.
- 6.3. The client's ICT Support Manager to be able to reprioritise
- 6.4. In agreement with the ICT Support Manager, the clock measuring performance can be stopped where a third party not directly subcontracted to the Supplier is involved (e.g. Azure, VMware or Microsoft etc.).

7. Priority Codes

- 7.1. Faults will be prioritised by Central according to the following criteria; the Priority Codes will be used by Central to target incident response times.

Priority Code	Impact on the client's business delivery capabilities
1	Emergency problem of critical operational and/or financial impact
2	Serious problem directly impacting on the service
3	Problem not impacting on the normal operations of the service
4	Minor problem or general enquiry and minor service request
5	Service request

8. Service Manager Support

- 8.1. A dedicated service manager will be assigned who will act as the prime point of contact with the client on all matters related to IT (other than incident calls which should be routed direct to the Support Desk). The Service Manager will be responsible for ensuring that all appropriate actions are taken within Central to achieve a satisfactory resolution of all IT enquiries.
- 8.2. The Service Manager will:
- 8.2.1. Act as a point of contact so that the client can raise their concerns and discuss pressing issues related to their IT.

- 8.2.2. Ensure that reported incidents are promptly acted upon by the Support Desk Team and provide regular feedback to the client on their progress.
- 8.2.3. Provide regular reporting material to the client regarding service performance, resolution of support desk queries/faults, and progress on current projects etc.
- 8.3. The Service Manager will also attend meetings to:
 - 8.3.1. Discuss progress statements at summary or detail level on the performance of current operational systems.
 - 8.3.2. Brief the client on current and future Central services or initiatives.
 - 8.3.3. Discuss at summary or detail level progress on current projects.
 - 8.3.4. Note any new client needs and requirements and provide advice on how to meet these.
 - 8.3.5. Review Central services delivery against the commitments given in the SLA.

9. Client Responsibilities

- 9.1. To facilitate the successful delivery of the services covered by the agreement, the client undertakes to: -
 - 9.1.1. Use active anti-virus software on all equipment and ensure this is updated regularly.
 - 9.1.2. Ensure bespoke software (Inhouse Software) is appropriately patched to prevent virus and other security incidents.
 - 9.1.3. Instruct/brief staff regularly on ICT security and appropriate behaviours to reduce the risk of security incidents.
 - 9.1.4. Receive the charges and make payment for the services as specified in this agreement on receipt of invoice on the agreed terms.
 - 9.1.5. Reimburse Central for any damage caused to its equipment because of client misuse.
 - 9.1.6. Provide a named officer(s) to act as point of contact for the client with respect to the provision of the various services covered by the agreement, including the initial reporting of any IT related problems or service requests.
 - 9.1.7. Take all reasonable measures to ensure that the requirements of all relevant Acts such as the Data Protection Act and the Copyright Act are complied with.
 - 9.1.8. Maintain an inventory of all IT to be supported by Central and notify Central of all staff changes or changes to supported assets
 - 9.1.9. Contribute to the testing of any Disaster Recovery Plan and other processes.
 - 9.1.10. Provide details of emergency contacts for out of hour's services.
 - 9.1.11. To agree to any reasonable changes proposed by Central In order to reduce recurring Incidents
 - 9.1.12. Maintain all equipment and software to versions supported by the appropriate manufacturer
 - 9.1.13. The follow agreed Change Control procedures.
 - 9.1.14. To not move equipment without first notifying Central
 - 9.1.15. To ensure that It has adequate data backup facilities In place.

10. Exclusions

- 10.1. Unless otherwise stated on the Order Form the following platforms are not supported:
 - 10.1.1. Bespoke application issues

- 10.1.2. Telephony system
- 10.1.3. Hardware assistance on workstations
- 10.1.4. Any equipment which the Company reasonably considers to be end of life, out of manufactures support, beyond repair, for which consumables, spare parts, drivers or updates are not readily available or require essential maintenance
- 10.1.5. End user computing facilities unless agreed in the Quote
- 10.1.6. Recovery from or Investigation into any kind of cyber-attack.
- 10.1.7. Application of vendor updates

11. Description of Services

- 11.1. The sections below define the services that will be provided by Central to the client under the terms of this agreement.

12. 1st Line Support

- 12.1. The Company shall provide 1st line support to the Client, including the collation, checks and triage of Incidents, with actions taken deemed to be moderate impact, low risk activities and dealt with as follows:
- 12.2. collecting the inbound request from the Client via either Central helpdesk system or an inbound call Desk;
- 12.3. confirming the name, location, contact details of the end user reporting, are complete (including Data Protection checks completed for phone-based incidents);
- 12.4. confirming the specific details of the request are complete, and;
- 12.5. assigning a priority status in accordance with Priority Codes above, the Company shall confirm if an action plan can be written for the request and if it can, then the ticket will be processed.
- 12.6. If the action plan fails to resolve the Incident, requires a site visit, a plan cannot be written or committed to (due to knowledge or access), the ticket will be escalated to the Company's service team (or nominated contact) to proceed with the initial request and resolve.

13. 3rd Line Support

- 13.1. Where escalated tickets that have been logged and triaged by the Client, then escalated to the Company via the Central helpdesk system, due to unsuccessful resolution via the Client's internal service team, the following must have been completed by the Client prior to escalation:
 - 13.1.1. All steps in paragraph 13 above have been documented in respect of 1st line support;
 - 13.1.2. Document and supply all actions taken by the Client's service team;
 - 13.1.3. Document and supply all logs, screen shots, supporting information, and;
 - 13.1.4. Ensure that the documented priority for the incident as stated in 1st line support is still current and correct upon acceptance of the request by the Company, the service team will review and manage the incident.
- 13.2. The Company shall communicate with the Client's service team or nominated contact to the point of resolution of the incident.

13.3. Where required the Company's service team will call upon the Client's service team or nominated contact to complete local actions, where appropriate.

14. Network and Infrastructure Support

14.1. The Company shall, where applicable, provide the Client with full incident lifecycle support of the Clients network and supported equipment which is used by the client to support its normal business operations, including one or more of the following options:

14.2. Hardware - maintain and deliver support in accordance with the Service Levels on applicable Supported Equipment, subject to a valid Third-Party Supplier warranty or support contract, and;

14.3. Operating System Software - maintain and deliver support in accordance with the Service Levels on applicable Operating System Software, subject to a valid License Agreement

14.4. Where appropriate and as set out in the Order. The services set out here may be supplied alongside other support services offered by the Company.

14.5. Support is focused on the active monitoring and care of the Client network and supported equipment on which the Client, through the RMM Platform (subject to the installation of RMM Agents) and is predominately delivered with remote support sessions by use of remote access tools, which enable the Company to monitor and alert on various metrics.

15. Change Management

15.1. The Supplier upon request by the Customer can undertake Change Requests and will manage all changes covered under the Services from scoping to release and testing in accordance with the Change Request process.

15.2. The Customer shall submit a Change Request through the Service Desk, subject to additional charges as follows:

15.3. Elective Changes on a fixed cost basis for common changes that do not require a detailed scope of works;

15.4. Customised Changes are specific to the Customer and are scoped on a case-by-case basis with the Customer being charged on a time and materials basis;

15.5. All Elective Changes are completed on a time/materials basis and charged to the Customer as per the Supplier's Standard Schedule of Rates.

15.6. The Customer may also purchase, at the Commencement Date, a specific quantity of Technical Attendance Days which will be set out in the applicable Order.

15.7. For the avoidance of doubt, Customised Changes under above shall be outside of the scope and terms of this Schedule and subject to a separate Order.

16. System and Monitoring

16.1. The Company shall provide real-time monitoring with intelligent alerting, subject to the mandatory installation of the company's preferred RMM tool.

16.2. The supported equipment will be installed with RMM agents to monitor and help manage the current state at any time, with data from the Client network being securely passed between the supported equipment and the RMM platform and displayed for the Company to action or escalate as appropriate.

- 16.3. Each RMM agent installed is responsible for monitoring the following details on the Client network and supported equipment as standard, as well as collecting performance data on metrics for reporting purposes
- 16.4. The Company shall agree with the Client criticality and business impact for the Client network and supported equipment, which will be stored within the RMM platform for reference by Central's service desk, with required actions and escalation procedures based upon the agreed criteria also agreed and stored on the RMM platform for reference.
- 16.5. Any changes or additions to the monitoring requirements shall be made by agreement between the Company and the Client in accordance with the Change control process. A monitoring schedule change shall be undertaken within ten (10) Working Days of the request.

17. Patch Management

- 17.1. The Company's remote patch management service provides comprehensive proactive service across the Clients network and supported equipment using its RMM platform, which provides real time monitoring of Client's monitored assets to ensure that applicable patches/updates are being used.
- 17.2. Hardware drivers, firmware and associated management software updates are outside of the scope of patch management services.
- 17.3. The Company recommends that updates are applied to keep the Client network within supported versions and the Client can request the Company to undertake an infrastructure health check at any time during the term, subject to an additional charge to the Client.
- 17.4. Before any patches or updates can be applied to servers, they must have the relevant recovery procedures in place, including but not limited to a full or adequate back up of the data and operating system. Once the server is updated, testing procedures will be carried out to validate the system and applications have not been adversely affected.
- 17.5. The Client is responsible for ensuring the backup is in place and viable with respect to automatic patching and will report any failures to the Company so the effected patching schedules can be adjusted.
- 17.6. Emergency patches are subject to a change request and changes will be raised as and when either the Client or the Company is made aware of the specific patch.
- 17.7. In the event of an error, the Company shall remove or roll back the patch identified as causing the problem and snapshots may be used by the Company to facilitate the removal but only in instances deemed necessary by the Company.